November 2018

Enhancing the Design of a Cybersecurity Risk Management Solution for Communities of Trust

James E. Fulford Jr.

University of South Florida, ed.fulford@yahoo.com

Follow this and additional works at: https://scholarcommons.usf.edu/etd

Part of the Business Administration, Management, and Operations Commons, and the Databases and Information Systems Commons

Scholar Commons Citation


This Dissertation is brought to you for free and open access by the Graduate School at Scholar Commons. It has been accepted for inclusion in Graduate Theses and Dissertations by an authorized administrator of Scholar Commons. For more information, please contact scholarcommons@usf.edu.
Enhancing the Design of a Cybersecurity Risk Management Solution
for Communities of Trust

by

James E. Fulford, Jr.

A dissertation submitted in partial fulfillment of the requirements for the degree of
Doctor of Business Administration
Muma College of Business
University of South Florida

Co-Major Professor: Alan R. Hevner, Ph.D.
Co-Major Professor: Allen R. DeSerranno, DBA
Donald Berndt, Ph.D.
Matthew Mullarkey, Ph.D.

Date of Approval:
October 12, 2018

Keywords: compliance, conceptual model, Design Science Research, Elaborated Action Design Research, Fitness-Utility Model, NIST CSF

Copyright © 2018, James, E. Fulford, Jr.
# TABLE OF CONTENTS

List of Tables ...................................................................................................................................................... iii

List of Figures ........................................................................................................................................................ iv

Abstract .................................................................................................................................................................. v

Chapter One: Introduction ................................................................................................................................. 1

References ........................................................................................................................................................... 4

Chapter Two: Implementing a Cybersecurity Community of Trust ................................................................. 5

Chapter Three: A Note on the Cybersecurity Problem Spaces in 2018 .......................................................... 6

Chapter Four: Evaluating and Enhancing the Risk Informing Capabilities of a Cybersecurity Solution Using Action Design Research ............................................................................................................. 7

Abstract .............................................................................................................................................................. 7

Introduction ......................................................................................................................................................... 7

Motivation ........................................................................................................................................................... 9

Research Method ............................................................................................................................................. 24

Description of First Artifact Created for the Reprivata CoT Solution ............................................................ 28

Reprivata Solution Conceptual Model .................................................................................................................. 28

Evaluation of the First Artifact Created for the Reprivata CoT Solution ....................................................... 34

Description of Second Set of Artifacts Created for the Reprivata CoT Solution ............................................ 35

Reprivata Solution NIST CSF Assessment ........................................................................................................... 35

Reprivata Solution Recommendations for Enhancing Master Agreements ................................................. 38

NIST CSF Functional Area — Identify (ID) Controls Language to Include .................................................. 39

Evaluation of the Second Set of Artifacts Created for the Reprivata CoT Solution ....................................... 40

Discussion .......................................................................................................................................................... 42

Limitations of Current Research ....................................................................................................................... 46

Conclusions ...................................................................................................................................................... 47

References .......................................................................................................................................................... 50

Chapter Five: Using a Fitness-Utility Model to Elaborate the Impacts of Artifacts Created to Enhance the Risk Informing Capabilities of a Cybersecurity Risk Management Solution ..................................... 52

Abstract .............................................................................................................................................................. 52

Introduction ........................................................................................................................................................ 52

Motivation .......................................................................................................................................................... 54

Interviewing Approach for Artifact Evaluation .................................................................................................. 55
Description of the Fitness-Utility Model Utilized .......................................................... 56
Artifact Description — Reprivata Community of Trust Conceptual Model ................. 58
  Artifact Evolution ........................................................................................................ 59
Risk Informing Changes Made When the Artifact Was Implemented ....................... 60
Specific Cases Where the Artifact Made the Company Make Changes in the Way They Communicated Cyber Risks ................................................................. 61
Quotes from Intervention Participants About the Artifact ....................................... 61
Artifact Description — NIST CSF Assessment for the Reprivata CoT
  Cybersecurity Risk Management Solution (version 4) .............................................. 62
  Artifact Evolution ........................................................................................................ 63
Risk Informing Changes Made When the Artifact Was Implemented ....................... 65
Specific Cases Where the Artifact Made the Company Make Changes in the Way They Communicated Cyber Risks ................................................................. 66
Quotes from Intervention Participants About the Artifact ....................................... 66
Evaluation of the Artifacts’ Usefulness Based on the Fitness-Utility Model ................ 66
  Reprivata Community of Trust Conceptual Model (version 2) ................................. 66
  NIST CSF Assessment for the Reprivata CoT Cybersecurity Risk Management Solution (version 4) ................................................................. 68
Discussion and Interpretation of Results .................................................................. 71
References .................................................................................................................. 72

Chapter Six: Conclusion, Contributions, Limitations, and Future Research .................. 74
  Conclusions ................................................................................................................ 74
  Contributions ............................................................................................................ 78
    Research Contributions .......................................................................................... 78
      Contributions from the Case Study Paper .............................................................. 78
      Contributions from the Technical Note Paper ....................................................... 78
      Contributions from the Design Science Research Paper ...................................... 78
      Contributions from the Enhance Action Design Research Paper ....................... 79
    Contributions to Practice ....................................................................................... 82
  Limitations of Current Research ............................................................................ 83
  Areas Requiring More Research ............................................................................. 84
  References .............................................................................................................. 87

Appendix A .................................................................................................................. 88

Appendix B .................................................................................................................. 137

Appendix C .................................................................................................................. 157
LIST OF TABLES

Table 1: Literature on Research Design Applicable to Cybersecurity Risks ..................12
Table 2: Literature on Understanding and Measuring Cybersecurity Risks ..................15
Table 3: Issues Identified that Impact the Better Understanding of Cybersecurity Risks ....20
Table 4: NIST CSF Security Functions and Control Categories [from NIST CSF v1.1, 2018] .........................................................................................................................30
Table 5: NIST CSF Maturity Tiers [from NIST CSF v1.1, 2018] ..................................30
Table 6: NIST CSF Assessment and Findings for the Reprivata Community of Trust (CoT) Cybersecurity Risk Management Solution .........................................................35
Table 7: Recommendations for Enhancement of Reprivata Master Agreements for Implementing Community of Trust (CoT) Cybersecurity Risk Management Solution .................................................................38
Table 8: NIST CSF Assessment and Findings for the Reprivata Community of Trust (CoT) Cybersecurity Risk Management Solution .........................................................63
Table 9: Estimates of Artifact Usefulness for the Proposed Conceptual Model for the Reprivata Cybersecurity Community of Trust .................................................................67
Table 10: Estimates of Artifact Usefulness for the NIST CSF Assessment for the Reprivata Cybersecurity Community of Trust .................................................................69
Table 11: Design Science Research Contributions by Artifact Type (from Gregor & Hevner, 2013) ..................................................................................................................81
LIST OF FIGURES

Figure 1: Action Design Research Methodology for Reprivata Community of Trust ..............24

Figure 2: Reprivata Community of Trust Conceptual Model ........................................29

Figure 3: Fitness-Utility Model for Design Research (Figure from Gill & Hevner, 2011) ....58

Figure 4: Proposed Conceptual Model – Reprivata Cybersecurity Community of Trust ..........59

Figure A1: Proposed Conceptual Model and Description – Reprivata Cybersecurity Community of Trust ........................................................................................................88
ABSTRACT

Research into cybersecurity risks and various methods of evaluating those threats has become an increasingly important area of academic and practitioner investigations. Of particular interest in this field is enhancing the designs and informing capabilities of cybersecurity risk management solutions for users who desire to understand how organizations are impacted when such risks are exploited. Many of the cybersecurity risk management solutions are extremely technical and require their users to have a commensurate level of technical acumen. In the situation evaluated during this research project, the founders of the company being researched had created a highly technical risk management solution composed of sophisticated networking and cryptography components. The company’s management team, on the other hand, had very little cybersecurity industry background but needed to effectively communicate the specialized capabilities of the solution to potential customers and business partners in an understandable way. In this case, improving the company’s solution design to better convey its technical foundation both inside and outside the company was required. Design Science Research (DSR) offers a methodology that was created to help analyze, create, and evaluate design artifacts that can identify useful ways to work through technical challenges such as those faced by the company. The Elaborated Action Design Research (eADR) methodology can be used to further improve design artifacts through an iterative process that is easily understood by practitioners and academics and grounded in theory. When DSR and eADR methodologies are used together, the result is the creation and demonstration of informing artifacts which will address technical
cybersecurity risk evaluation and communication issues. This research project contains a case study, an accompanying technical note, and two research papers which will address research questions informed by the DSR methodology process in response to related communication and compliance issues noted in the cybersecurity risk management problem space.
CHAPTER ONE:
INTRODUCTION

This research project is motivated by the need for better informing capabilities in current cybersecurity risk management solutions. Cybersecurity practitioners have faced challenges in finding effective ways to communicate the impacts of technology risks for years. The rapid growth in the numbers and types of cyber risks have made these challenges even more formidable. Designing cybersecurity solutions that can bridge the knowledge and information gaps between industry practitioners and stakeholders who need to understand and act on these risks is now a high priority for many organizations, including nation-states. Exacerbating this issue is the increasing business and contractual requirement for such solutions to comply with cybersecurity standards such as the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).

The research approach and design for this dissertation project will incorporate several different qualitative methods including case study, Design Science Research (DSR) and Elaborated Action Design Research (eADR). Four research papers have been written during this project that show the iterative nature of analyzing the design of a cybersecurity solution, building design artifacts to increase the solution’s informing capabilities related to cybersecurity risks, and evaluating the utility of those artifacts with cybersecurity practitioners to determine how the artifacts affect the ability to better understand the impacts of cybersecurity risks.
The primary goal of this research project is to describe or explain the internal and external effects that cybersecurity risks have on organizations. This will be accomplished by creating a conceptual model that can assist IT security practitioners to successfully communicate cybersecurity control interactions in their organizations, based on the NIST CSF framework and findings from this study. To accomplish these goals, the research activities will focus on answering the following questions:

- **What is a conceptual model that can be constructed to identify key IT security risks that a company must address?** – Explanatory Question

- **What are cybersecurity risk management evaluation mechanisms that can be utilized to inform a company of the effective implementation of its cybersecurity controls?** – Explanatory Question

This conceptual model and control evaluation mechanisms are then assessed to determine their utility as used to design a maturity measurement framework for organizations. They can demonstrate how they manage and communicate the company’s ability to mitigate IT security risks as part of their overall risk management processes.

The motivation for this research project is discussed in the third and fourth papers in a separate section that considers related academic literature that either articulated prior work on the research problem or provided a detailed depiction of cybersecurity problem spaces and relevant evidence supporting the investigation. These sections covered findings in the current research and gaps in academic literature that inform the research problem. Following the research motivation, the initial design artifact requirements are analyzed. The requirements are used to build the artifact based on the DSR methodology. Each artifact was iteratively documented and then discussed by internal participants and cybersecurity Subject Matter Experts (SMEs) to
determine its ability to inform those contributors. The research goal of the DSR methodology is to design an artifact that exhibits utility in practice, addresses the research question being studied, and uses a methodology that demonstrates rigorous research principles. The final section of the dissertation project addresses the evaluation of the DSR artifacts through the lens of a fitness-utility model proposed for use by both academics and practitioners (Gill & Hevner, 2011).

The first paper, titled “Implementing a Cybersecurity Community of Trust: Reprivata Seeks an “Early Adopter,”” utilized the case study methodology (Gill, 2011) to inform on specific design gaps identified in the launch of a cybersecurity risk management solution. The second paper, a technical note (Gill, 2011) on cybersecurity problem spaces titled “A Note on the Cybersecurity Problem Spaces in 2018,” performed a review of current literature on the cybersecurity challenges facing businesses, governments, and other entities. The third paper, titled “Evaluating and Enhancing the Risk Informing Capabilities of a Cybersecurity Risk Management Solution Using Action Design Research,” detailed the interactions with the cybersecurity risk management solutions company to analyze and build design artifacts in an iterative fashion that would close the gaps noted in the case study (Hevner, 2014).

After the motivation, build, and review of the DSR artifacts were studied within the context of the cybersecurity risk management solution being assessed, an eADR methodology (Mullarkey & Hevner, 2018) was used to progress and improve the artifacts. The fourth paper, titled “Using a Fitness-Utility Model to Elaborate the Impacts of Artifacts Created to Enhance the Risk Informing Capabilities of a Cybersecurity Risk Management Solution,” discusses how the design artifacts created in the second paper were evaluated using a fitness-utility model (Gill & Hevner, 2011). Cybersecurity practitioners, the management team of the cybersecurity risk
management company, and the company’s business partners were included in these discussions and provided informed estimates of the artifacts’ utility in relation to the cybersecurity risk management solution. The eADR approach documented in the fourth paper demonstrates that the artifacts show real-world utility and introduce design values and principles that are both rigorous and informing to practice.

References


CHAPTER TWO:

SEE APPENDIX B
CHAPTER THREE:

SEE APPENDIX C
CHAPTER FOUR:
EVALUATING AND ENHANCING THE RISK INFORMING CAPABILITIES OF A CYBERSECURITY SOLUTION USING ACTION DESIGN RESEARCH

Abstract
This research project is focused on assisting a startup cybersecurity company in increasing its clients’ understanding of cybersecurity risks as identified by the company’s technology risk management solution. Several artifacts have been created for the solution, including compliance matrices, a solution architecture, a conceptual model for the solution, and recommendations on enhancing the legal agreement between users of the Reprivata Community of Trust (CoT) cybersecurity risk management solution, and other supporting documentation while acting as a researcher embedded within the firm. Discussions with the company’s management and potential clients confirmed that the inclusion of the new artifacts in strategic and technical presentations have increased their understanding of the cybersecurity risks identified by the solution and how those risks are now more meaningful to their clients.

Introduction
The numbers and types of cybersecurity risks that governments, companies, and individuals face are becoming overwhelming and nearly incomprehensible to many of those parties. In current academic literature, researchers investigate ways to foster better understanding of such risks when few cybersecurity risk management applications are available that could help parties manage and comprehend the majority of those risks (Contreras, DeNardis, & Teplinsky, 2012). The emerging types of technology risk management measurements and supporting risk
management methodologies can inform these entities by helping them better understand cybersecurity risks to their particular technology environments while increasing their abilities to comply with cybersecurity program standards and maturity measures (Epstein & Brown, 2008).

In January 2018, the researcher was introduced to the senior executives of a startup cybersecurity risk management company named Reprivata. During a discussion with the company’s management team, the researcher found that while the Reprivata team had a great deal of experience implementing the large interconnected networks that comprised the commercial Internet, they had limited experience in cybersecurity and software development. In fact, the cybersecurity application they had developed was designed originally to set up virtual private networks.

After some review, the researcher determined the Reprivata CoT solution possessed three advantages over other cybersecurity solutions. First, the Reprivata solution created a secure Community of Trust (CoT), where entities communicated securely and exchanged sensitive data inside the closed private network using embedded collaboration and data sharing applications. Second, the Reprivata solution required the entities using the closed private network to sign Master Agreements that committed them to implementing the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) as their organizational cybersecurity model. As part of its design, the NIST CSF drives the consistent application of business practices for maturing cybersecurity programs and collaborating on mutual cybersecurity issues, which no other cybersecurity standards require. Third, the solution had a Global Threat Intelligence (GTI) component that, in real time and with a technology agnostic stance, monitors and mitigates security threats to the entities’ private networks as well as potential cybersecurity risks inside the CoT network.
During additional discussion with the Reprivata senior management team, the researcher learned they did not understand how to map their solution to the NIST CSF key controls in order to assess its compliance with those standards. Additionally, they did not understand how to effectively demonstrate to potential clients that the solution’s encryption and threat management capabilities could help those clients better understand, respond to, and mitigate their cybersecurity risks.

At the request of Reprivata management, the researcher began to investigate ways to create compliance testing artifacts for the solution and a NISF CSF mapping of the solution in order to illustrate how each component met the NIST CSF requirements for cybersecurity behavior management, risk management, and collaboration between all interconnected parties doing business together over the Internet.

Motivation

As a cybersecurity practitioner and executive for over 25 years, I have found that one of the most challenging things to do is effectively and accurately communicate cybersecurity information to those parties who are not well-versed in the field. In particular, cybersecurity risks and impacts are very difficult to communicate because those issues can be very technical or theoretical and need to be “translated” into a vocabulary that can be better understood by people with non-cyber backgrounds.

This communication problem came into sharp focus when I began assisting Reprivata, a startup cybersecurity risk management solution company, with their go-to-market strategy. This required me to re-think how to communicate what is a very technical and complex technology solution into more conceptual terms that could show how the solution actually worked without
confusing them by utilizing some of the potentially arcane and confusing language used by cybersecurity practitioners.

To accomplish this, I began to appraise how to inform the Reprivata stakeholders and potential customers by creating a design artifact in the form of a conceptual model, which showed the solution in pictorial format. This artifact was created to show stakeholders how the solution could work across an organization to improve its security controls posture. Once the conceptual model was created and its initial assessment had been performed, I began working on a compliance matrix, which broke the solution down into its primary security controls, to identify how well the solution complied with the NIST CSF. The matrix also gave an overview of how the solution could help mature the security control posture.

This research article is based on the Elaborated Action Design Research (eADR) process model developed or described by Mullarkey and Hevner (2018). The diagnosis phase of this research project included exploratory personnel interviews and problem analyses performed with the Reprivata management team. Then, the findings on the design and product strategy of Reprivata’s cybersecurity solution were detailed.

The findings resulted in several artifacts in the form of a business case discussing Reprivata’s current business issues and pending decisions as well as technical overviews of Reprivata’s cybersecurity collaboration solution software. Additionally, further analyses of the cybersecurity problem spaces affecting Reprivata’s product strategy were performed to learn how well the Reprivata CoT solution addressed some of the more prevalent issues around understanding cybersecurity risks in the context of an organization’s technology risk posture.

Once created, the first set of artifacts that were created during the writing of the Reprivata case study was evaluated by the Reprivata management team, updated based on their comments
and recommendations, and incorporated into the overall cybersecurity solution design, architecture, and productization strategy presentations. Then, these artifacts were used as the basis for the next ADR phase.

Reprivata and its clients cited the informing aspects of applying a more cybersecurity-focused vocabulary and taxonomy to the company’s product strategy as a key enhancement that would enable a better understanding of the cyber risks identified and reported by the Reprivata cybersecurity solution, which is consistent with findings in the academic literature reviewed for this article (Elnagdy, Qiu, & Gai, 2016).

The motivation for these research activities is to develop additional suitable artifacts to further improve the solution’s cybersecurity risk management capabilities. After additional conversations and further documentation reviews with Reprivata’s management team, the next artifacts to be created would include a conceptual model that illustrated the interrelationships of the solution’s software components, its operational processes, and the technical cybersecurity standards applied to the solution. Also, to demonstrate to clients how the solution, at the modular level, complied with the NIST CSF standard that Reprivata had adopted when developing the solution, a mapping of the Reprivata CoT solution architecture to provide a visual representation of its components and how they work together was required. These artifacts will be evaluated by Reprivata management, technical Subject Matter Experts (SMEs) in the cybersecurity field, and Reprivata’s potential clients to determine further product design and strategy enhancement opportunities for the Reprivata cybersecurity solution. The results of the interventions with the cybersecurity SMEs and potential clients will be documented in the next paper of this research project.
The literature review was performed in two phases. The first phase was a survey of the types of research methodologies used in the study of cybersecurity and related risk management topics (see Table 1). These articles also included an overview of legal and ethical issues that have arisen in prior research that, if not handled appropriately, could impact current and future cybersecurity research projects. From this literature review, it was determined that Action Design Research (ADR) has been used in previous cybersecurity research in the area of how to effectively communicate information about cybersecurity risks to stakeholders. The Design Science Research (DSR) approach helped guide the development of informing artifacts and other documentation on cyber risks to provide more assistance to cybersecurity risk practitioners and those entities that interact with them to better understand cyber risks as well as their potential impacts on the organization.

**Table 1 – Literature on Research Design Applicable to Cybersecurity Risks**

<table>
<thead>
<tr>
<th>Source</th>
<th>Findings</th>
</tr>
</thead>
</table>
| Burstein, A. J. (2008). Conducting Cybersecurity Research Legally and Ethically. *LEET*, 8, 1-8 | - A variety of federal and state statutes either prohibit activities that would provide cybersecurity researchers with data about real systems and real attackers, or cast such doubt on research activities that investigators modify their programs or conduct them with a sense of uncertainty as to their legality. (Page 1).  
- Though U.S. law does not permit everything that cybersecurity researchers would like to do, relatively few research activities are flatly prohibited. (Page 2).  
- Researchers should consider whether the papers or datasets that they publish could reveal information that could help adversaries attack the researcher's own network (or other friendly networks). (Page 12). |
Table 1 (Continued)

| Da Veiga, A. (2016, July). A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. In *SAI Computing Conference (SAI), 2016* (pp. 1006-1015). IEEE. | • To mitigate cyber risks and minimize cybercrime, cybersecurity is aimed at protecting information resources connected in cyberspace, the information available via cyberspace, and the individual who could fall prey to cyber-attacks. (Page 1007).  
• An information security culture has been defined as the attitudes, assumptions, beliefs, values, and knowledge that employees/stakeholders use to interact with the organization’s systems and procedures at any point in time. (Page 1008).  
• The assessment of the cybersecurity culture level in an organization can be incorporated in existing information security risk management and incident management frameworks to understand the risk from a human perspective. (Page 1014). |
| --- | --- |
• A common set of performance indicators or metrics that can be used as a gold standard for systematically evaluating the effectiveness of national cybersecurity strategies is yet to be developed. (Page 2).  
Latent Dirichlet Allocation (LDA) topic modeling was an effective method for identifying a number of key topics and corresponding words relevant to prior knowledge and extent experiences in cybersecurity and public policy studies. (Page 8).  
• Globally accepted best practices that can be compared with the result of topic modelling and topic labels for cybersecurity are not available at this time. (Page 10). |
• Cybersecurity specialists can manipulate cognitive limitations to overdramatize and oversimplify cybersecurity risks to critical infrastructures. (Page 6).  
• The proposed design science process is a “learning machine,” in which design principles provide a focal point for collaboration between infrastructures, codify specialized knowledge in a teachable form that can be more easily communicated to others, elevate attention from point solutions to higher-impact problems, enable knowledge sharing between different infrastructures, and increase both the rate of learning and the frequency of opportunities for learning. (Page 7).  
• Open source software projects are a high-potential setting for collaboration where critical infrastructure providers can tap into the benefits of high-quality software, and other developers and users benefit from the critical infrastructure providers’ high demands for security and testing. (Page 12). |
In the literature review on the types of cybersecurity research methods, databases such as ABI-Informs, Google Scholar and JSTOR.org were used for those searches. These databases were selected as excellent starting points for the first phase of the literature review, based on the recommendations of the USF librarians and the DBA dissertation committee professors. The search queries concentrated on cybersecurity research methods to find the articles that were ultimately reviewed and cited here.

The queries to these databases found a body of literature on these subjects by both academics and practitioners dating from the 2000s. These are the selected results of the database queries. Further review and summarization of the referenced articles and books are planned to

| Mullarkey, M. T., & Hevner, A. R. (2018). An elaborated action design research process model. *European Journal of Information Systems*, 1-15. | • Action Design Research (ADR) is used effectively in many research projects and, because of its ever-expanding applications, the ADR concepts and process model continue to grow and evolve to meet the demands of new and challenging environments. (Page 1).  
• A key addition to the activities in the ADR intervention cycle is the inclusion of the Artifact Creation activity. This activity highlights the essential artifact build activities that are central to the Design Science Research (DSR) process. (Page 15).  
• Practitioners from multiple application areas (such as healthcare, education, government, and others) can be brought together in common ADR projects by use of a shared process model and produce innovative artifacts of value across disciplines. (Page 16). |
• Ontologies and the associated inference mechanisms permit us to reason about connections between diverse domains and contexts that are pertinent for the general threat picture, and to highlight the effects and ramifications of the mitigation strategies considered. (Page 1).  
• Ontologies are crucial tools for understanding the threat space for new technology space, for increasing security experts’ situational awareness, and, ultimately, as decision-support tools for rapid development of mitigation strategies. (Page 1). |

| In the literature review on the types of cybersecurity research methods, databases such as ABI-Informs, Google Scholar and JSTOR.org were used for those searches. These databases were selected as excellent starting points for the first phase of the literature review, based on the recommendations of the USF librarians and the DBA dissertation committee professors. The search queries concentrated on cybersecurity research methods to find the articles that were ultimately reviewed and cited here. The queries to these databases found a body of literature on these subjects by both academics and practitioners dating from the 2000s. These are the selected results of the database queries. Further review and summarization of the referenced articles and books are planned to... |
refine future queries as part of the ongoing research. Theses searches were completed between
June 28, 2018 and June 30, 2018.

The second phase of the literature review was focused on surveying selected articles that
provided insights on the ways cybersecurity risks were measured and how those measurements
were evaluated and understood by stakeholders (see Table 2). From these articles, consistent
findings were identified indicating the cybersecurity field has challenges informing internal
stakeholders, external stakeholders, and cybersecurity practitioners on the types of cyber risks
being faced. As the numbers and types of cyber threats and risks continue to increase, the ability
to measure their impacts accurately will lag, which will limit the ability to inform cybersecurity
practitioners. There are significant opportunities abound for cybersecurity researchers to help
create better risk informing measurement and evaluation solutions for this problem.

Table 2 – Literature on Understanding and Measuring Cybersecurity Risks

<table>
<thead>
<tr>
<th>Source</th>
<th>Findings</th>
</tr>
</thead>
</table>
| Butler, A. (2012). When cyber weapons end up on private networks: third amendment implications for cybersecurity policy. *Am. UL Rev.*, 62, 1203. | • Regardless of the sources of many cyber-attacks, the sophisticated malware programs utilized reveal the capacities to capture credentials, communications, audio, video, and a wide range of other sensitive data from a broad range of devices and networks. (Page 1214).
• The Third Amendment to the Constitution has prohibitions that govern any military intrusions onto private property, such as situations where military cyber operations can affect private computers and networks, including innocent third-party systems. (Page 1227).
• When framed as a right to exclude the military from private property, it is clear that computers, networks, and other systems fall within the scope of the Third Amendment. (Page 1230).
So far, no United States government policy efforts have adequately addressed the civil liberties impact of cyber operations. (Page 1234). |
<table>
<thead>
<tr>
<th>Source</th>
<th>Summary</th>
</tr>
</thead>
</table>
| **Contreras, J. L., DeNardis, L., & Teplinsky, M. (2012).** Mapping today's cybersecurity landscape. *Am. UL Rev.*, 62, 1113. | • Cyber threats overtook terrorism as the number one global threat to America, according to the 2013 global threat assessment performed by the United States intelligence community. (Page 1114).  
• Interoperability is critical in communications and national infrastructure, including the national power grid and the medical and financial establishments. The result of the tens of thousands of technology standards in use is a world that is massively interconnected. (Page 1117).  
• The security and stability of the Internet depend on the preservation of three Internet characteristics:  
  - Permissionless innovation  
  - Open access  
  - Collaboration (Page 1121).  
• Several practical steps that firms can take to protect themselves include:  
  - Implement best practices in cybersecurity risk management  
  - Engage senior leadership  
  - Encourage a culture of cybersecurity through education and implementation of policies to control cyber risk  
• The cause effect relationships between cyber incidents and cyber risks are hard to be accurately defined, because most situations represent a multi-to-multi relation and very rarely do one-to-one relations exist. (Page 297).  
• The vital issue is finding out the methods of creating taxonomy of cybersecurity, which is the fundamental of organizing cyber incidents and relevant technical issues in a group-based manner. (Page 298). |
| **Epstein, R. A., & Brown, T. P. (2008).** Cybersecurity in the Payment Card Industry. *The University of Chicago Law Review*, 75(1), 203-223. | • The object of choosing the right rules for risk allocation was to minimize the net costs of theft, as measured by the losses from the theft, less the costs of prevention, including the costs of running the system. (Page 207).  
• When a third party is the source of the stolen information, consumers are unlikely to know the precise source of a breach. (Page 213).  
• Breaches have occurred most often, almost 50 percent of the time, in the government and education sectors, but the most records have been stolen from retailers and processors of financial data. (Page 213). |
• Research in both government and commercial sectors reveal that although the proportion of insider events is declining, the financial impact and operating losses due to insider intrusions are increasing. (Page 61).
• A complete and effective insider threat mitigation strategy must take into account human motivations and behaviors along with organizational factors such as policies, hiring, and training practices, and the technical vulnerabilities and best practices for prevention or early detection of unauthorized insider activity or access. (Page 63). |
| --- | --- |
| Jones, W., & Gallo, A. (2007). A Process-Based Approach to Handling Risks. *IT Professional, 9*(2). | • The risk management process begins with the development of a policy, including a clear definition of an acceptable risk tolerance. (Page 11).
• A comprehensive risk management approach to cybersecurity requires the early identification of threats and vulnerabilities most likely to occur, the ability to qualify and quantify the potential harm to the agency, and the development and implementation of appropriate mitigation steps to achieve an acceptable risk level. (Page 13).
• The process model for continuously managing risk is essentially equivalent, whether considering a program or project with discrete start and end dates and well-defined deliverables or for an ongoing service or infrastructure support activity. (Page 64). |
| Loukaka, A., & Rahman, S. (2017). Discovering new cyber protection approaches from a security professional prospective. *Int. J. Comput. Netw. Commun. (IJCNC), 9*(4). | • In order to detect attacks more accurately and to build on a robust detection system, it is imperative to apply other areas that include new technologies, big data, attacker philosophies and the normal user activities. (Page 14).
Today’s network infrastructures are so complex that it is categorically impossible to adequately distinguish plausible valid alerts. (Page 16).
Current research in cyber protection shows that economic impact can be very serious after a cyber-attack or data breach but it also underlines that most organizations reluctance to change, adaptation, and collaboration in addressing potentially serious cybersecurity issues. (Page 21). |
<table>
<thead>
<tr>
<th>Source</th>
<th>Text</th>
</tr>
</thead>
</table>
• The U.S. Department of Homeland Security has developed an assessment methodology called the Cyber Resilience Review (CRR) which helps organizations better understand their role in critical infrastructure protection and provides a lightweight review of how they are managing the capabilities that are crucial for ensuring the cybersecurity and continuity of high-value services during times of stress, when effective management is needed most. (Page 85).  
• Goals in the assurance review are refined into specific goals and sub-goals which are eventually turned into the assessment questions that are asked of organizations under review to determine the extent to which the goals are satisfied. (Page 87). |
| Myron, W., & Muita, K. (2014). Cybersecurity capability maturity models for providers of critical infrastructure. *Technology Innovation Management Review, 4*(10). | • To help cope with the security risks associated with the complexity and interdependencies within various critical infrastructure systems, standards bodies and federal agencies in at least twelve countries or regions of the world have defined criteria for security standards as well as implementation methods. (Page 34).  
• These modern cybersecurity capability maturity models provide the stages for an evolutionary path to developing policies and processes for the security and reporting of cybersecurity readiness of critical infrastructure. (Page 36).  
• The review of the current cybersecurity capability maturity models highlighted that, although many models exist, none are specifically crafted to address the scenario of an operator of multiple interdependent systems and are instead focused on federal infrastructures or specific industry sub-sectors, and are all at a high level. (Page 38). |
• The presentation and format, relevance and specificity of information also become key factors in increasing a user’s trust in a security risk message displayed. (Page 66).  
• Keeping communications about cybersecurity risk simple and minimalistic, assisting users in seeing the potential consequences of security-related decisions, and engaging in some level of customization of the context and content of cybersecurity risk information to specific target audiences are all important factors to ensure effective and informing risk communications to stakeholders and other affected parties. (Page 66). |
<table>
<thead>
<tr>
<th>Source</th>
<th>Citations</th>
<th>Summary</th>
</tr>
</thead>
</table>
| Shane, P. M., & Hunker, J. A. (Eds.). (2013). *Cybersecurity: Shared risks, shared responsibilities*. Carolina Academic Press. | - While the proposed United States cybersecurity framework may well be a reasonable approach to security from the perspective of stakeholders (including citizens) whose security may be breached, we should also note that our government may itself be an active agent in some breaches and attacks. (Page 1).  
- Many of our public laws and legal institutions are under stress because they have not kept pace with technological developments. (Page 2).  
- The pace of events in cyber space moves so quickly that policy enhancements and requirements cannot keep up. (Page 2). |
| Shields, K. (2015). *Cybersecurity: Recognizing the risk and protecting against attacks*. *NC Banking Inst.*, 19, 345. | - Despite regulatory pressure and financial institutions' efforts to protect against security threats, sophisticated cyberattacks against financial institutions occur every day, and the resulting costs have become an increasingly significant part of the business. (Page 348).  
- Even if cybercriminals cannot directly breach a financial institution's network, they may still gain access to the institution's network through the network of a third-party vendor because some of these third parties' security practices are remiss or even nonexistent. (Page 350).  
- Educating employees and consumers on how to distinguish legitimate entities from fraudulent ones is key to protecting against cybersecurity attacks. (Page 366). |
- Currently, no baselines or comprehensive cybersecurity obligations are imposed across the United States critical infrastructure, but regulations do exist for certain sectors, leaving the status quo a complex patchwork of oftentimes ambiguous state and federal regulations overlaying applicable common law doctrines. (Page 310).  
- Despite gaps in the legal framework and the ever-changing cyber threat, courts are increasingly willing to hold both organizations and firms liable for not protecting sensitive information. (Page 312). |
<table>
<thead>
<tr>
<th>Source</th>
<th>Additional Notes</th>
</tr>
</thead>
</table>
| Sommer, P., & Brown, I. (2011). Reducing systemic cybersecurity risk. | - Analysis of cybersecurity issues has been weakened by the lack of agreement on terminology and the use of exaggerated language. (Page 7).  
- The cyber infrastructure, as well as providing a potential vector for propagating and magnifying an original triggering event, may also be the means of mitigating the effects of cyber-attacks and data breaches. (Page 8).  
- One important characteristic of a global shock from cybersecurity events is that responses limited to the level of the nation state are likely to be inadequate; coordinated international activity, with all the associated problems of nation states reaching collaborative agreements and then acting in concert, is what is required to deal with these types of cybersecurity issues. (Page 11). |
- Automated processing of bulk data should be viewed differently than individualized surveillance because the distinction between content and metadata needs to be linked to the purpose of monitoring; and the surveillance requirements, particularly on a large scale, must be buttressed by measures of privacy by design. (Page 401).  
- Cybersecurity threats in particular can be embedded into all layers of a communication, regardless of the distinction between content and metadata. (Page 412).  
- In addition to mechanisms of legal oversight, cybersecurity monitoring programs require the creation of operational accountability processes within intelligence and national security agencies. (Page 424). |
| Trope, R. L. (2012). "There's No App for That": Calibrating Cybersecurity Safeguards and Disclosures. *The Business Lawyer, 183*-195. | - For years, the risks cyber threats remained obscure because companies preferred not to disclose that they had been breached and damaged. (Page 183).  
- Cybersecurity can longer be focused exclusively on protecting the enterprise and its assets and reputation, but, in light of several highly publicized data breaches, cybersecurity measures need to be broadened if an enterprise is to be in a position to defend its response cyber-attack. (Page 194).  
- The longer it takes an enterprise to detect an attack that results in damage to a customer or a third party with whom the enterprise has a formal commercial or corporate relationship, and the longer it takes the enterprise such circumstances to interdict and remediate the attack, the harder pressed the enterprise and its counsel will be to demonstrate to a court that an enterprise's actions did not fall short of reasonably commercial standards of fair dealing. (Page 194). |
In the literature review on the communication of cybersecurity risks and impacts to stakeholders, databases such as ABI-Informs, Google Scholar and JSTOR.org were used for those searches. These databases were selected as excellent starting points for the second phase of the literature review, based on the recommendations of the USF librarians and the DBA dissertation committee professors. The search queries concentrated on communicating, understanding, and measuring cybersecurity risks and impacts to find the articles that were ultimately reviewed and cited here.

The queries to these databases found a body of literature on these subjects by both academics and practitioners dating from the 2000s. These are the selected results of the database queries. Further review and summarization of the referenced articles and books are planned to refine future queries as part of the ongoing research. These searches were completed between July 1, 2018 and July 3, 2018.

Both phases of the research provided significant insights into the challenges of performing cybersecurity research and the manner in which details on cyber risk are communicated to inform stakeholders effectively. A number of constraints and other challenges can impact an organization’s ability to identify, analyze, and understand cyber risks (see Table 3).

<table>
<thead>
<tr>
<th>Identified Issue</th>
<th>Impact on Informing of Cybersecurity Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal or Regulatory Restrictions</td>
<td>• In Federal and state law, regulations are in place that prevent or severely limit the ability of entities to legally share information about cyber risks.</td>
</tr>
<tr>
<td></td>
<td>• Legal contracts often limit the disclosure of information between entities. This non-disclosure language restricts sharing of information on cyber risks to specific situations (such as a data breach).</td>
</tr>
</tbody>
</table>
Table 3 (Continued)

<table>
<thead>
<tr>
<th>Ethical Constraints</th>
<th>• While cybersecurity practitioners have ethical obligations on the sharing of cyber risk information with other entities with “need to know” requirements, no similar obligations are present between business and their third-party interconnections, such as suppliers or service providers.</th>
</tr>
</thead>
</table>
| Limited Collaboration between Parties                                                | • Many cybersecurity frameworks and standards do not require the collaboration between businesses or other entities on the identification, analysis, and understanding of cyber risks.  
• The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) requires collaboration as part of its maturity model, but the NIST CSF is not widely adopted in the United States at this time.  
• Because the NIST CSF is primarily a United States cybersecurity standard, it is unlikely to be widely embraced outside of the United States. |
| Lack of Common Cybersecurity Risk Vocabulary and Taxonomy                           | • Industries with their own cybersecurity standards (such as the Payment Card and Energy industries) have subtle, and sometimes significant, differences in definitions and usages of cybersecurity terms, which can make the understanding of cyber risks more difficult when risk information is shared. |
| Limited Mechanisms for Securely Share Cybersecurity Risk Information                 | • Very few cyber risk collaboration and sharing solutions are in wide use that enable entities (particularly those in different organizations) to securely share cybersecurity risk information that impacts all the related entities. |

As shown in Table 3, cybersecurity risk management issues clearly require further research and evaluation in order to determine long term pragmatic ways to address them so that cybersecurity research can be performed with fewer obstacles to such assessments. Continued studies are necessary so researchers can effectively communicate opportunities for advancing cybersecurity risk management processes and procedure. As cyber risk management requirements on businesses and government agencies become more regulated and stringent, the needs of stakeholders to share risk information and assist each other in understanding the implications of those risks on the ways the stakeholders do business together become a necessity.
The researcher compared the capabilities of the Reprivata cybersecurity risk management solution to some of the risk-informing challenges as noted in Table 3. In three areas, the Reprivata CoT solution provides users with ways to meet several issues noted. The Reprivata CoT solution has secure voice, video, and texting capabilities to facilitate collaboration and information sharing on cyber risks between organizations. These functions were developed using encryption algorithms used by the United States.

The Reprivata solution was designed to meet the NIST CSF standards. These standards require external participation and collaboration in order for organizations that use the standard to comply with its requirements. This design intent is further elaborated in the artifact created to assess the solution’s compliance with the NIST CSF guideline (see Artifact 2 in Appendix A).

The Reprivata solution has legal contracts (in the form of Master Agreements) that define the rules of engagement and collaboration obligations for the entities that use the solution. This enables the entities to have a well-defined process for helping all the stakeholders to learn more about cyber risks through interactions and exchanges with other organizations with which they do business. Over time, these collaborations will raise the cyber threat awareness for all entities in addition to strengthening and maturing their cyber risk programs from the informing process. Recommendations on ways to improve the Master Agreements to include additional and more compliance-oriented language for the CoT users are provided in Artifact 3 in Appendix A.

This literature review has demonstrated that research on effective methods for informing on cybersecurity risks is an emerging area with many opportunities for investigation. The numbers and types of cybersecurity threats are rapidly expanding; therefore, the need for better cyber risk-informing solutions for all types of stakeholders is of paramount importance. Additional research is required to identify ways to minimize the differences that exist in the
current approaches to cybersecurity risk management (Contreras, 2012). As mentioned above, a
trend was found showing that cybersecurity and risk management solutions are lagging in their
abilities to help stakeholders identify, analyze, and understand cyber risks (Trope, 2012).

A compelling area of research referenced in the current literature on cyber security risk
involves the use of data analytics to help measure key cyber risk performance measurements and
indicators (Tene, 2014). This approach could bring a common data-drive language to the field,
where cyber risks to organizations could be quantified as financial and operational impacts
(Sommer & Brown, 2011). Additional investigation, through the use of statistical techniques,
could better evaluate when, where, and how these cyber risks are found and more effectively
communicate this information to all affected stakeholders (Loukaka & Rahman, 2017). Such
communication and collaboration, governed by the appropriate legal language, will create more
risk-informed cybersecurity programs for many entities that are currently less prepared or mature
now and cannot effectively address the expanding challenges from cyber risks and threats (Shane
& Hunker, 2013).
Research Method

**Figure 1 – Action Design Research Methodology for Reprivata Community of Trust**

The Action Design Research (ADR) methodology was chosen for this research project for several reasons. First, ADR had been used successfully in other cybersecurity research efforts (Muegge & Craigen, 2015). Similar academic articles reviewed drew on design science research done by Dr. Alan Hevner, a leading international expert on ADR methods who is a professor at the University of South Florida. Second, the work relationship between the researcher and the target company (Reprivata) provided a unique opportunity for the analysis, design, creation, and evaluation of specific ADR artifacts that could assist Reprivata’s management team to better articulate the informing capabilities of Reprivata’s cybersecurity risk management solution,
especially in relationship to cybersecurity risks identified by the application. Third, the proximity of the Florida Center for Cybersecurity (Cyber Florida) on the University of South Florida campus gave the researcher the ability to have cybersecurity Subject Matter Experts (SMEs) independently evaluate and comment on the ADR artifacts to determine how those items might inform a broader audience in the cybersecurity field. Fourth, the ADR approach enabled the researcher to engage with Reprivata’s partners and potential customers and gauge how effective the ADR artifacts were in helping them understand the cybersecurity risks identified by Reprivata’s security control mechanisms. Finally, the ADR approach facilitated an in-depth evaluation of Reprivata’s security controls in relationship the NIST CSF standards, which identified how the Reprivata cybersecurity risk management solution met that standard or enabled other security controls external to the solution (such as policies, procedures, and security software) to become compliant with the NIST CSF.

The ADR approach utilized in this research project was drawn from a 2018 article by Dr. Matthew Mullarkey and Dr. Alan Hevner (Mullarkey & Hevner, 2018). ADR concepts and process modelling are growing in various research areas and have been found as very effective ways of describing a variety of technology environments. The addition of artifact creation activities as part of ADR intervention activities highlights the essential artifact build and evaluation activities that are key to Design Science Research (DSR). Researchers and practitioners from multiple application areas, such as healthcare, education, government, and others, can be brought together in common ADR projects by use of a shared process model and then produce inventive and original artifacts of value across research disciplines. (Mullarkey & Hevner, 2018).
The researcher first engaged with Reprivata in January 2018. After discussions with the Reprivata management team, the researcher executed a Non-Disclosure Agreement (NDA) which included language that allowed the researcher to perform an ADR project on the company and its cybersecurity solution. The researcher then interviewed the Reprivata team to learn more about the company and its go-to-market strategy. They then provided access to the company’s technical documentation of its software, its current productization strategy, customer presentations, and the security certification assessment report on the software solution from the Underwriters’ Laboratory (UL), and the company’s Master Agreements used to set up the responsibilities and rules of engagement for users of the Reprivata cybersecurity risk management solution.

The Reprivata management requested a review the company’s cybersecurity risk management solution against the NIST CSF standards to determine the solution’s level of compliance with that security framework. Based on the documentation reviewed, the researcher determined there were gaps in the way Reprivata had implemented the key security controls in the solution. In particular, the researcher found that no current design documentation or model of the solution could be mapped directly against the NIST CSF standard. Using action design research principles, an artifact was designed, evaluated, and enhanced. This item was a conceptual model of the Reprivata cybersecurity risk management solution (see Figure 4).

Once the artifact was created, it was shared with Reprivata’s management team. Overall, they agreed that the artifact more clearly articulated the key security controls of the solution and its compliance with the NIST CSF. The artifact was then incorporated to the Reprivata product presentations that were given to potential customers. From the types of comments received during the customer meetings, the customers stated that, while the recently developed artifact
was very helpful in communicating how the Reprivata CoT solution mapped to the NIST CSF key controls, it did not discuss which of the NIST CSF security controls were not implemented in the solution, which of those controls were covered by external processes or parties, and how that information could be communicated to help potential customers and business partners understand cyber risks related to those controls. These comments were captured for inclusion in the next iteration of artifacts about the Reprivata CoT solution. The conversations were captured using unstructured interviews and the themes were coded using open and axial coding techniques. As outlined in Figure 1, the design artifact requirements and evaluation criteria were created using the Action Design Research methodology for each iteration of the design artifacts.

In the discussions that followed, the team asked if the artifacts could be assessed by Subject Matter Experts (SMEs) in the cybersecurity field so the team could get more feedback on the solution to see if it could be enhanced to accelerate its productization and go-to-market strategies. The researcher contacted the Cyber Florida team and asked for a meeting between the Cyber Florida senior staff and the Reprivata management team. The intervention session was scheduled for March 2018. During the meeting, the Reprivata and Cyber Florida teams discussed the details of the cybersecurity risk management solution in addition to a product strategy presentation. The Cyber Florida team members asked for clarification on how the Reprivata CoT solution would be deployed. The Cyber Florida team provided recommendations on how to more clearly articulate the capabilities of the solution and also suggested several potential use cases. At the close of the meeting, the two organizations agreed to a second meeting to review the enhanced solution and its informing capabilities to enable better understanding of cyber risks.

From Cyber Florida’s recommendations, the researcher began to create a more detailed control mapping of the Reprivata cybersecurity risk management solution to the NIST CSF. This
change was necessary to review and map all the new key security controls that were included in version 1.1 of the framework that was published in April 2018. The Cyber Florida suggestions also required a review of Reprivata’s Master Agreements to ensure that any appropriate key security control language was added to the agreements and provide better compliance with the updated NIST CSF.

The researcher then created an expanded NIST CSF version 1.1 assessment matrix. This new matrix mapped the key security controls that were included in the design of the Reprivata CoT solution, and also identified those that were not integral to the solution’s design but could be enabled by controls already integrated into the solution. Additionally, the Master Agreements were assessed in more detail to identify opportunities for improvement and to make recommendations regarding the proposed changes to the legal language in the documents so they align to the newest version of the NIST CSF.

After the newest artifacts were developed, they were shared with Reprivata’s management team. In their comments, the Reprivata team agreed the artifacts would help them more clearly inform their customers on the NIST CSF compliance of the solution as well as improve the definition of user responsibilities and rules of engagement in the Master Agreements.

Before sharing these new artifacts with potential customers, the Reprivata team then requested another meeting with Cyber Florida senior staff to get more of their insights on how to better position the solution so it had broader appeal in the cybersecurity risk management market. That intervention with Cyber Florida was held in August 2018 and documented in the detailed interventions article that is the third part of this research project.
Description of First Artifact Created for the Reprivata CoT Solution

Reprivata Solution Conceptual Model

The first key artifacts discussed below were part of the initial design phase of this research project. Each artifact addresses an aspect of the cyber risk informing capabilities of the Reprivata cybersecurity risk management solution.

The Reprivata Community of Trust (CoT) Conceptual Model (see Figure 2) was developed to articulate the interactions of elements that influence successful cybersecurity CoT implementations using the Reprivata cybersecurity risk management solution. These elements help determine and, in some cases, manage the resources within these projects as the part of the overarching corporate business strategy which determines the cyber risk posture, and how that posture can be managed and measured. These are two distinct groups of elements: one that is composed of the cybersecurity frameworks and legal documents that provide structure to the CoT, and one that constitutes the Internal and External Stakeholders of the CoT.

Figure 2 – Reprivata Community of Trust Conceptual Model
Reprivata selected the NIST CSF as part of their design strategy for two reasons. First, it is a comprehensive set of cybersecurity control requirements based on 23 control categories across 5 cybersecurity functional areas (see Table 4).

Table 4 – NIST CSF Security Functions and Control Categories [from NIST CSF v1.1, 2018]

<table>
<thead>
<tr>
<th>Functions</th>
<th>Categories</th>
</tr>
</thead>
</table>
| Identify (ID) | Asset Management (AM)  
Business Environment (BE)  
Governance (GV)  
Risk Assessment (RA)  
Risk Management Strategy (RM)  
Supply Chain Risk Management (SC) |
| Protect (PR)       | Identity Management, Authentication and Access Control (AC)  
Awareness and Training (AT)  
Data Security (DS)  
Information Protection Processes and Procedures (IP)  
Maintenance (MA)  
Protection Technologies (PT) |
| Detect (DT)        | Anomalies and Events (AE)  
Security Continuous Monitoring (CM)  
Detection Processes |
| Respond (RS)       | Response Planning (RP)  
Communications (CO)  
Analysis (AN)  
Mitigation (MI)  
Improvements (IM) |
| Recover (RC)       | Recovery Planning (RP)  
Improvements (IM)  
Communications (CO) |

As such, the CSF offers a comprehensive framework on which companies can build their cybersecurity programs. Second, the CSF includes a maturity model (see Table 5) that gives companies ways to determine how they are performing as they implement the CSF security controls.
Table 5 – NIST CSF Maturity Tiers [from NIST CSF v1.1, 2018]

<table>
<thead>
<tr>
<th>Maturity Tier</th>
<th>Definition and Characteristics</th>
</tr>
</thead>
</table>
| 1. Partial    | **Risk Management Process** – Organizational cybersecurity risk management practices are not formalized, and risk is managed in an *ad hoc* and sometimes reactive manner. Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements.  
**Integrated Risk Management Program** – Limited awareness of cybersecurity risk at the organizational level is exists. The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources. The organization may not have processes that enable cybersecurity information to be shared within the organization.  
**External Participation** – The organization does not understand its role in the larger ecosystem with respect to either its dependencies or dependents. The organization does not collaborate with or receive information (e.g., threat intelligence, best practices, technologies) from other entities (e.g., buyers, suppliers, dependencies, dependents, ISAOs, researchers, governments), nor does it share information. The organization is generally unaware of the cyber supply chain risks of the products and services it provides and that it uses. |
| 2. Risk Informed | **Risk Management Process** – Risk management practices are approved by management but may not be established as organizational-wide policy. Prioritization of cybersecurity activities and protection needs is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.  
**Integrated Risk Management Program** – An awareness of cybersecurity risk at the organizational level is acknowledged, but an organization-wide approach to managing cybersecurity risk has not been established. Cybersecurity information is shared within the organization on an informal basis. Consideration of cybersecurity in organizational objectives and programs may occur at some but not all levels of the organization. Cyber risk assessment of organizational and external assets occur, but is not typically repeatable or reoccurring.  
**External Participation** – Generally, the organization understands its role in the larger ecosystem with respect to either its own dependencies or dependents, but not both. The organization collaborates with and receives some information from other entities and generates some of its own information, but may not share information with others. Additionally, the organization is aware of the cyber supply chain risks associated with the products and services it provides and uses, but does not act consistently or formally upon those risks. |
Table 5 (Continued)

<table>
<thead>
<tr>
<th></th>
<th>Repeatability</th>
<th>Adaptive</th>
</tr>
</thead>
</table>
| 3. | **Risk Management Process** – The organization’s risk management practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape.  
**Integrated Risk Management Program** – An organization-wide approach to manage cybersecurity risk is in place. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities. The organization consistently and accurately monitors cybersecurity risk of organizational assets. Senior cybersecurity and non-cybersecurity executives communicate regularly regarding cybersecurity risk. Senior executives ensure consideration of cybersecurity through all lines of operation in the organization.  
**External Participation** – The organization understands its role, dependencies, and dependents in the larger ecosystem and may contribute to the community’s broader understanding of risks. It collaborates with and receives information from other entities regularly that complements internally generated information, and shares information with other entities. The organization is aware of the cyber supply chain risks associated with the products and services it provides and that it uses. Additionally, it usually acts formally upon those risks, including mechanisms such as written agreements to communicate baseline requirements, governance structures (e.g., risk councils), and policy implementation and monitoring. | **Risk Management Process** – The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators. Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing threat and technology landscape and responds in a timely and effective manner to evolving, sophisticated threats.  
**Integrated Risk Management Program** – An organization-wide approach to managing cybersecurity risk exists that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. The relationship between cybersecurity risk and organizational objectives is clearly understood and considered when making decisions. Senior executives monitor cybersecurity risk in the same context as financial risk and other organizational risks. The organizational budget is based on an understanding of the current and predicted risk environment and risk tolerance. Business units implement executive vision and analyze system-level risks in the context of the organizational risk tolerances. |
As part of the creation of the Conceptual Model, the Reprivata solution design documents were reviewed and compared against the NIST CSF version 1.0, which was released in 2014. The initial Conceptual Model was designed to demonstrate how the Reprivata cybersecurity risk management solution’s overall design and component integration showed its linkage to NISF CSF. The Conceptual Model was evaluated by the Reprivata senior management team and provided the researcher with a number of comments and recommendations, especially of the security controls implemented in the solution regarding interconnected third parties. As part of this effort, the researcher reviewed articles focused on the adoption of the NIST CSF framework to support the updates to the Conceptual Model (Dedeke, 2017).

When the NIST CSF version 1.1 was released in April 2018, the Conceptual Model was reviewed again to ensure that any new and enhanced security control elements were included. Additional literature was surveyed on the integration of the updated and enhanced security
controls (Chaput, 2017). This comparison of the initial and revised standards sought to ensure that the Conceptual Model accurately conveyed how those security controls complemented the initial design and presentation.

In the Conceptual Model, the CoT Risk Management Strategy element maps directly to the Reprivata solution. This element defines the cybersecurity control requirements that the CoT members follow. In the case of Reprivata, the company selected the NIST CSF framework in 2014 as they began development on their cybersecurity risk management solution. When the NIST CSF was updated in 2018 to version 1.1, Reprivata used that event as rationale to reevaluate the solution’s compliance with the new and enhanced standards.

For a more comprehensive description of the Reprivata Community of Trust (CoT) Conceptual Model, please refer to Artifact 1 in Appendix A.

Evaluation of the First Artifact Created for the Reprivata CoT Solution

Due to reiterative design and evaluation process that is inherent to ADR, the artifact was assessed multiple times by the Reprivata management team prior to the artifact’s adoption. This process provided the team with a number of opportunities ask questions about cybersecurity control risks, learn more about the vocabulary and taxonomy used by cybersecurity professionals like the researcher, and begin to have a better understanding of how to better communicate the Reprivata CoT solution’s cyber risk management capabilities. Because the Reprivata management team was actively involved in the artifact design and evaluation sessions, they accepted them more readily and were better able to communicate the benefits of the artifacts.

During the evaluation of the Conceptual Model for the Reprivata cybersecurity risk management solution, one of the techniques utilized in this process was to compare documented security controls with the NIST CSF version 1.0 standards. This comparison was done by
creating a matrix of the design elements that make up the Conceptual Model of the solution with the NIST CSF Security Functions and Control Categories from version 1.0 of the standards. This matrix was one of the key informing activities in the minds of Repriviata’s management team because, for the first time, they could better understand that their original security control design intent was actually integrated in the solution. As part of the next ADR design phase, Reprivata’s management asked for a complete NIST CSF controls assessment for version 1.1, which had recently been released. This request led to the creation of the full NIST CSF version 1.1 compliance assessment (see Artifact 2 in Appendix A), which was completed in August 2018.

An example of the informing abilities of the Conceptual came in a meeting with the Department of Homeland Security (DHS). The DHS security team had been seeking a secure communication solution to enable collaboration with other Federal agencies like the Department of Justice and the Federal Bureau of Investigation (FBI). The Reprivata team used the conceptual model artifact to show how the security control functions in the cybersecurity risk management solution were consistent to the DHS risk management strategy and mapped to its primary goals and objectives. This meeting led to the creation of a use case for that collaborative communication closed network so the DHS team could assess how the Reprivata solution could meet those operational and security requirements for such inter-agency cooperation initiatives.

**Description of Second Set of Artifacts Created for the Reprivata CoT Solution**

The following description of the second key artifacts are part of the second design phase of this research project. Each one was created in response to the Reprivata management team’s request to better articulate the solution’s mapping to the NIST CSF version 1.1 standards so this information could be used to inform potential customers on the solution’s level of compliance to that standard.
Reprivata Solution NIST CSF Assessment

The evaluation of the Reprivata solution’s technical controls was important for the Reprivata team and potential customers. While the solution had been certified under the UL 2900 cybersecurity standards in 2016, it had not been assessed for compliance with the NIST CSF criteria or any other cybersecurity control frameworks. Two separate NIST CSF compliance assessments were performed during this research project: first, using NIST CSF version 1.0 and then with NIST CSF version 1.1. The artifact presented in this article is the results of the NIST CSF version 1.1 assessment of the Reprivata solution.

Table 6 – NIST CSF Assessment and Findings for the Reprivata Community of Trust (CoT) Cybersecurity Risk Management Solution

<table>
<thead>
<tr>
<th>NIST CSF Functional Area</th>
<th>Reprivata CoT Solution Compliant with Key Controls</th>
<th>Technology Controls</th>
<th>Enabling Controls</th>
<th>Master Agreement Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify</td>
<td>15 out of 29 key controls</td>
<td>5</td>
<td>14</td>
<td>10</td>
</tr>
<tr>
<td>Protect</td>
<td>18 out of 39 key controls</td>
<td>12</td>
<td>21</td>
<td>6</td>
</tr>
<tr>
<td>Detect</td>
<td>15 out of 18 key controls</td>
<td>11</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Respond</td>
<td>13 out of 15 key controls</td>
<td>3</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>Recover</td>
<td>4 out of 6 key controls</td>
<td>0</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>65 out of 107 key controls</strong></td>
<td><strong>31</strong></td>
<td><strong>42</strong></td>
<td><strong>34</strong></td>
</tr>
</tbody>
</table>

As part of the original design intent, the capabilities of the Reprivata Community of Trust (CoT) cybersecurity risk management solution controls were based on and implemented to comply with the initial version of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) version 1.0, which was published in 2014. This control mapping analysis reviews the Reprivata solution’s compliance to the NIST CSF version 1.1, which was released in April 2018.
As stated in Section 6, the NIST CSF version 1.1 controls assessment matrix (see Table 6) was created at the request of Reprivata’s management team to determine how many of the key security controls were integrated into the cybersecurity risk management solution. The matrix is the summary of the assessment of the 107 key security controls across the 5 functional areas that are included in the NIST CSF standard. The complete assessment provided guidance to the Reprivata team on what types of control mechanism (such as policies, process, procedures, tools, etc.) that would be required for the specific security control in the Reprivata CoT solution to be deemed compliant with the key security control. The assessment also determined which of the NIST CSF key security controls were either not applicable or not integral to the security capabilities of the Reprivata CoT solution.

The technology security controls in the Reprivata solution were found to directly map to 31 of the NIST CSF key controls, with 22 of those controls covering compliance requirements for the Protect functional area (which includes Identity Management, Remote Access, and Encryption controls) and the Detect functional area (which includes Threat Monitoring and Mitigation controls). This control coverage was important to note because the collaborative capabilities of the Reprivata CoT solution heavily leverage the implementation of those Protect and Detect security controls. The nine NIST CSF key controls that the solution did not map to were related to the implementation of policies and procedures, such as Physical Security, Awareness and Training, and Maintenance. While the Reprivata solution’s technology and cybersecurity controls do not directly implement those policies and procedures, use of the solution for collaborating on how to develop and implement such controls can enable their deployment throughout the organization.
Enabling controls, which are ones that can support or assist in the implementation of other related controls (such as Access Controls, Physical Security, etc.) were also evaluated. In this part of the assessment, the 42 such controls (like policies, practices, procedures, and processes) that are external to the Reprivata technology controls were evaluated to determine what potential use cases would facilitate implementation of the enabling controls. This appraisal helped determine that Reprivata’s technology controls could support those controls that are more process-oriented. The findings indicated that the collaboration, encryption, and threat management capabilities of the solution could provide positive effects that could assist in enabling these types of policies and procedures.

The review of the 34 key controls that map the Reprivata’s Master Agreements was performed and specific recommendations were made for enhancing those agreements. With the recent update of the NIST CSF standard to version 1.1, it is necessary to ensure the legal language is consistent with the security and compliance requirements for the CoT users to ensure accountability to and fulfilment of their contractual obligations.

As part of future design and enhancement of artifacts, the software control mapping will be included in a comprehensive Encrypted Collaboration Software Architecture. This will include more details on the NIST CSF key controls and the specific security mechanisms that are implemented in the Encrypted Collaboration Software.

Reprivata Solution Recommendations for Enhancing Master Agreements

Similar types of assessments were performed to determine which of the NIST CSF controls might be included as legal language in the Reprivata Master Agreements. The specific recommendations on the verbiage to be included in the Master Agreements were documented as a way for Reprivata’s management team to determine where NIST CSF security-related verbiage
could more effectively communicate CoT compliance and collaboration requirements when the agreement was executed by users. This language is particularly critical because it establishes the rules of engagement on how CoT users work together and share critical security and business information when using the Reprivata cybersecurity risk management solution.

Table 7 – Recommendations for Enhancement of Reprivata Master Agreements for Implementing Community of Trust (CoT) Cybersecurity Risk Management Solution

<table>
<thead>
<tr>
<th>NIST CSF Key Control - Identity (ID)</th>
<th>Rationale for inclusion in Master Agreements</th>
</tr>
</thead>
<tbody>
<tr>
<td>• ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.</td>
<td>• Documenting the cybersecurity roles and responsibilities of internal stakeholders and third parties such as suppliers and business partners enables the CoT owner establish access control, incident response reporting, user collaboration, and data sharing processes to meet the needs of the CoT as a whole.</td>
</tr>
<tr>
<td>• ID.BE-1: The organization’s role in the supply chain is identified and communicated.</td>
<td>• The cybersecurity roles for event identification for the organization and its third parties like suppliers and partners that are CoT users should be legally defined in writing to ensure all obligations are understood.</td>
</tr>
<tr>
<td>• ID.GV-1: Organizational cybersecurity policy is established and communicated.</td>
<td>• Compliance to cybersecurity policies by stakeholders should be specific and with assessment and reporting requirements for all CoT users.</td>
</tr>
<tr>
<td>• ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners.</td>
<td>• Documentation of cybersecurity roles for all internal and external stakeholders should be documented and mutual collaboration and data sharing responsibilities outlined in writing for all CoT users.</td>
</tr>
<tr>
<td>• ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.</td>
<td>• Legal and regulatory compliance cybersecurity requirements should be clearly documented for all CoT users.</td>
</tr>
<tr>
<td>• ID.RA-6: Risk responses are identified and prioritized.</td>
<td>• Risk management collaboration requirements for all CoT users should be clearly defined and stakeholder obligations for risk review are documented.</td>
</tr>
<tr>
<td>• ID.SC-2: Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process.</td>
<td>• Risk management and review obligations for third parties should be legally binding when collaborating in the CoT.</td>
</tr>
</tbody>
</table>
Table 7 (Continued)

| ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization’s cybersecurity program and Cyber Supply Chain Risk Management Plan. | Third party contracts should include provisions for measuring and managing cybersecurity risks and implementing cybersecurity controls for controlling related risks. |
| ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations. | Cybersecurity audit and assessment provisions should be clearly documented and assessment reporting requirements specified. |
| ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers. | Cybersecurity recovery and response plans should be required of all CoT users. |

The complete NIST CSF Compliance Assessment and Findings for the Reprivata Community of Trust (CoT) cybersecurity risk management solution can be found in Artifact 2 in Appendix A.

NIST CSF Functional Area – Identify (ID) Controls Language to Include:

The report on recommendations for enhancement of the Reprivata Master Agreements was requested by Reprivata’s management team as a result of the NIST CSF assessment report as shown in Table 7. Recommendations were made for all of the five functional areas that are included in the NIST CSF standard. Only the recommendations for the Identify functional area are shown here.

With the update of the NIST CSF to version 1.1 in April 2018, Reprivata’s management team wanted to ensure that the Master Agreements included appropriate verbiage for new key security control areas such as Supply Chain Risk Management. Because one of the purposes of Reprivata’s Master Agreements is to provide guidelines for interconnections with third party business partners, determining and adding any required supply chain language to the agreements is important.
Of particular interest were the process improvement-related security controls. These controls were aimed at helping those organizations that adopted the NIST CSF guidelines to demonstrate their cybersecurity programs. As such, incorporating process improvement language in the Master Agreements would commit all CoT users to maturing their cybersecurity programs.

The NIST CSF assessment noted that, of the 34 key control specific to the Master Agreements, over 20 of them were related to security policy, process, or procedural requirements. As such, the Reprivata team decided to engage with their external legal counsel to determine which key controls should be covered in the Master Agreements and which one could be addressed in the security language in the contracts prepared by CoT users to manage how they work with their business partners and other third parties.

The complete documentation of Recommendations for Enhancement of Reprivata Master Agreements for Implementing Community of Trust (CoT) risk management solution can be found in Artifact 3 in Appendix A.

**Evaluation of the Second Set of Artifacts Created for the Reprivata CoT Solution**

During the creation of the second set of artifacts, the evaluation process differed slightly from the one used for the first artifacts. While the first set of artifacts were primarily used for informing external parties on the cybersecurity risk management capabilities of the Reprivata CoT solution, these artifacts were created for informing the Reprivata organization on the CoT solution’s mapping to the NIST CSF. The Reprivata management team, who are not cybersecurity practitioners by training or experience, needed assistance on understanding more about the implementation of cybersecurity controls in organizations.

The initial artifact created was a NIST CSF version 1.0 compliance assessment of the Reprivata cybersecurity risk management solution. This creation was done prior to the release of
NIST CSF version 1.1 in April 2018. The focus of this review was to determine how many of the security controls were integrated into the Reprivata solution. This exercise was performed as a result of recommendation from the Cyber Florida staff at an intervention meeting in March 2018. When this assessment was completed, it was discussed with Reprivata’s management team as well as several potential clients. One of the comments on the initial assessment was that it did not provide sufficient information on how the security controls could potentially enable other controls because of the collaboration and data sharing capabilities of the solution.

In April 2018, just after the meeting with Cyber Florida, the NIST CSF version 1.1 was released for implementation by government agencies. At that time, a second cycle of assessments were performed. Since the primary change in the NIST CSF version 1.1 standards from the initial one was the inclusion of cybersecurity controls related to Supply Chain Management, it was straightforward to add the evaluations of these controls to the first assessment artifact. When Reprivata’s management reviewed the new report, the team asked how they could better inform potential clients on how the Reprivata solution could support the legal language with its functional collaboration and encryption capabilities. This additional information was added to the final legal recommendation artifact.

As with the evaluation of the first artifacts on the Reprivata solution’s technology controls, both of the new ones on legal recommendations for the Master Agreements were assessed several times by the Reprivata management team prior to the artifacts’ formal acceptance. As before, the Reprivata team were able to both question and comment on the process of assessing cybersecurity compliance across an organization. As they began to understand the compliance process, they determined that the messaging was being shared with potential customers on the Reprivata CoT solution’s cyber risk management capabilities. They
also realized that the messaging needed to be enhanced to include these new insights. As a result, additional artifacts, including product strategy presentations and new marketing collateral, were scheduled for development.

Again, because the Reprivata management team was actively involved in the artifact design and evaluation sessions, they were able to communicate the benefits of the artifacts very clearly internally, with plans to create similar informing messages for potential customers and other external parties. Additionally, the Reprivata team reported an increased understanding of the challenges of complying with cybersecurity standards. In particular, the team stated that Reprivata’s messaging regarding facilitating compliance with cybersecurity standards had become better at describing how well the Reprivata CoT solution met those compliance requirements.

Discussion

Cybersecurity researchers clearly need to continue exploring ways to create informing artifacts that help explain the impacts of cyber risks to cybersecurity practitioners and other stakeholders (Nurse, Creese, Goldsmith, & Lamberts, 2011). Research centers, such as Cyber Florida, are working to create broad collaborative networks of researchers to facilitate this research. Even so, the security of these collaboration networks is often limited by lack of funding, the scarcity of trained personnel, or both. Continuously managing risk requires a process that has specific dates for implementing capabilities, defined deliverables, and ongoing service and support activities, so organizations must strive to overcome these resource issues soon. (Jones & Gallo, 2007).

This issue is one reason that research based on ADR is important in cybersecurity research in particular. By embedding cyber-trained researchers with organizations’ cybersecurity
programs, the research is being conducted closer to the actual cyber risks. The outcomes and artifacts from these research initiatives can help foster collaboration both inside and between organizations as the reach of cyber risks is better understood and more affected parties. Such mutually beneficial arrangements can provide a knowledge exchange on the understanding of cyber risks and enable organizations to mature their cybersecurity programs by implementing some of the practice-based artifacts that the organization helped develop to meet their cybersecurity program needs. This approach was a success at Reprivata because of the company’s desire to become more cyber aware about the security capabilities of its own solution, as well as learning about the broader challenges, constraints, and opportunities of implementing and maturing a new cybersecurity company in what has become an increasingly complex field.

As shown in Table 3 in the Literature Review section, two of the most significant challenges that limit the abilities of organizations to understand cyber risks are legal and regulatory restrictions and the lack of collaboration between parties dealing with shared cyber risks (Shane & Hunker, 2013). While this research project did not face these particular problems, the researcher has addressed these types of constraints as a cybersecurity executive and practitioner working on cyber breach events. The inability to effectively and securely share cybersecurity risk and threat information has been shown to decrease the opportunities to analyze and understand cyber risks on a timely basis (Loukaka & Rahman, 2017). This limitation also impacts the ability of any first responders to mitigate cyber risks discovered due to the lack of actionable data about the technical vulnerabilities that have been exploited during an event (Greitzer, Moore, Cappelli, Andrews, Carroll, & Hull, 2008).

The ethical commitments required of cybersecurity professionals is very significant, especially as the need for practitioners to collaborate and share cyber risk information (Burstein,
Cybersecurity practitioners must meet the ethical requirements set forth by their professional credentialing agencies in order for those credentials to remain in good standing. Appropriate disclosure of information is one of those requirements. These ethical and legal limitations impede the collaboration between cybersecurity practitioners in the same way the NDAs and Federal and state laws restrict such disclosure. This issue comes into direct conflict when companies have business relationships with their third-party interconnections, such as suppliers or service providers. Often, no such ethical obligations exist.

While the cybersecurity field started initiatively for businesses to establish collective security or defense relationships, many of the cybersecurity standards do not require such collaboration by companies that implement those control frameworks. Except for the NIST CSF framework, the majority of other cybersecurity frameworks and standards are silent on requiring entities to share information on the identification, analysis, and understanding of cyber risks. By encouraging a broader adoption of the NISF CSF, such collaboration would be required because it affects how a company can mature its cybersecurity programs and comply with the standard (Shackelford, Proia, Martell, & Craig, 2015). However, because the NIST CSF is primarily a United States cybersecurity standard, it is unlikely to be embraced widely outside of the United States, though it can be mapped to other widely accepted security frameworks, such as the International Organization for Standardization (ISO) 27001 security standard and the Payment Card Industry Data Security Standard (PCI DSS) guidelines.

A number of industry governing bodies, such as Energy and Payment Cards, have created their own cybersecurity standards. Such industry standards, though similar to the NIST CSF, have differences in the number and types of cybersecurity controls that are required in definitions and usages of cybersecurity terms. Many cases exist where companies may be required to
implement more than one of these cybersecurity standards. In such cases, the determination of which standard will take precedence can be obscured by a number of factors, such as industry auditors, internal compliance managers, and Federal and state regulators. The difference in the interpretation of potentially conflicting standards can make it more difficult for internal and external stakeholders to understand the cybersecurity control requirements, to determine funding and other resource allocations for compliance programs, and to effectively share information on cyber risks because of the variances of the vocabulary and taxonomy in communications (Elnagdy, Qiu, & Gai, 2016).

Research noted that a limited number of technology solutions are available for securely sharing cybersecurity risk information (Fulford, 2017). As the cybersecurity landscape becomes more complicated to both navigate and understand, such cyber risk collaboration and sharing solutions will be required. This claim is especially true where business partners, particularly those with interconnected third parties, need to share sensitive cybersecurity risk information that impacts all the related parties (Trope, 2012).

The interventions with the cybersecurity SMEs were very revealing. Many questions and comments that arose during those sessions directly resulted from the Reprivata team’s lack of cybersecurity background and understanding of the terminology used by practitioners in the field. With the researcher’s assistance and by including the artifacts in the company’s product presentations and other collateral, the Reprivata cybersecurity message became clearer and more focused. After two artifact design and build cycles, the Reprivata management team gained a better understanding of the risk informing capabilities of their CoT solution, as well as the language of cybersecurity. The next step is to better educate potential customers on the benefits
of using the Reprivata CoT solution to help foster the same understanding in the customer organizations.

**Limitations of Current Research**

Several limitations to this research were noted. First, the members of the Reprivata management team lived all over the United States and overseas. This factor made scheduling of meetings for interviews, artifact design sessions, and subsequent evaluations very difficult. The researcher was able to meet with three of the Reprivata team in person on two different occasions, which did allow for very useful interchanges. More face-to-face meetings would have likely provided more insights into the informing capabilities of the Reprivata CoT solutions and the artifacts produced as a result of this research project.

Another limitation of the research was the small number of potential Reprivata customers and cybersecurity SMEs that were able to review and comment on the artifacts through either presentations or intervention sessions. The researcher was involved in six such meetings, four with customers and two with SME groups, and was able to gather valuable comments from the participants. However, to better judge the informing capabilities of the artifacts to help improve understanding of cyber risks, more evaluation and intervention sessions would be required.

A lack of cybersecurity-related literature on how to assist companies to better understand cyber risks was noted throughout this project. As noted in the Literature Review section, such research about informing stakeholders to enable their understanding of cybersecurity risks is very promising because of the rapid spread of cyber risks and threats and the urgent need to comprehend their effects more fully.

The researcher could not complete all the planned build phases because of the timing of the external legal reviews of the Reprivata Master agreements. While the recommendations for
enhancing the agreements to map to the NIST CSF version 1.1 standards have been reviewed by Reprivata management team, they have not been submitted to the attorneys for updating the Master Agreements until later in 2018.

**Conclusions**

Assisting a startup cybersecurity company to productize its cyber risk management solution, particularly one like Reprivata where only one member of the Reprivata team has real-world cybersecurity background and experience, can be challenging and rewarding. The differences in the use of cybersecurity terminology between the researcher and the Reprivata management team was one of the significant obstacles in the cyber risk informing objectives of this project. Through the analysis, design, and evaluation cycles that were part of creating the artifacts for this project, the overarching goal was increasing the Reprivata team’s understanding of the broader cybersecurity industry, its vocabulary, and the ways that practitioners in the field communicated with each other about cyber risks. While this objective was met, it was clear that a number of informing methods were required to effectively communicate the impacts of cyber risks. This finding was more related to the specific industry that the cyber risk information was being shared with than any other factor. Such differences, even small ones, impacted the success of informing potential clients about the cybersecurity risk management capabilities of the Reprivata solution during several presentations and also during the interventions.

Even as the researcher and the Reprivata team would gain a common understanding of the current cyber issues facing the company, another set of risks would appear and the informing process would begin again. The ultimate success of this research project came down to the researcher and the Reprivata team reaching an agreement–sometimes on a daily basis–on which artifacts and other comprehension enablers actually helped both parties understand cyber risks in
the same way, especially the ones that might affect the Reprivata CoT solution and its implementation by customers. When this agreement was reached and the Reprivata team presented the artifacts to potential customers, the meetings were successful in helping the customers understand the Reprivata cybersecurity controls and functionality, and to identify how the solution would be useful in the customer’s technology environment to secure sensitive communications and data. The identification of such use cases led to the first client Proof of Concept (PoC) agreement with DHS, which was signed in August 2018.

A number of findings were drawn from this ADR project on evaluating and enhancing the cyber risk informing capabilities of the Reprivata cybersecurity risk management solution. In this case, potential challenges to current cybersecurity research initiatives, such as how to deploy commercially available applications inside the Reprivata solution’s encrypted core and how to operationalize the threat intelligence functionality both inside and outside Reprivata’s closed network architecture, were overcome by the use of ADR techniques. Embedding this researcher in an organization improved team collaboration on creating operations documentation for the client PoC because sharing design information and improving client deliverables and other artifacts were seen as informing exercises that enhanced the quality of the communications between the Reprivata team and DHS. The collaboration that resulted allowed both parties to both understand and solve cyber risk issues related to the PoC quickly.

This research showed that active involvement of company personnel, SMEs, and potential customers in ADR artifact evaluations and interventions was most effective when multiple parties, such as company stakeholder and external SMEs, participated in the sessions. As a result of this approach, the artifacts took fewer reviews to be accepted. This approach worked well with DHS as the PoC was defined. Multiple work sessions involving Reprivata and
DHS personnel used DSR techniques to analyze and design project artifacts. By having already created a common design approach and agreeing on the PoC functional and operational requirements, the project had fewer delays in getting formal service agreement approved and signed.

In creating better ways to inform understanding of cybersecurity risks, cybersecurity practitioners and stakeholders are still struggling with the terminology required to enable better understanding of cyber risks. Researchers should continue to account for this when creating artifacts attempting to increase such comprehension in stakeholders. However, as demonstrated during this research project, continuously engaging with stakeholders to educate them on the vocabulary and taxonomy of cybersecurity communications is critical before any informing messages can be successfully created and then understood by the stakeholders.

Conclusions from the literature review identified a lack of cybersecurity-related literature on how to assist companies to better understand cyber risks. Research on enabling stakeholders’ understanding of cybersecurity risks appears to be a very promising area of investigation. The Reprivata cybersecurity risk management solution, as a secure, robust, and extensible method of providing collaboration and data sharing to interconnected stakeholders, provides an interesting opportunity to evaluate how risk informing the solution would be across industry and corporate boundaries.

Also, the implementations of cybersecurity risk management solutions to help raise the understanding of cyber risks with stakeholders face a number of challenges. In particular, the implementation of such solutions are not keeping pace with the rapid spread of cyber risks and threats and the urgent needs to determine their effects as accurately and quickly as possible. The Reprivata solution can be implemented on a number of technology platforms using open source
software. This ease of implementation could improve the successful deployment of other technology risk management methodologies if they follow Reprivata’s example for using DSR techniques to analyze and develop new cybersecurity risk management solutions.

References


Reprivata Community of Trust Secure Collaboration Software (SCS) Encrypted Core Concepts, version 1.0, March, 2018

Reprivata PC CoT Software Overview & Specification Private Collaboration Community of Trust (PC CoT), version 3.0, April 2018

Reprivata's Private Collaboration Community of Trust (PC CoT) UL Certified Software, April, 2018


CHAPTER FIVE:

USING A FITNESS-UTILITY MODEL TO ELABORATE THE IMPACTS OF ARTIFACTS CREATED TO ENHANCE THE RISK INFORMING CAPABILITIES OF A CYBERSECURITY RISK MANAGEMENT SOLUTION

Abstract

While assisting a startup cybersecurity company to productize its cyber risk management solution, the company’s management team stated that, as a group, they had very little real world working experience in the cybersecurity field. In an effort to become more cyber aware, the company’s management requested assistance in creating artifacts, such as solution documentation and other collateral. The artifacts would enable them to better communicate the risk informing capabilities of their cybersecurity risk management solution internally to their business partners and to potential customers. Once these artifacts were created, the Fitness-Utility Model proposed by Dr. Grandon Gill and Dr. Alan Hevner (Gill & Hevner, 2011) was used to evaluate how useful and impactful the artifacts were in increasing the solution’s risk informing capabilities and to help the company’s management team and other third parties, such as business partners and potential customers, to better understand cyber risks identified by the solution.

Introduction

In the academic journals that publish cybersecurity research, scholars are investigating how to advance a better understanding of cyber risks. However, few cybersecurity risk management solutions are available to practitioners that could help them both manage and comprehend the majority of those risks (Contreras, DeNardis, & Teplinsky, 2012). In this body
of literature, few studies of cybersecurity risk management methodologies have been done to
determine how well they inform users about cyber risks to their particular technology
environments. Additionally, these methods have not been formally evaluated to establish how
well they enable compliance with cybersecurity program standards and maturity measures
(Epstein, & Brown, 2008). With the lack of scholarly articles that have measured the usefulness
and fitness of cybersecurity risk management solutions using research methods, more work is
required. That situation gave rise to this research project, which was an investigation into what
types of artifacts could be created for the Reprivata cybersecurity risk management solution that
could be useful and effective in informing its users about cyber risks.

The creation of the first artifacts began with two requests from the Reprivata
management team in January 2018. First, they asked for a way to pictorially illustrate the
technology security controls and capabilities in the solution that would make the types of
controls clearer and easier to describe to potential customers. Because the management team did
not have a strong background in cybersecurity controls, such as encryption, access control, and
vulnerability and threat mitigation, a way to clearly and concisely inform potential customers on
the solution’s technical security functionality was needed.

Second, they inquired on better ways to assess and then communicate that the company’s
cybersecurity risk management solution complied with the National Institute of Standards and
Technology (NIST) Cybersecurity Framework (CSF). In 2014, the company had based the
original design of their cybersecurity risk management solution on the newly released NIST
CSF. However, the company had never performed a detailed security control assessment on the
solution against the NIST CSF standards. With business partners and potential customers
requesting validation that the company had performed NIST CSF and other security standards
reviews on the solution, this became a requirement to increase customer understanding of and confidence in the solution’s security compliance posture.

The objective of this research project was to research the types of artifacts that could assist the company in meeting its stated needs and requirements, and use the Action Design Research (ADR) process to create and evaluate the effectiveness of the artifacts developed. In this phase of research, the artifact interventions performed as part of the ADR process will be described and how the fitness and utility of the artifacts can be assessed using the Fitness-Utility Model, which was proposed by Dr. Grandon Gill and Dr. Alan Hevner in their Association for Computing Machinery Transactions on Management Information Systems (ACM TMIS) journal article published in 2011.

Motivation

Determining how the design artifacts developed during this research project enabled the Reprivata management team to better communicate cyber risk internally, to potential customers, and to business partners, has been the main of objective of the study since it started. Reprivata is a four year old company that has struggled with effectively informing partners and potential users of the industry-leading capabilities of its cybersecurity risk management solution. To meet these challenges, the researcher created design artifacts to address specific information sharing requirements related to how the solution communicates cyber risks to users.

This research article discusses the interventions and evaluations performed on the artifacts developed for enhancing the Reprivata cybersecurity risk management solution. The estimates of the artifacts’ fitness and utility were based on the Fitness-Utility Model proposed by Dr. Gill and Dr. Hevner in 2011. This Model enabled the researcher to study the artifacts and to
estimate their usefulness as parts of the Reprivata cybersecurity risk management solution’s overall design intent.

**Interviewing Approach for Artifact Evaluation**

During the evaluation of the design artifacts created by utilizing the Design Science Research (DSR) methodology, participant feedback on the utility of the artifacts gathered direct observations, such as in-person meetings, Webinars, and conference calls with the participants, in-depth, open-ended interviews performed with Reprivata’s management team, and written solution and company documentations including design documents, client presentations, and legal agreements. Every interaction was focused on engaging the participants to capture their real-world interpretations of the process of designing the artifacts and in the usefulness of the artifacts in practice. Realistic scenarios were used frequently to identify patterns of response and common themes by the participants (Patton, 2002).

Of concern with research where the participants provide estimates in response to questions and other inquiries, the validity of those responses is an important factor. For the purpose of this investigation, validity is defined as “how accurately the account represents participants’ realities of the social phenomena and is credible to them” (Cresswell & Miller, 2000). The research assumes the validity refers to the interpretations that can be made from the data gathered and not to the data itself (Hammersley & Atkinson, 1983).

Two of the particular techniques used to determine the validity of participant responses was by looking at the language and vocabulary used in participant replies and by making use of participants’ life experiences expressed during the evaluation sessions. This approach was drawn from the recommended qualitative data analysis strategies recommended by Juliet Corbin and Anselm Strauss in their book *Basics of Qualitative Research* (Corbin & Strauss, 2014). Corbin
and Strauss stated that unstructured interviews and observations are recommended in this type of research because the approach allows the participants to focus on those issues that are most meaningful to them and go into such topics in great detail (Corbin & Strauss, 2014). This approach is very advantageous when developing analyzing design requirements and evaluating the results of the design build iteration for its utility and applicability to practice.

Personal observations were an important part of this study, as suggested by qualitative research literature (Rubin & Rubin, 2011). From a researcher’s perspective, these in-person discussions and collaborations were critically important for capturing the company’s information for the case study, and for documenting the design requirements for the artifacts during the DSR iterations. These observations offered opportunities to develop more context around both the interview responses and the recommendations for enhancing the design artifacts.

**Description of the Fitness-Utility Model Utilized**

The Fitness-Utility Model was developed as a way to capture and evaluate how design artifacts change and improve over time. This Model also assists in determining the fitness of a particular design across a fitness landscape, which is defined by the authors as “a mapping between attributes and fitness that exists in the real world, but which is not observable” (Gill & Hevner, 2011).

This particular method has several advantages that make it suited for this research. As proposed by Drs. Gill and Hevner, determining the usefulness for design artifacts is in alignment with Design Research concepts. The use of fitness and utility models is understood by both academics and practitioners, and has been found to communicate how well artifacts can demonstrate fitness in attributes of their designs (Gill & Hevner, 2011).
The Fitness-Utility Model applied to this research (see Figure 3) is used to help demonstrate that a design artifact has an associated fitness, based on specific attributes that the artifact’s creator uses to make estimates of the artifact’s usefulness within the system it is being designed for. Once evaluated, artifacts can provide more concrete evidence that a particular design has intrinsic value within that system and can otherwise evolve over time and improve the artifact’s abilities to describe the fitness of the particular design system (Gill and Hevner, 2011).

Important in the case of this research project, the Fitness-Utility Model provides a vehicle for communicating between the creators of the potential design system and other stakeholders, and for providing a way to keep and share pertinent information about the design of the artifacts that are indicators of its usefulness.

Design Science strives to impact the design space that is being reviewed or used in such a way that design artifacts with a high level of fitness are continually introduced into the design system. This effect is realized in two ways: through the creation of artifacts that can show adaptability or the ability to evolve, and through the improvements in utility of the design artifacts that are shown through evaluations of those artifacts (Gill & Hevner, 2011).

The evaluation of design artifacts should be based on a more extensive and detailed utility function, instead of just the artifact’s usefulness, that estimates the artifact’s ability to evolve to maintain or extend its fitness. Utility attributes support a design artifact and a design system to evolve on an incremental basis, inspire designers and users to test and experiment with artifacts and their related systems, and to communicate ideas and other information that will help the design system and artifacts to proliferate and to become new and interesting over time (Gill & Hevner, 2011).
Figure 3 – Fitness-Utity Model for Design Research (Figure from Gill & Hevner, 2011)

Artifact Description – Reprivata Community of Trust Conceptual Model

The Conceptual Model for the Reprivata Community of Trust cybersecurity risk management solution describes the elements that are part of the solution and shows, in a pictorial way, how those elements can be affected and act together under the NISF CSF compliance requirements. In the Conceptual Model (see Figure 4), it seeks to articulate and explain the interactions of elements that influence successful Community of Trust (CoT) implementations. These elements help determine and, in some cases, manage the resources within these projects as part of the overarching corporate business strategy which determines the cyber risk posture, and how that posture can be managed and measured. These are two distinct groups of elements. One element is composed of the cybersecurity frameworks and contractual obligations, in the form of Master Agreement legal documents that provide structure to the CoT. The other element provides the rules of engagement and operational requirements for the Internal and External
Stakeholders of the CoT. These Stakeholders take the form of company management and governance as well as third parties that do business with or have influence on the company as oversight and compliance functions.

The External Stakeholders in the Model are CoT oversight functions, known as the CoT Privacy Authority. The CoT Privacy Authority is charged with reviewing how the CoT users meet their obligations under the Master Agreements and their NIST CSF compliance requirements.

Figure 4 – Proposed Conceptual Model – Reprivata Cybersecurity Community of Trust

Artifact Evolution

When the Conceptual Model was being designed and created, it was a new artifact that did not exist previously as part of Reprivata’s risk informing collateral. The Model went through
2 iterations before it was accepted by the Reprivata management team and published in its current version.

The first version of the Model only mapped the Community of Trust Risk Management Strategy and Community of Trust Governance elements, which map very closely to the NIST CSF version 1.0 controls.

The second version of the Model was mapped to NIST CSF version 1.1, which had been released in April 2018. The most important update to NIST CSF version 1.1 was the inclusion of Supply Chain Management (shown in the Model as Interconnected Third Parties) and the controls required by the updated framework. The revised model also included the Internal Stakeholders, which are shown as corporate management functions.

*Risk Informing Changes Made When the Artifact Was Implemented*

When the Conceptual Model was shared with Reprivata’s business partners and potential customers, these groups were able to better understand how security governance, compliance, and other controls in the NIST CSF could be enabled or enhanced by using the Reprivata cybersecurity risk management solution. Potential customers, including the Cyber Florida and the Department of Homeland Security (DHS), defined specific secure data sharing and collaboration use cases that could improve their understanding of cyber risks. C2, DHS, FS-ISAC were able to define use cases based on the Conceptual Model that could improve understanding of cyber risks. Some of the use cases identified included:

- The deployment of a CoT for the Chief Information Security Officers (CISOs) in the State of Florida University System to use when they were required to collaborate and share data regarding security events that affected one or more of the state universities.
• The design of a Proof of Concept (PoC) that would enable DHS investigators to share information on investigations and interact securely with other government agencies like the Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI).

• The Financial Services-Information Sharing and Analysis Center (FS-ISAC) requested a PoC to securely share sensitive security information about Internet threats and vulnerabilities with members of the ISAC.

Specific Cases Where the Artifact Made the Company Make Changes in the Way They Communicated Cyber Risks

Initially, Reprivata’s management believed that the Master Agreements, which set forth the terms and conditions for companies that deployed a CoT for itself and entities it desired to collaborate and share information with, were their primary product. At that time, Reprivata had decided to give away its CoT cybersecurity risk management solution if customers purchased the Master Agreements. This approach confused potential customers and devalued the company’s unique technology. Also, while the Master Agreements addressed the requirement for CoT users to comply with the NIST CSF standards, they did not show how the overall structure of the CoT solution complied with the security controls as part of its overall design.

However, after sharing the Conceptual Model with potential customers, the company realized the integration of the CoT cybersecurity risk management solution and the Master Agreements was the approach that better informed customers of Reprivata’s product and its capabilities. The Conceptual Model made the company realize that the integrated solution was a unique cybersecurity risk management offering that had NIST CSF compliance designed into and implemented by the solution.
Quotes from Intervention Participants About the Artifact

“The Conceptual Model enabled us to visualize how our solution, based on the NIST CSF, could enable collaboration between groups in an organization that needed to communicate and share data.” – Reprivata Management Team

“The Model helped us understand the concepts and relationships of the Reprivata solution. We used it when creating our use case to determine if we had identified the related work groups that needed to collaborate on security investigations.” – Customer who engaged Reprivata for Proof of Concept

“The Model helped us quickly understand how the Reprivata solution could be leverage the NIST CSF controls and help those controls be more widely implemented across an organization.” – Reprivata Business Partner

Artifact Description – NIST CSF Assessment for the Reprivata CoT Cybersecurity Risk Management Solution (version 4)

The NIST CSF Compliance Matrix was created to assess the security controls and capabilities of the Reprivata CoT cybersecurity risk management solution (see Table 8). The Compliance Matrix provides information on how those controls are implemented and if they are compliant with the NIST CSF requirements. The Matrix categorizes the security controls as Technology controls, Enabling controls, or controls that should be considered for inclusion in Reprivata’s Master Agreements to inform users of their security responsibilities as members of the CoT.

Technology controls are security functions that are part of the CoT solution’s design, architecture, and implementation. The Reprivata CoT cybersecurity risk management solution, in its initial design, was conceived to meet or exceed the security control requirements outlined in the NIST CSF. This Matrix provided the Reprivata management team and its potential customers with a very straightforward way to identify how its technology complied with the NIST CSF security requirements.
Enabling Controls, where the CoT security functionality supports or enhances the implementation of another control, were an important addition to the Matrix. This specific control review was added to the Matrix in order to inform potential customers on how the Technology-related controls in the CoT application and other controls which are based more on policies and procedures could be more easily managed and monitored through the use of the collaboration and data sharing functions of the solution.

Process improvement, program management, and similar controls that, when implemented, would help users mature their risk management postures through exchanging threat and security information. These controls were recommended for inclusion in the Reprivata Master Agreement to add more structure and focus to the CoT rules of engagement on how users are required to manage and improve their interactions with other users while they are collaborating and sharing sensitive data in the CoT.

Table 8 - NIST CSF Assessment and Findings for the Reprivata Community of Trust (CoT) Cybersecurity Risk Management Solution

<table>
<thead>
<tr>
<th>NIST CSF Functional Area</th>
<th>Reprivata CoT Solution Compliant with Key Controls</th>
<th>Technology Controls</th>
<th>Enabling Controls</th>
<th>Master Agreement Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify</td>
<td>15 out of 29 key controls</td>
<td>5</td>
<td>14</td>
<td>10</td>
</tr>
<tr>
<td>Protect</td>
<td>18 out of 39 key controls</td>
<td>12</td>
<td>21</td>
<td>6</td>
</tr>
<tr>
<td>Detect</td>
<td>15 out of 18 key controls</td>
<td>11</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Respond</td>
<td>13 out of 15 key controls</td>
<td>3</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>Recover</td>
<td>4 out of 6 key controls</td>
<td>0</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>65 out of 107 key controls</strong></td>
<td><strong>31</strong></td>
<td><strong>42</strong></td>
<td><strong>34</strong></td>
</tr>
</tbody>
</table>
Artifact Evolution

When the Compliance Matrix was being designed and created, it was a new artifact that did not exist previously as part of Reprivata’s security documentation for the solution. The Matrix went through four iterations before it was accepted by the Reprivata management team and published in its current version.

The first version of the Matrix mapped the solution compliance by high level Function and Category of the NIST CSF version 1.0 controls. It was originally created after a meeting with DHS in Washington, DC. The DHS security Subject Matter Experts (SMEs) asked if Reprivata had ever assessed its solution against the NIST CSF guidelines, and Reprivata answered that it had not. That afternoon, the researcher drafted the first assessment Matrix that covered the five Functional areas and 22 Categories of NIST CSF version 1.0. When the Reprivata solution was reviewed, it was determined that it could, at a high level, meet or exceed 20 of the 22 requirements. The two Categories that the solution could not directly meet were Protection functional controls related to categories Awareness and Training and Maintenance.

The second version of the Matrix was expanded to do a more detailed mapping of the Technology controls in NIST CSF version 1.0 to the solution. This version was a very revealing document to both the Reprivata management team and to potential customers. This Matrix demonstrated that, through the use of technology such as data encryption, security monitoring, and access management, the solution could meet 30 of the over 100 security controls in the NIST CSF version 1.0.

After the second revision of the Matrix, the Reprivata management team asked if a demonstration could be performed to show that using the CoT could actually make it easier for customers to implement security controls like policies and procedures. After some discussion,
the researcher developed the idea of Enabling Controls, where technology controls would support or speed up the deployment of security processes based on policies and procedures. The third version of the Matrix was designed to evaluate how such Enabling controls might work in practice. While documenting the third iteration, some controls were identified that attempted to address the need for factors like security program maturity and process improvements. After reviewing these items with the Reprivata management team, a new control evaluation was identified for these factors and were captured separately. Because they are potentially useful to many other CoT users, the researcher decided to use the factors as recommendations for inclusion in the Reprivata Master Agreements, where they can influence how CoT users interact with each other over time.

The fourth version of the Matrix was performed in July 2018 in response to the publication of NIST CSF version 1.1 in April 2018. This version was a relatively minor update, since the new NIST CSF guidelines added only one new category of controls for Supply Chain Management. In Table 8, the overall compliance with the NIST CSF version 1.1 controls reached 65 of 107 total controls, with 42 controls being enabled and supported because of the interaction with technology controls.

*Risk Informing Changes Made When the Artifact Was Implemented*

Using the Compliance Matrix for both internal solution design and implementation discussions, Reprivata management learned how to better communicate, at the individual security control level, how the solution complied with the NIST CSF. As the Matrix information was added to product presentations, customer interest in use cases and PoCs grew because Reprivata could now demonstrate the solution’s NIST CSF compliance in an easy-to-understand and risk informed way.
With the addition of the Enabling control assessment information in the Matrix, Reprivata’s management could better explain how the solution supported the more effective implementation of policy, process, and procedure controls. The CoT provided a secure communication, collaboration, and data sharing environment for security and risk management practitioners to utilize when they created and discussed these controls and any attendant risks. After reviewing the Matrix, Reprivata customers better understood how the CoT solution could improve their compliance postures by enabling them to more quickly create, deploy, and mature risk informed security programs, which are deemed to be at the Tier 2 level of maturity in the NIST CSF. The goal for security organizations that adopt the NIST CSF is aspiring to implement a security program with repeatable security controls using technologies, processes, and policies, described as the Tier 3 level of maturity.

Specific Cases Where the Artifact Made the Company Make Changes in the Way They Communicated Cyber Risks

After reviewing the Matrix with a key business partner, the Reprivata management team realized that the Technology control compliance achieved by the CoT solution met the requirements of the General Data Protection Regulation (GDPR), which standardizes data protection laws across all 28 European Union (EU) countries and imposes strict new rules on controlling and processing Personally Identifiable Information (PII). This realization opened a potentially new market for Reprivata’s CoT solution for Europe and other areas of the world. The NIST CSF is primarily a United States security standard, so the CoT solution’s ability to readily comply with international standards like GDPR is a tremendous market advantage.

Quotes from Intervention Participants About the Artifact

“The Compliance Matrix provided us with an understanding of the solution’s overall compliance with NIST CSF as well as a way to explain to customer how the solution
supports the implementation of policies and procedure through the use of its collaboration capabilities.” – Reprivata Management

“Upon review of the Compliance Matrix, it was easy to see how the solution would also provide a way for a CoT to comply with GDPR, because the control guidelines are very similar and the controls are already implemented in the solution.” – Reprivata Business Partner

Evaluation of the Artifacts’ Usefulness Based on the Fitness-Utility Model

Reprivata Community of Trust Conceptual Model (version 2)

The final intervention on the CoT Conceptual Model artifact was held at the Cyber Florida offices at the University of South Florida on August 22, 2018. This meeting was the follow up from the intervention performed with the Cyber Florida team on March 9, 2018, where the Reprivata team discussed the first version of the Conceptual Model with the Cyber Florida SMEs.

The purpose of this intervention was for the Cyber Florida team to provide their professional evaluations and observations on how well the Model informed them on the potential interactions of the CoT solution with its internal and external stakeholders as they worked to become more compliant with the NIST CSF.

This table shows how the intervention participants rated the Model’s usefulness, based on the fitness attributes that make up the Fitness-Utility model (see Table 9).

Table 9 – Estimates of Artifact Usefulness for the Proposed Conceptual Model for the Reprivata Cybersecurity Community of Trust

<table>
<thead>
<tr>
<th>Artifact Fitness Attribute</th>
<th>Estimate of Artifact’s Usefulness</th>
<th>Observations from Intervention Participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decomposable</td>
<td>• New conceptual elements could be easily added to the Model when required. • Interactions of conceptual elements could be readily identified.</td>
<td></td>
</tr>
</tbody>
</table>

The ability of a design to evolve incrementally.
Table 9 (Continued)

<table>
<thead>
<tr>
<th>Malleable</th>
<th>• The Model could be used by both government agencies and commercial firms. • Use cases where internal and external stakeholders needed to collaborate could be created.</th>
</tr>
</thead>
<tbody>
<tr>
<td>The degree to which artifacts can be adapted by its users and respond to changing use/market environments.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Open</th>
<th>• The Model was modified to address customer-specific conceptual elements and showed how they interacted with other elements.</th>
</tr>
</thead>
<tbody>
<tr>
<td>The degree to which artifacts are open to inspection, modification, and reuse.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Embedded in Design System</th>
<th>• Conceptual elements in the Model are part of the CoT solution’s overall design. • The Model could be adapted to new design criteria in the CoT solution.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Artifacts created are part of a sustainable design system environment rather than one that is produced in a context where design is an unusual activity.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Novel</th>
<th>• The Model is a common design artifact so it is easy to understand by stakeholders.</th>
</tr>
</thead>
<tbody>
<tr>
<td>A design that originates from an unexplored region of the design fitness landscape.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interesting</th>
<th>• The Model helps to identify unique interactions between the organization and the capabilities of the CoT solution.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Artifacts that demonstrate unexpected emergent behaviors that are worthy of subsequent investigation and the creation of subsequent artifacts or artifacts that can be constructed in an unexpected way that intrigue other designers or design researchers.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Elegant</th>
<th>• The Model is straightforward and communicates compliance interactions between internal and external stakeholders.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Artifacts which have design characteristics, such as compactness, simplicity, transparency of use, transparency of behavior, clarity of representation, that can invite surprise about, delight in, imitation of, and enhancement of the artifact.</td>
<td></td>
</tr>
</tbody>
</table>

Legend:

<table>
<thead>
<tr>
<th>Artifact Attribute Meets Definition</th>
<th>Artifact Attribute Meets Part of Definition</th>
<th>Artifact Attribute Does Not Meet Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
From review of the estimates of the Model’s Fitness-Utility attributes, the Reprivata Community of Trust Conceptual Model improved communication about the cybersecurity risk management capabilities of the CoT solution and how groups that used or were planning to use the CoT solution could interact based in its internal security functionality. Improvement to its informing capabilities could have been made as subsequent versions of the artifacts were designed and implemented.

*NIST CSF Assessment for the Reprivata CoT Cybersecurity Risk Management Solution (version 4)*

The final intervention on the NIST CSF Assessment Matrix for the Reprivata CoT solution artifact was held at the University of South Florida on August 10, 2018. This meeting was held between the Reprivata management team and one of the company’s key business partners. That partner had developed an online Web site that enabled customers to perform an assessment of various security frameworks, including the NIST CSF.

The purpose of this intervention was for a group of SMEs with a key Reprivata business partner to provide their professional evaluations and observations on how well the Matrix informed them on the overall compliance of the CoT solution with the NISF CSF standards. This assessment identified the ways the CoT solution’s technology controls and their potential enabling abilities supported the implementation of other non-technology controls, such as policies and procedures. The CoT solution was determined, based on the discussions with its internal and external stakeholders as they worked to become more compliant with the NIST CSF standards, to provide a significant level of compliance with the security control requirements.

This table shows how the intervention participants rated the Matrix’s usefulness based on the fitness attributes that make up the Fitness-Utility model (see Table 10).
<table>
<thead>
<tr>
<th>Artifact Fitness Attribute</th>
<th>Estimate of Artifact’s Usefulness</th>
<th>Observations from Intervention Participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decomposable</td>
<td>• The Matrix was straightforward and communicated control interactions. • The effects of Enabling Controls on overall compliance was communicated clearly.</td>
<td></td>
</tr>
<tr>
<td>Malleable</td>
<td>• Individual control requirements could be compared with each other and with those of other security standards to evaluate their similarities and differences.</td>
<td></td>
</tr>
<tr>
<td>Open</td>
<td>• The Matrix could be restructured to map controls of specific types, implementation, or governance. • The Matrix could be readily adapted to other security standards.</td>
<td></td>
</tr>
<tr>
<td>Embedded in Design System</td>
<td>• The Matrix demonstrated that compliance to NIST CSF security standard was integral to the CoT solution design intent.</td>
<td></td>
</tr>
<tr>
<td>Novel</td>
<td>• The inclusion of Enabling Controls and Master Agreement Control recommendations showed that the CoT solution is integrated to enable compliance at each part.</td>
<td></td>
</tr>
<tr>
<td>Interesting</td>
<td>• Significant interest has been expressed in determining how the CoT solution can be utilized in other areas, such as Legal, Human Resources, and Mergers and Acquisitions, where the need to secure collaboration and data sharing are required. • Further investigation on how Enabling Controls lead to cyber maturity was recommended.</td>
<td></td>
</tr>
<tr>
<td>Elegant</td>
<td>• The Matrix was very comprehensive but could have been easier to work with. • Automating the compliance assessment and evaluation was recommended.</td>
<td></td>
</tr>
</tbody>
</table>
From a review of the Model’s Fitness-Utility attributes estimates, the NIST CSF Assessment for the Reprivata CoT solution improved communication about how well the CoT solution complied with the NIST CSF standards. Of particular interest was how the assessment of Enabling Controls enhanced the CoT solution’s overall compliance potential for organizations. By supporting the implementation of non-technology controls through the use of collaboration and data sharing functionalities designed into the CoT solution, achieving, maintaining, and maturing future compliance to the NIST CSF and other cybersecurity standards could be easier.

**Discussion and Interpretation of Results**

The impacts from the interventions were significant to the Reprivata management team and the intervention participants. For both design artifacts, the Reprivata team and the intervention participants agreed that they were better informed about cyber risk compliance and how various groups could collaborate together to achieve NIST CSF compliance. Additionally, the groups stated that their understanding of the vocabulary used in cybersecurity increased with the reviews of the design artifacts as they were about to gain more context about cybersecurity concepts in relation to their organizations and how they managed their security programs.

In the discussion with potential clients and the intervention participants about the versions of the Reprivata Community of Trust Conceptual Model, the most interesting impact of the Model was the way that various compliance requirements between internal and external
stakeholders could be easily identified and discussed. Demonstrating, initially at a high level, the various types of potential activities that an organization’s internal and external stakeholder must evaluate as they worked to comply with the NIST CSF implementation and maturity requirements led to some rich conversations. These communications began to articulate the usefulness of the CoT solution’s capabilities as an important enabling part of a maturing cybersecurity program.

In the case of the NIST CSF Assessment Matrix for the Reprivata CoT Solution, the interesting impact of the design artifact was the introduction and acceptance of Enabling Controls as a way to increase the adoption of critical security controls and measure their compliance with the NIST CSF. The intervention participants agreed that the Enabling Controls helped them easily identify and show the interrelationships of various types of controls and how technology controls can influence the effectiveness of controls based on policies and procedures. While this research did not propose a quantitative method for measuring the influences of Enabling Controls on an organization’s compliance program, such research would be an interesting area of future investigation.

Using a Fitness-Utility Model, such as the one proposed by Drs. Gill and Hevner, helped both the researcher and the intervention participants to break down the various impacts of the design artifacts and to estimate which fitness attributes were important in showing the usefulness of the artifacts. As stated above, additional study into finding more quantitative ways to evaluate the fitness attributes to show improvements in the evolution of design artifacts would be a stimulating project.

References


CHAPTER SIX:
CONCLUSION, CONTRIBUTIONS, LIMITATIONS, AND FUTURE RESEARCH

Conclusions

Based on the literature review performed, a number of cybersecurity gaps were noted, especially related to the effective communication and measurement of cybersecurity risks. The differences in the use of cybersecurity terminology between the participants in this project were significant obstacles in the cyber risk informing objectives of this research. Additionally, the literature review identified a lack of cybersecurity-related literature on how to assist companies to better understand cyber risks.

The Reprivata CoT cybersecurity risk management solution is an industry-leading application with the capability to help disseminate a wide variety of cybersecurity information to the internal and external stakeholders of an organization. By developing an understanding of the security control types that were part of the solution’s design requirements, useful design artifacts were created that improved the ways that Reprivata, its business partners, and potential customers could discuss the solution’s security controls and their ability to comply with the NIST CSF more easily and in more detail, with a better understanding between the parties.

Helping cybersecurity practitioners as well as other people who are impacted by cyber risks to better understand those risks is a daunting task. It is becoming more difficult as the number and types of cyber risks grow over time. Taking up this challenge, this research project was able to appraise the usefulness of design artifacts that, according to cybersecurity
practitioners, improved the understanding of these risks when evaluated using a Fitness-Utility Model. While the findings are estimates, the increase in communication and information sharing by internal and external stakeholders of the solution were strong indicators that improvements did occur, though they could not be quantitatively measured at this time.

The interventions performed on the design artifacts identified the ways that cybersecurity practitioners communicate with each other and how they do so with people with less cybersecurity experience. This realization was very important to the Reprivata management team because it radically changed the way they communicated how their solution informed its users about cyber risks. The artifacts designed to assist in this informing process were not unique, but they did include new concepts, such as demonstrating the interactions of Enabling Controls on other controls and providing important context on how the Reprivata CoT solution was able to take advantage of these Enabling Controls because of the design intent where the NIST CSF cybersecurity framework was integrated into the technology.

The differences in the use of cybersecurity terminology used by the research participants was a significant obstacle in meeting the cyber risk informing objectives of this project. Through the DSR analysis, design, and evaluation cycles that were part of creating the artifacts for this project, the overarching goal was increasing the participants’ understanding of the vocabulary of cybersecurity risks and improving the ways cyber risks are communicated. While this objective was met, it was clear that a number of informing methods were required to effectively communicate the impacts of cyber risks. This finding was more related to the specific industry that cyber risk information was being shared with than any other factor. Such differences, even small ones, impacted the success of informing potential clients about the cybersecurity risk.
management capabilities of the Reprivata solution during several presentations and also during the interventions.

Even as the study participants would gain a common understanding of the current cyber issues facing the company, another set of risks would appear and the informing process would begin again. The ultimate success of this research project came down to the participants reaching an agreement – sometimes on a daily basis – on which artifacts and other comprehension aids actually helped both parties understand cyber risks in the same way, especially the ones that might affect the Reprivata CoT solution and its implementation by customers. When this agreement was reached and the Reprivata team presented the artifacts to potential customers, the meetings were successful in helping the customers understand the Reprivata cybersecurity controls and functionality, and to identify how the solution would be useful in the customer’s technology environment to secure sensitive communications and data. The identification of such use cases led to the first client Proof of Concept (PoC) agreement with DHS, which was signed in August 2018.

A number of conclusions were drawn from this ADR project on evaluating and enhancing the cyber risk informing capabilities of the Reprivata cybersecurity risk management solution. In this case, potential challenges to current cybersecurity research initiatives, such as how to deploy commercially available applications inside the Reprivata solution’s encrypted core and how to operationalize the threat intelligence functionality both inside and outside Reprivata’s closed network architecture, were overcome by the use of ADR techniques. Embedding this researcher in an organization improved team collaboration on creating operations documentation for the client PoC because sharing of design information and improving client deliverables and other artifacts were seen as informing exercises that enhanced
the quality of the communications between the Reprivata team and DHS. The collaboration that resulted allowed both parties to understand and solve cyber risk issues related to the PoC quickly.

This research showed that active involvement of company personnel, SMEs, and potential customers in ADR artifact evaluations and interventions was most effective when multiple parties, such as company stakeholder and external SMEs, participated in the sessions. As a result of this approach, the artifacts took fewer reviews to be accepted. This approach worked well with DHS as the PoC was defined. Multiple work sessions involving Reprivata and DHS personnel used DSR techniques to analyze and design project artifacts. By having already created a common design approach and agreeing on the PoC functional and operational requirements, the project had fewer delays in getting formal service agreement approved and signed.

In creating better ways to inform understanding of cybersecurity risks, cybersecurity practitioners and stakeholders are still struggling with the terminology required to enable better understanding of cyber risks. Researchers should continue to account for this when creating artifacts attempting to increase such comprehension in stakeholders. However, as demonstrated during this research project, continuously engaging with stakeholders to educate them on the vocabulary and taxonomy of cybersecurity communications is critical before any informing messages can be successfully created and then understood by the stakeholders.

Also, the implementations of cybersecurity risk management solutions to help raise the understanding cyber risks with stakeholders face a number of challenges. In particular, the implementation of such solutions are not keeping pace with the rapid spread of cyber risks and threats and the urgent needs to determine their effects as accurately and quickly as possible. The
Reprivata solution can be implemented on a number of technology platforms using open source software. This ease of implementation could improve the successful deployment of other technology risk management methodologies if they follow Reprivata’s example for using DSR techniques to analyze and develop new cybersecurity risk management solutions.

Contributions

Research Contributions

- **Contributions from the Case Study Paper**

  In this paper, “Implementing a Cybersecurity Community of Trust: Reprivata Seeks an “Early Adopter”” (Fulford, 2018), a new and promising cybersecurity risk management solution was identified and the management team was interviewed to determine some of the challenges it faced while attempting to get its first client. The case study identified several challenges the company faced, both with the design of its solution as well as with the messaging and communications about the solution’s cybersecurity risk management capabilities. These gaps served as the initial topics of discussion for analyzing the solution design for creating the requirements for the artifacts. The case study will inform both academics and practitioners on how differences in vocabulary and taxonomy can negatively impact both the design and ultimate customer acceptance of a new cybersecurity risk management solution.

- **Contributions from the Technical Note Paper**

  This paper, “A Note on the Cybersecurity Problem Spaces in 2018” (Fulford, 2018), was a supplement to the case study. It identified challenges that are facing governments, industries, and individuals related to cybersecurity. Informing gaps and cybersecurity control implementation issues were identified from the discussions of the numerous cybersecurity problem spaces. This gap analysis was used to help determine what type of artifacts would be
required and what types of information they would need to convey to internal and external stakeholders of cybersecurity risk management solutions.

- **Contributions from the Design Science Research Paper**

  This paper, “Evaluating and Enhancing the Risk Informing Capabilities of a Cybersecurity Risk Management Solution Using Action Design Research” (Fulford, 2018), was authored while the researcher was embedded with the target company, Reprivata. This ability to review all design documentation of the company’s cybersecurity risk management solution, interact with company management, and participate in meeting with business partners and potential clients offered advantages for this research. It made understanding the solution’s design much easier and facilitated the analysis, creation, and evaluation of the design artifacts. A key contribution of this paper was the identification of Enabling Controls and being able to perform an initial assessment of control interrelationships as they were implemented in the solution.

- **Contributions from the Enhance Action Design Research Paper**

  This paper, “Using a Fitness-Utility Model to Elaborate the Impacts of Artifacts Created to Enhance the Risk Informing Capabilities of a Cybersecurity Risk Management Solution” (Fulford, 2018), demonstrated the use of a proposed fitness-utility model during the evaluations of the design artifacts created and reviewed in Paper 3. By informing on expert estimates of design utility, this model provides practitioners with a way to facilitate discussions on the usefulness of future artifacts. This paper also showed the design research contribution types (see Table 11) for each of the artifacts. By estimating design artifacts for usefulness and then determining what types of contribution is being made to the overall design, practitioners now have a better way to inform their stakeholders on the risk informing capabilities of cybersecurity control and risk management solutions.
Overall, in evaluating the results from the interventions, improvements were noted on how the intervention participants moved toward a more consistent use of cybersecurity vocabulary over the course of those meetings. Such an improvement of the communication of cybersecurity risks and controls was the primary objective of this research. As the first design artifact was created, the Conceptual Model helped set a starting point for discussing how compliance to the NIST CSF could impact an organization at multiple levels, which was very useful in showing how the Reprivata CoT solution could enable a compliance program’s implementation and maturity.

However, the iterations of the Model did not include enough operational elements of an organization to show where the intersection of control definition and control management meet and where the compliance requirements of a cybersecurity program are actually measured. A deeper operational analysis of control deployment and compliance measures should be performed so the conceptual elements and their interactions with other elements can be included in the future iterations of the Model.

Because more interventions were performed on the NIST CSF Assessment Matrix for the Reprivata CoT Solution than on the Conceptual Model, the intervention participants stated that it was easier to understand and communicate its findings. Also, the participants found it to have more flexibility in examining controls, especially how the Technology Controls and the Enabling Controls worked in concert to support overall compliance with the NIST CSF.

The participants also stated that the Matrix was cumbersome and more difficult to use in its current form, especially when automated compliance assessment tools are available. While the automated compliance tools reviewed to not include Enabling Controls, adding that type of control analysis to such a tool would not be difficult. At this time, Reprivata is speaking with one
of its business partners that offers a control analysis application about updating it with a section that measures the potential impacts of Enabling Controls on the broader compliance cybersecurity program.

The design intent and characteristics of the two artifacts were reviewed against the Design Science Contribution Types table, which was included in the MIS Quarterly article by Drs. Gregor and Hevner published in 2013 (see Table 11) (Gregor & Hevner, 2013). From that evaluation, the Conceptual Model would be considered a Level 2 contribution to research. The Model’s use of key conceptual organizational elements to describe and communicate how those elements interact to influence compliance with the NIST CSF is key because of its potential impact on better understanding how cybersecurity risks and compliance to cybersecurity standards are useful in the ways an organization works with internal and external stakeholders.

The NIST CSF Assessment Matrix would be considered a Level 1 contribution to research because it focuses on implemented or established processes. Designed to be a more comprehensive cyber risk communicator than the Conceptual Model, the Matrix can be used to quickly analyze control compliance and comment upon the ways some controls can support and enable the implementation and maturity of other ones. Such matrices are often developed when cybersecurity researchers are studying how organizations comply with security and risk management guidelines. This Matrix, through its design intent and subsequent enhancements through interventions, begins to assess the impact of Enabling Controls on organizational compliance with cybersecurity standards, and suggests avenues of future research on the measurement of Enabling Control impacts on other security and operational controls.
Table 11 – Design Science Research Contributions by Artifact Type (from Gregor & Hevner, 2013)

<table>
<thead>
<tr>
<th>Contribution Types</th>
<th>Example Artifacts</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Level 3.</strong> Well-developed design theory about embedded phenomena</td>
<td>Design theories (mid-range and grand theories)</td>
</tr>
<tr>
<td><strong>Level 2.</strong> Nascent design theory—knowledge as operational principles/architecture</td>
<td>Constructs, methods, models, design principles, technological rules.</td>
</tr>
<tr>
<td><strong>Level 1.</strong> Situated implementation of artifact</td>
<td>Instantiations (software products or implemented processes)</td>
</tr>
</tbody>
</table>

Perhaps the most significant outcome from the uses of the design artifacts created during this research project is that Reprivata has acquired several customers since the project began. Reprivata’s management team has stated that including these design artifacts in Reprivata’s sales and product presentations has helped improve internal understanding of cybersecurity risks and increased customer interest in the CoT solution.

**Contributions to Practice**

Both of the design artifacts are useful in a broader context for cybersecurity and compliance practitioners. For example, the Conceptual Model was created so the various elements could be compared, individually, in groups, or all together, in order to investigate how the elements influence NIST CSF compliance. The same type of Model would work when comparing other compliance frameworks beyond cybersecurity, since the implementation processes for compliance programs have many of the same requirements, regardless of the type of standard or guideline to be deployed.
The Compliance Matrix could be very helpful in situations where compliance professionals are attempting to understand how specific types of cybersecurity controls work in different compliance environments. While the Matrix is designed to help evaluate the NIST CSF standard, it could be used to map other security control frameworks, such as the International Organization for Standardization (ISO) 27001 and GDPR.

By adding the analysis of Enabling Controls into the assessment evaluation process presented in this research, practitioners will be able to get a much broader view of their organization’s compliance environment and potentially find areas of non-compliance of controls before any control weakness can be exploited.

**Limitations of Current Research**

Limitations of this research were related to the challenges with setting up interventions and getting feedback from participants. In particular, non-disclosure agreements with potential customers limited the researcher’s ability to hold group meetings to discuss the design artifacts, which could have led to more enhancements to the design artifacts.

One issue in the research was the proximity of the participants. They lived all over the United States and overseas. This factor made scheduling of meetings for interviews, artifact design sessions, and subsequent evaluations very difficult. Interventions were held with three of the Reprivata team in person on two different occasions, which did allow for very useful interchanges. More face-to-face meetings would have likely provided additional and better insights into the informing capabilities of the Reprivata CoT solutions and the artifacts produced.

The small number of potential Reprivata customers and cybersecurity SMEs that were able to review and comment on the artifacts through either presentations or intervention sessions meant there were fewer estimates of the utility of the design artifacts. A total of six intervention
meetings, four with customers and two with SME groups, were held and the feedback from those sessions provided valuable comments and recommendations for improving the artifacts. However, to better judge the informing capabilities of the artifacts to help improve understanding of cyber risks, more such evaluation and intervention sessions would be required.

Another limitation is that the artifacts ability to improve in communicating cybersecurity risks was only estimated during the evaluation discussions. The participants stated that their understanding of cybersecurity risks increased during the interventions and they were better able to communicate the implications of those risks afterwards. Even with that advance in informing capabilities, the research did not include any comprehension or content testing in order to get more accurate measurements of those improvement.

Also, the Master Agreement control recommendations, while reviewed, were not implemented in the legal documents so they could be reviewed by the intervention participants. The participants discussed how the Master Agreements could be used to establish rules of engagement for collaborating on cyber risk, but they could not comment on how the recommendations actually increased the usefulness of the Master Agreements.

A lack of cybersecurity-related literature on how to assist companies to better understand cyber risks was noted throughout this project. As noted above, such research about informing stakeholders to enable their understanding of cybersecurity risks is very promising because of the rapid spread of cyber risks and threats, and the urgent need to comprehend their effects more fully.

All the planned build phases related to the Master Agreements could not be completed because of the timing of the external legal reviews of those contracts. While the recommendations for enhancing the agreements to map to the NIST CSF version 1.1 standards
have been reviewed by Reprivata management team, they have not been submitted to the attorneys for updating the Master Agreements until later in 2018.

The maturity assessment mechanism for the cybersecurity risk management solution could not be completed during this research project. The compliance matrix that was created provides a way to measure the effective implementation of cybersecurity controls, but it does not provide the repeatability measures that the maturity assessment could provide.

**Areas Requiring More Research**

Research into data analytic techniques that help determine how particular cybersecurity controls can be exploited shows a great deal of promise. In particular, the Reprivata Global Threat Intelligence (GTI) module captures a significant amount of network security data. Research methods that were examined as part of the Literature Review, such as utilizing the Latent Dirichlet Allocation algorithm to perform topic modeling of cybersecurity-related data sources, would be very useful artifacts for inclusion in cybersecurity risk management solutions (Kolini & Janczewski, 2017).

Investigating the interaction of Enabling Controls within a cybersecurity control framework implementation holds a great deal of potential. At present, no academic literature exists on this subject and current cybersecurity standards and control frameworks do not discuss how particular controls can enhance or speed the implementation of other similar or related controls. A research project on Enabling Controls is being performed by a team that includes Dr. Carol Saunders. Dr. Saunders is working to determine if there are any relevant management or social science theories, such as agency theory, that contribute to the implementation of cybersecurity controls. This study is assessing how cybersecurity controls interact with each
other and how some cybersecurity controls influence the deployment of complementary or related controls.

Further work on creating a quantitative method for measuring the influences of Enabling Controls on an organization’s compliance program could be a valuable contribution on the understanding and communicating of how cybersecurity risks can be mitigated and to what extent they can be eliminated or remediated. Understanding how and when those Enabling Controls impact other controls will be a necessity for practitioners as the risk and threat environment expands. Creating a measure or maturity metric that can demonstrate such things as funding, personnel, equipment, and other requirements and what their impacts would be in financial terms would be one goal of this research project.

Additional research into finding more quantitative ways to evaluate the fitness attributes of the design artifacts to show improvements in their evolution would help to better measure how useful the artifacts are. By helping practitioners to evaluate the level of understanding (measured as comprehension) that stakeholders have on the usefulness of design artifacts and how those artifacts can inform the stakeholders in practice, better solutions can be designed and the subsequent artifacts can be more effectively measured in use.

Research into cybersecurity risk management and compliance holds many opportunities to advance knowledge in the field. The estimation of the usefulness of artifacts in communicating cyber risk issues and analysis is a good start, but studies into quantifying the effectiveness of cybersecurity risk management solutions to inform their users can provide new insights on how cybersecurity solutions should approach the next generation of tools for cyber risk collaboration and information sharing.
Another topic for study would be expanding the mapping of other security control standards to include Enabling Controls and then determining what generalizable ways exist to implement these Enabling Controls that can improve compliance across multiple security standards. In today’s compliance-driven business environment, organizations are often required to implement more than one cybersecurity standard. A generalizable way of deploying such Enabling Controls could streamline the implementation of cybersecurity standards, meet the majority of the security requirements, and lessen the compliance assessment and management process by decreasing the number of security controls that must be regularly reviewed or classified as exceptions for closer management oversight and governance.

Performing interventions with groups of participants with less cybersecurity background and experience would be a valuable project to undertake. Evaluating how these groups improve in their understanding and communication of cybersecurity risk concepts and then comparing these results with those of practitioners or people with more cyber experience to find which topics are most easy to assimilate and which ones required focused design artifacts to improve cyber risk understanding and communication.

As discussed above, future directions in cybersecurity risk management should address how security controls interact with each other so that such relationships can be measured. In particular, the usefulness of future artifacts for the Reprivata cybersecurity risk management solution will require the inclusion of such measures in order to show its maturity against the NIST CSF and other cybersecurity standards, and how well it can maintain and monitor its compliance with those frameworks.

References


APPENDIX A

Artifact 1 – Proposed Conceptual Model for the Reprivata Community of Trust (CoT) Cybersecurity Risk Management Solution

Figure A1 - Proposed Conceptual Model and Description – Reprivata Cybersecurity Community of Trust

In the Proposed Conceptual Model above (also shown as Figure 2 in Section 5 above), the research will seek to articulate the interactions of elements that influence successful Cybersecurity Community of Trust (CoT) implementations. These elements help determine and, in some cases, manage the resources within these projects as the part of the overarching corporate business strategy which determines the cyber risk posture, and how that posture can be managed and measured. These are two distinct groups of elements: one that is composed of the cybersecurity frameworks and legal documents that provide structure to the CoT, and one that constitutes the Internal and External Stakeholders of the CoT.

In the Proposed Conceptual Model, the CoT Risk Management Strategy element (see Figure 2 in Section 5 above) defines the cybersecurity control requirements that the CoT members follow. In the case of Reprivata, the company selected the Cybersecurity Framework (CSF) that was developed by the National Institute of Standards and Technology (NIST) in 2014. The CSF was selected for two reasons. The CSF is a comprehensive set of cybersecurity control requirements based on 23 control categories across five
cybersecurity functional areas (see Table 4 in Section 5 above). As such, the CSF offers a comprehensive framework on which companies can build their cybersecurity programs. Also, the CSF includes a maturity model (see Table 5 in Section 5 above) that gives companies ways to determine how they are performing as they implement the CSF security controls.

The CoT Governance element (see Figure 2 in Section 5 above) is based on the Master Agreements that are executed between the overall Community of Trust’s Internal Stakeholders and its External Stakeholders. The Master Agreements provide the legal guidance over its governance functions that the CoT members will utilize in interactions between themselves, and are the basis for the on-going collaboration activities in the CoT. The IT risk assessment processes are defined, outlining the risk management requirements for each member, such as purchasing cyber insurance and the how the cybersecurity program maturity of the members will be evaluated against the CSF security controls framework. The contractual obligations of each member with regard to its IT compliance and how the technical and business interconnections are to be managed are also specified by this element. Finally, the risk metrics are defined, outlining what risk measurements and the frequency of reporting those measurements are stipulated.

These two elements (CoT Risk Management Strategy and CoT Governance) augment each other as required to implement the selected Cyber Risk Management methodology (see Figure 2 in Section 5 above). The provisions of CoT Governance empower the company’s ability to measure risk and show the company’s overall risk posture is being managed effectively. If risk management requirements are changed, the company will reassess its risk posture and determine how such changes impact its operational stance within the CoT and under the conditions of the Master Agreement. In this way, the Proposed Conceptual Model would demonstrate that any change in by one or both of these elements will typically require a business to re-assess its cyber risk posture with respect to the overall change in its technology footprint it uses to support the CoT and its strategic and operational decisions and initiatives. The effects on the corporation’s internal technology environment are ways that these elements influence the direction and scope of the cyber-related management program. These influencers provide both an internal and external context on how the CoT Risk Management Strategy is implemented, how its success is measured, and how it is evaluated against CoT Governance requirements, such as internal or external audits, external risk assessments, or regulatory reviews. These evaluations influence the CoT Risk Management Strategy implementation by providing the legal and cybersecurity orientation for enhancing cyber risk management, as well as the key performance metrics and reporting required by management.

The CoT Internal Stakeholders (see Figure 2 in Section 5 above) are the leaders of the company that is engaged in starting and maintaining the CoT. Boards of Directors Stakeholders assign the strategic and tactical responsibilities for implementing and maintaining effective cybersecurity and cyber risk management programs to the Management Stakeholders. These Stakeholders also provide oversight, advice, and review on Management’s performance on maturing these cyber-related programs, based on their fiduciary responsibilities to the company. The Management Stakeholders include the executives of the organization that are charged with resourcing, staffing, and monitoring the cyber-related programs in order to better secure and manage the risks prevalent in its interconnections with business partners. The executives are supported by the Cyber Security and Cyber Risk teams in this effort. The Cyber Security team is responsible for implementing and maintaining the requisite security controls required under the CSF framework, as well as performing regular “health checks” on those controls through the use of security management tools and techniques. The Cyber Risk team works closely with the Cyber Security group. They are charged with identifying, researching, and providing ways to measure the potential likelihood of threats that could impact the company and the CoT as a whole, the degree to which the applicable security controls are implemented, and the potential impact to the company and the CoT as a whole if a specific security control was not implemented effectively. The Cyber Risk also provides risk
reporting, as required under the CoT Governance element, on the relationships between the required security controls and the potential impacts where those controls are exposed by cyber-related threats and vulnerabilities.

The CoT External Stakeholders (see Figure 2 in Section 5 above) are those companies and other entities that are the third-party business interconnections connected to the overarching Cybersecurity CoT and the CoT Privacy Authority, which provides assessment and oversight of the privacy compliance of the COT. The CoT External Stakeholders are required under the Master Service agreements to implement, manage, and maintain robust cybersecurity and cyber risk programs in support of their organizations as well as the Cot, and strive to mature those programs over time. These Stakeholders have internal teams that ensure that risk analysis and measurement capabilities are in place and providing effective feedback on how the organization is managing to the CSF security framework and the executed CoT Master Agreement. They are making sure that continuous collaboration with the other members of the CoT takes place to share any real and potential security issues that do or could affect the CoT as a whole. These Stakeholders also assess the compliance of the company to all appropriate security controls required under the CSF and the maturity of the cyber-related programs. They then report on the security and risk management processes and practices for both the implementation of the applicable security controls as well as the maturation of those internal management control structures.

Other entities, such as the CoT Internal Stakeholders and the CoT External Stakeholders (see Figure 2 in Section 5 above), have a very different effect on the success of the implementation of the CoT Risk Management Strategy as required under the CoT Master Agreement. They can influence many of the business and cultural factors that will aid in both the success of the implementation of the cyber-related management programs and their long-term acceptance and maturation. The CoT Risk Management Strategy provides the enterprise-level structure of the security controls environment as well as the mechanism for the security and risk collaboration within the CoT. Each of these Stakeholder groups carries on the risk and compliance assessments of the CoT risk posture and how it impacts their organizations. As the CoT Internal Stakeholders and CoT External Stakeholders cooperate to support the business interconnections between them, they provide other important feedback on how the cyber-risk management programs are operating within the corporation and report on its effectiveness. This interchange between the Stakeholder groups is critical to the success of both companies’ cyber risk management programs within the CoT. When this collaboration is done well, these Stakeholder groups have created a cyber risk management reporting vehicle risk analysis and reporting that will provide significant benefits for all members of the CoT.

Key Terms for the Forces Used in the Proposed Conceptual Model Include:

- **Cybersecurity Community of Trust**: A group or entity (usually led by one entity that establishes the community and is considered its owner) that contract together to collaborate and create secure business interconnections. This Community’s cybersecurity posture is based on a robust set of cybersecurity controls that assist the companies in developing and maturing their enterprise cybersecurity and cyber risk programs.

- **Community of Trust Risk Management Strategy**: Those cybersecurity and cyber risk practices and processes, based on a robust and standard set of cybersecurity controls, that entities must implement (as required by legal agreements) in order to participate in the Cybersecurity Community of Trust. This Strategy must be applied by all entities to assess, categorize, prioritize, and assist in the remediation of cyber risks within the entity as part of strong and mature cybersecurity and cyber risk programs.

- **Community of Trust Governance**: The contractual management control and risk management processes requirements that the members of the Cybersecurity Community of Trust utilize to as
part of building, managing, assessing, and reporting on the security and risk postures of the Community.

- **Community of Trust Internal Stakeholders**: Those functional groups inside the entity establishing the Cybersecurity Community of Trust that support, assess, or are the recipients of outputs from the cybersecurity and cyber risk programs within the entity and the broader Community.

- **Community of Trust External Stakeholders**: Those functional groups inside the entity joining the Cybersecurity Community of Trust that support, assess, or are the recipients of outputs from the cybersecurity and cyber risk programs within the entity and the broader.
Artifact 2 – Assessment of the Reprivata Community of Trust (CoT) Cybersecurity Risk Management Solution Compliance with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) version 1.1

As part of the original design intent, the capabilities of the Reprivata Community of Trust (CoT) cybersecurity risk management solution controls were based on and implemented to comply with the initial version of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), which was published in 2014.

This control mapping analysis reviews the Reprivata solution’s compliance to the NIST CSF version 1.1, which was released in April 2018. This analysis expands on the initial NIST CSF version 1.0 control mapping performed on the Reprivata solution in March 2018.

The NIST CSF Functional Areas are documented in Table 4 of Section 5 of this document. The primary change in the NIST CSF Functional Areas from version 1.0 to version 1.1 is the inclusion of controls for Supply Chain Management that address security controls related to suppliers, vendors, and other interconnected business partners.

The color code used in the control’s assessment is as follows:

- **Bold Black** – Controls that are compliant with the NIST CSF version 1.1 standards.
- **Bold Blue** – Controls that, once implemented, can enable the implementation of other related controls (such as Access Controls, Physical Security, etc.).
- **Bold Red** – Controls that are recommended for inclusion in the Reprivata Master Agreements that would enable their implementation by the CoT users.

The Reprivata cybersecurity risk management control details and descriptions were provided by the Reprivata application design and supporting documentation as of April 2018 and from interviews with Reprivata’s Chief Executive Officer and Chief Technology Officer from January 2018 to August 2018.

**Overview of Reprivata CoT NIST CSF Compliance Assessment**

<table>
<thead>
<tr>
<th>NIST CSF Functional Area</th>
<th>Reprivata CoT Solution Compliant with Key Controls</th>
<th>Technology Controls</th>
<th>Enabling Controls</th>
<th>Master Agreement Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify</td>
<td>15 out of 29 key controls</td>
<td>5</td>
<td>14</td>
<td>10</td>
</tr>
<tr>
<td>Protect</td>
<td>18 out of 39 key controls</td>
<td>12</td>
<td>21</td>
<td>6</td>
</tr>
<tr>
<td>Detect</td>
<td>15 out of 18 key controls</td>
<td>11</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Respond</td>
<td>13 out of 15 key controls</td>
<td>3</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>Recover</td>
<td>4 out of 6 key controls</td>
<td>0</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>65 out of 107 key controls</strong></td>
<td><strong>31</strong></td>
<td><strong>42</strong></td>
<td><strong>34</strong></td>
</tr>
</tbody>
</table>
1. Identify – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. (28 key controls)

a. Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization’s risk strategy.

i. ID.AM-1: Physical devices and systems within the organization are inventoried

Asset management application or capabilities are in place for network, desktop, server, and mobile devices.

Reprivata CoT identifies end users and attached devices through the use of certificates during provisioning of devices and for access control for end users and devices.

Compliant with NIST CSF Control implemented in the Reprivata solution

Configuration management databases can provide this type of device information.

ii. ID.AM-2: Software platforms and applications within the organization are inventoried

Software management application or capabilities are in place for enterprise and workgroup applications for network,

Reprivata’s software components are documented in the Underwriter’s Laboratory certification report.

Compliant with NIST CSF Control implemented in the Reprivata solution

Software licensing and management databases can provide this type of device information.
|   | ID.AM-3: Organization communication and data flows are mapped | Data flows and communication paths have been mapped for critical business functions.  
Data flows are included in all business process documentation.  
Data flows are included in all business continuity plans. | Reprivata’s CoT data flows are captured in the software documentation prepared for the UL certification process. | Compliant with NIST CSF  
Control implemented in the Reprivata solution | Enterprise network management systems have the capability to create network communication maps. |
|---|-----------------|-------------------------------------------------|-----------------------------------------------|-----------------------------------------------|-----------------------------------------------------------------|
|   | ID.AM-4: External information systems are catalogued | Asset and software management applications or capabilities are in place for external information systems not directly managed by internal company personnel | External software requirements for the Reprivata CoT solution are captured in the software documentation prepared for the UL certification process. | Compliant with NIST CSF  
Control implemented in the Reprivata solution | Configuration management databases can provide this type of device information.  
Software licensing and management databases can provide this type of device information. |
|   | ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value | Hardware and software resources are prioritized by function and included in business continuity plans.  
A data classification program is in place and regularly reviewed.  
Technology and operational risk assessments are performed regularly. | Resource classification policies and procedures are implemented as part of the organization’s cybersecurity risk management program. | The Reprivata solution enables these policies and procedures and provides information that can be used to determine data classification, criticality, and business value. | Cybersecurity policies and procedures can be created and evaluated by companies that offer cybersecurity awareness and training software as well as by external consulting firms.  
Training for creating cybersecurity policies and procedures is available with a variety of online and in-person sessions. |
|   | ID.AM-6: Cybersecurity roles and responsibilities for internal | Security responsibilities for internal | When included in the Reprivata Master | Cybersecurity roles and responsibilities | The Master Agreements are designed to be |
b. Business Environment (ID.BE): The organization’s mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.  

| ID.BE-1: The organization’s role in the supply chain is identified and communicated | Senior management has created appropriate tactical and strategic responsibilities for the supply chain management program and communicated that information to the appropriate stakeholders. | When included in the Reprivata Master Agreement, this enables compliance with NIST CSF. | The Reprivata solution enables secure communication of supply chain management responsibilities related to supply chain management by providing encrypted data sharing and collaboration capabilities for the CoT users. | The Master Agreements are designed to be easily updated by internal and/or external legal counsel as required by the CoT owner. All CoT users are required to sign the Master Agreement before they can utilize the data sharing and collaboration capabilities of the CoT. |
| ID.BE-2: The organization’s place in critical infrastructure and its industry sector is identified and communicated | Senior management has created appropriate tactical and strategic responsibilities for the supply chain management | The assignment and communication of supply chain management responsibilities require senior management input and approval. | The Reprivata solution enables secure communication of supply chain management responsibilities to stakeholders by providing encrypted data | Supply chain management strategies and tactical procedures can be created and evaluated by companies that offer supply chain management responsibilities. |
| ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated | Senior management has created appropriate tactical and strategic responsibilities for the supply chain management program and communicated that information to the appropriate stakeholders. | The prioritization and communication of supply chain management goals and objectives require senior management input and approval. | Supply chain management strategies and tactical procedures can be created and evaluated by companies that offer supply chain management software as well as by external consulting firms. |
| ID.BE-4: Dependencies and critical functions for delivery of critical services are established | Critical services have been identified and the dependencies on those services are documented. Critical service dependencies are documented by function and included in business continuity plans. | The critical service delivery requirements must be created and approved by key management stakeholders. These requirements must be included in business resiliency and recovery plans. | Service delivery strategies and business resiliency procedures can be created and evaluated by companies that offer business resilience management software as well as by external consulting firms. |
| ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations) | Critical service dependencies are documented by function and included in business continuity plans. | The critical service delivery requirements must be created and approved by key management stakeholders. These requirements must be included in business resiliency and recovery plans. | Service delivery strategies and business resiliency procedures can be created and evaluated by companies that offer business resilience management software as well as by external consulting firms. |
| Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements are understood and inform | | The Reprivata solution enables secure collaboration and data sharing by key management stakeholders when discussing mission-critical service delivery requirements. | |
the management of cybersecurity risk.

<table>
<thead>
<tr>
<th>ID.GV-1: Organizational Cybersecurity Policy is Established and Communicated</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>i.</strong></td>
</tr>
<tr>
<td>Senior management has established a cybersecurity program and assigned leadership for the function.</td>
</tr>
<tr>
<td>The Reprivata solution enables secure collaboration and data sharing by key management stakeholders when discussing the governance of the cybersecurity organization and its operation.</td>
</tr>
<tr>
<td>The Master Agreements are designed to be easily updated by internal and/or external legal counsel as required by the CoT owner. All CoT users are required to sign the Master Agreement before they can utilize the data sharing and collaboration capabilities of the CoT.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ID.GV-2: Cybersecurity Roles and Responsibilities are Coordinated and Aligned with Internal Roles and External Partners</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ii.</strong></td>
</tr>
<tr>
<td>Senior management has established a cybersecurity program and assigned leadership for the function. Cybersecurity program requirements have been documented, implemented, and communicated to both internal and external stakeholders.</td>
</tr>
<tr>
<td>The Reprivata solution enables secure collaboration and data sharing by key internal and external stakeholders when discussing the governance of the cybersecurity requirements for all CoT users.</td>
</tr>
<tr>
<td>The Master Agreements are designed to be easily updated by internal and/or external legal counsel as required by the CoT owner. All CoT users are required to sign the Master Agreement before they can utilize the data sharing and collaboration capabilities of the CoT.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ID.GV-3: Legal and Regulatory Requirements Regarding Cybersecurity, Including Privacy and Civil Liberties Obligations, are Understood and Managed</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>iii.</strong></td>
</tr>
<tr>
<td>Cybersecurity program compliance and legal requirements have been documented, implemented, and communicated to both internal and external stakeholders.</td>
</tr>
<tr>
<td>The Reprivata Master Agreement is a legal document that can be customized as required by the CoT owner so the appropriate security, operational, and policy requirements are in place for all CoT users.</td>
</tr>
<tr>
<td>The Master Agreements are designed to be easily updated by internal and/or external legal counsel as required by the CoT owner. All CoT users are required to sign the Master Agreement before they can utilize the data sharing and</td>
</tr>
<tr>
<td>iv.</td>
</tr>
<tr>
<td>d.</td>
</tr>
<tr>
<td>i.</td>
</tr>
</tbody>
</table>
| ii. | ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources | A threat intelligence assessment and review process is documented, implemented, and communicated to both internal and external stakeholders. | Reprivata CoT can integrate active network threat monitoring, identification, and mitigation both inside and outside the CoT through its Global Threat Intelligence capabilities. | Compliant with NIST CSF Control 01-27. | External threat intelligence and vulnerability databases can provide this type of threat and vulnerability information.
### iii. ID.RA-3: Threats, both internal and external, are identified and documented

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
<th>Senior Management</th>
<th>The Reprivata Solution Enables</th>
<th>Cybersecurity Threat Assessment and Intelligence Programs Can Be Created and Evaluated by Companies That Offer Threat Assessment and Intelligence Software As Well As by External Consulting Firms.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A threat intelligence assessment and review process is documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>Senior management is required to create and implement a cybersecurity threat assessment and intelligence program that is consistent with the organization’s risk posture.</td>
<td>The Reprivata solution enables secure collaboration and data sharing by key management stakeholders when discussing the risks associated with the threat assessment and intelligence program.</td>
<td>Cybersecurity threat assessment and intelligence programs can be created and evaluated by companies that offer threat assessment and intelligence software as well as by external consulting firms.</td>
</tr>
</tbody>
</table>

### iv. ID.RA-4: Potential business impacts and likelihoods are identified

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
<th>Senior Management</th>
<th>The Reprivata Solution Enables</th>
<th>Cybersecurity Threat Assessment and Intelligence Programs Can Be Created and Evaluated by Companies That Offer Threat Assessment and Intelligence Software As Well As by External Consulting Firms.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A threat and vulnerability research and evaluation process is documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>Senior management is required to create and implement a cybersecurity threat assessment and intelligence program that is consistent with the organization’s risk posture.</td>
<td>The Reprivata solution enables secure collaboration and data sharing by key management stakeholders when discussing the risks associated with the threat assessment and intelligence program.</td>
<td>Cybersecurity threat assessment and intelligence programs can be created and evaluated by companies that offer threat assessment and intelligence software as well as by external consulting firms.</td>
</tr>
</tbody>
</table>

### v. ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
<th>Senior Management</th>
<th>The Reprivata Solution Enables</th>
<th>Cybersecurity Threat Assessment and Intelligence Programs Can Be Created and Evaluated by Companies That Offer Threat Assessment and Intelligence Software As Well As by External Consulting Firms.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A threat and vulnerability research and evaluation process is documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>Senior management is required to create and implement a cybersecurity threat assessment and intelligence program that is consistent with the organization’s risk posture.</td>
<td>The Reprivata solution enables secure collaboration and data sharing by key management stakeholders when discussing the risks associated with the threat assessment and intelligence program.</td>
<td>Cybersecurity threat assessment and intelligence programs can be created and evaluated by companies that offer threat assessment and intelligence software as well as by external consulting firms.</td>
</tr>
</tbody>
</table>

### vi. ID.RA-6: Risk responses are identified and prioritized

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
<th>When Included in the Reprivata Master Agreement, This Enables</th>
<th>The Master Agreements Are Designed to Be Easily Updated by Internal</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A risk management and communication program is documented.</td>
<td>The Reprivata Master Agreement is a legal document that can be</td>
<td>The Master Agreements are designed to be easily updated by internal</td>
</tr>
</tbody>
</table>

(SIEM) software and analytics tools can provide this type of device information.
implemented, and communicated to both internal and external stakeholders.  

| Implemented, and communicated to both internal and external stakeholders. | Compliance with NIST CSF. | Customized as required by the CoT owner so the appropriate risk management response and communication requirements are in place for all CoT users. | and/or external legal counsel as required by the CoT owner. All CoT users are required to sign the Master Agreement before they can utilize the data sharing and collaboration capabilities of the CoT. |

| **Risk Management Strategy (ID.RM): The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.** | \[1.5ex\] Senior management has established a risk management and communication program and assigned leadership for the function. A risk management and communication program is documented, implemented, and communicated to both internal and external stakeholders. | Senior management is required to create and implement a cybersecurity risk management strategy and assign appropriate leadership that is consistent with the organization’s risk posture. | The Reprivata solution enables secure collaboration and data sharing by key operational risk management stakeholders when discussing the risks associated with the cybersecurity risk management strategy. Cybersecurity risk management strategies can be created and evaluated by external consulting firms. |

| **i. ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders** | \[1.5ex\] An operational risk management and communication program is documented, implemented, and communicated to both internal and external stakeholders. | Senior management is required to create and implement an operational risk management strategy and assign appropriate leadership that is consistent with the organization’s risk posture. | The Reprivata solution enables secure collaboration and data sharing by key operational risk management stakeholders when discussing the risks associated with the operational risk management strategy. Cybersecurity risk management strategies can be created and evaluated by external consulting firms. |

| **ii. ID.RM-2: Organizational risk tolerance is determined and clearly expressed** | \[1.5ex\] | | |
### iii. ID.RM-3: The organization’s determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis

| Senior management has established a risk tolerance and posture based on the analysis of its technology footprint, industry position, and other critical business indicators. | Senior management is required to create and implement a cybersecurity risk posture that is consistent with the organization’s overall risk appetite. | The Reprivata solution enables secure collaboration and data sharing by key risk management stakeholders when discussing the corporate risk posture. | Cybersecurity risk management postures can be created and evaluated by external consulting firms. |

### f. Supply Chain Risk Management (ID.SC): The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess, and manage supply chain risks.

| Senior management has established a supply chain management program and assigned leadership for the function. A risk management and communication program is documented, implemented, and communicated to both internal and external stakeholders. | The establishment, agreement, and communication of supply chain cybersecurity risk management responsibilities require senior management and key stakeholders input and approval. | The Reprivata solution enables secure communication of supply chain management cybersecurity risk management responsibilities to stakeholders by providing encrypted data sharing and collaboration capabilities. | Supply chain management strategies and tactical procedures can be created and evaluated by companies that offer supply chain management software as well as by external consulting firms. |

### i. ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders

| Cybersecurity risk management and review processes for critical suppliers have been documented. | When included in the Reprivata Master Agreement, this enables compliance with NIST CSF. | The Reprivata solution enables secure communication of supply chain management cybersecurity risk management responsibilities to stakeholders by providing encrypted data sharing and collaboration capabilities. | The Master Agreements are designed to be easily updated by internal and/or external legal counsel as |
and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process.

<table>
<thead>
<tr>
<th>ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization’s cybersecurity program and Cyber Supply Chain Risk Management Plan</th>
<th>Cybersecurity legal requirements for suppliers have been documented, implemented, and communicated to both internal and external stakeholders.</th>
<th>When included in the Reprivata Master Agreement, this enables compliance with NIST CSF.</th>
<th>The Reprivata solution enables secure communication of contractual obligations related to supply chain management cybersecurity responsibilities by providing encrypted data sharing and collaboration capabilities.</th>
<th>The Master Agreements are designed to be easily updated by internal and/or external legal counsel as required by the CoT owner. All CoT users are required to sign the Master Agreement before they can utilize the data sharing and collaboration capabilities of the CoT.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations</td>
<td>Cybersecurity legal and regulatory compliance requirements for suppliers have been documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>When included in the Reprivata Master Agreement, this enables compliance with NIST CSF.</td>
<td>The Reprivata solution enables secure communication of contractual obligations related to supply chain management cybersecurity audit and assessments responsibilities and reporting by providing encrypted data sharing and collaboration capabilities.</td>
<td>The Master Agreements are designed to be easily updated by internal and/or external legal counsel as required by the CoT owner. All CoT users are required to sign the Master Agreement before they can utilize the data sharing and collaboration capabilities of the CoT.</td>
</tr>
<tr>
<td>ID.SC-5: Response and recovery planning and testing are</td>
<td>Incident response, recovery, and management requirements for</td>
<td>When included in the Reprivata Master Agreement, this enables</td>
<td>The Reprivata solution enables secure communication of contractual</td>
<td>The Master Agreements are designed to be easily updated by internal</td>
</tr>
<tr>
<td>Conducted with suppliers and third-party providers</td>
<td>Suppliers have been documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>Compliance with NIST CSF.</td>
<td>Obligations related to supply chain management business resiliency testing and reporting responsibilities by providing encrypted data sharing and collaboration capabilities.</td>
<td>and/or external legal counsel as required by the CoT owner. All CoT users are required to sign the Master Agreement before they can utilize the data sharing and collaboration capabilities of the CoT.</td>
</tr>
</tbody>
</table>

2. **Protect – Develop and implement appropriate safeguards to ensure delivery of critical services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. (39 key controls)**

| a. Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions. | An identity and access management, review, and assessment program has been have been documented, implemented, and communicated to both internal and external stakeholders. | Reprivata CoT identifies end users and attached devices through the use of certificates during provisioning of devices and for access control for end users and devices. | Compliant with NIST CSF Control implemented in the Reprivata solution |

| i. PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes | Physical access requirements for facilities where information and technology | Senior management is required to create and implement a | The Reprivata solution enables secure collaboration and data |

<p>| ii. PR.AC-2: Physical access to assets is managed and protected | Physical security access management systems can provide this type of user and device access information. Security log management software and analytics tools can provide this type of user and device access information. |</p>
<table>
<thead>
<tr>
<th></th>
<th>PR.AC-3: Remote access is managed</th>
<th>User and service remote access to technology assets have been documented, implemented, and communicated to both internal and external stakeholders.</th>
<th>Reprivata CoT requires end users and attached devices to connect through the use of encrypted virtual private network tunnels.</th>
<th>Compliant with NIST CSF Control implemented in the Reprivata solution</th>
<th>Remote access software can provide this type of functionality. Next-generation firewalls can provide this type of functionality.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties</td>
<td>User identities, roles, permissions, and access requirements that ensure that the only minimum necessary access to technology assets is granted have been documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>Reprivata CoT enables access control permissions for end users and attached devices through the use of certificates.</td>
<td>Compliant with NIST CSF Control implemented in the Reprivata solution</td>
<td>Identity and access management systems can provide this type user and device access information.</td>
</tr>
<tr>
<td></td>
<td>PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)</td>
<td>Network architecture requirements to implement secure network design and connectivity have been documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>Reprivata CoT includes network segregation and segmentation capabilities as part of the implemented cybersecurity trusted and closed network control structure.</td>
<td>Compliant with NIST CSF Control implemented in the Reprivata solution</td>
<td>Network device configuration controls and device management software provides this type of functionality.</td>
</tr>
<tr>
<td></td>
<td>PR.AC-6: Identities are proofed and bound to credentials and</td>
<td>User identities, permissions, and access requirements that ensure that</td>
<td>Reprivata CoT identifies end users and attached devices</td>
<td>Compliant with NIST CSF Control implemented in</td>
<td>Identity and access management systems can provide this type</td>
</tr>
<tr>
<td>asserted in interactions</td>
<td>only authorized users have access to technology assets have been documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>through the use of certificates.</td>
<td>the Reprivata solution user and device access information.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>---------------------------------</td>
<td>---------------------------------</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| vii. R.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals’ security and privacy risks and other organizational risks) | The use of user authentication mechanisms for user access to technology assets is based on the risks inherent to the specific user role and technology asset type has been documented, implemented, and communicated to both internal and external stakeholders. | Reprivata CoT enables access control permissions for end users and attached devices through the use of certificates. | Compliant with NIST CSF Control implemented in the Reprivata solution |

| b. Awareness and Training (PR.AT): The organization’s personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements. | A cybersecurity awareness program has been documented, implemented, and communicated to both internal and external stakeholders. | Senior management is required to create and implement a cybersecurity awareness program that is consistent with the organization’s risk posture. | The Reprivata solution enables secure collaboration and data sharing by key internal and external stakeholders when discussing the cybersecurity risks. |

<p>| i. PR.AT-1: All users are informed and trained | | Cybersecurity awareness training can be obtained from companies that offer cybersecurity awareness and training software as well as by external consulting firms. | Cybersecurity awareness training is available with a variety of online |</p>
<table>
<thead>
<tr>
<th>ii. PR.AT-2: Privileged users understand their roles and responsibilities</th>
<th>Privileged and administrative user identities, roles, permissions, responsibilities, and access requirements for information and technology assets have been documented, implemented, and communicated to both internal and external stakeholders.</th>
<th>Cybersecurity management is required to create the roles and responsibilities for privileged users such as system administrators and network analysts.</th>
<th>The Reprivata solution enables secure collaboration and data sharing by privileged users when discussing their roles and responsibilities related to cybersecurity.</th>
<th>Privileged user responsibilities can be created and evaluated by device and software companies as well as by external consulting firms.</th>
</tr>
</thead>
<tbody>
<tr>
<td>iii. PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities</td>
<td>Supplier and other third party identities, roles, permissions, responsibilities, and access requirements for information and technology assets have been documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>When included in the Reprivata Master Agreement, this enables compliance with NIST CSF.</td>
<td>The Reprivata solution enables secure communication of third party contractual obligations related to data and system protection responsibilities by providing encrypted data sharing and collaboration capabilities.</td>
<td>The Master Agreements are designed to be easily updated by internal and/or external legal counsel as required by the CoT owner. All CoT users are required to sign the Master Agreement before they can utilize the data sharing and collaboration capabilities of the CoT.</td>
</tr>
<tr>
<td>iv. PR.AT-4: Senior executives understand their roles and responsibilities</td>
<td>Senior executive identities, roles, permissions, responsibilities, and access requirements for information and technology assets have been documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>Senior management is required to create, document, and implement an executive-level cybersecurity responsibilities management and reporting system that is consistent with the organization’s risk posture.</td>
<td>The Reprivata solution enables secure collaboration and data sharing by senior executives and upper management when discussing their cybersecurity responsibilities.</td>
<td>Executive-level cybersecurity responsibilities training can be obtained from companies that offer cybersecurity training software as well as from external consulting firms. Cybersecurity awareness training is available with a variety of online resources.</td>
</tr>
<tr>
<td>v. PR.AT-5:</td>
<td>Physical and cybersecurity personnel understand their roles and responsibilities</td>
<td>Physical security personnel identities, roles, permissions, responsibilities, and access requirements for information and technology assets is granted have been documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>Senior management is required to create and implement a physical security management program that is consistent with the organization’s risk posture.</td>
<td>The Reprivata solution enables secure collaboration and data sharing by key management stakeholders when discussing the risks associated with physical security management program.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>c. Data Security (PR.DS): Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.</td>
<td>Data encryption requirements for all electronic information assets residing on technology platforms and other devices have been documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>Reprivata CoT implements multi-level encryption for data at rest.</td>
<td>Compliant with NIST CSF Control implemented in the Reprivata solution</td>
<td>No applicable external solutions are available since the Reprivata CoT implements government-level encryption in the software solution.</td>
</tr>
<tr>
<td>i. PR.DS-1: Data-at-rest is protected</td>
<td>Data encryption requirements for all electronic information assets residing on technology platforms and other devices have been documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>Reprivata CoT requires end users and attached devices to connect through the use of encrypted virtual private network tunnels.</td>
<td>Compliant with NIST CSF Control implemented in the Reprivata solution</td>
<td>No applicable external solutions are available since the Reprivata CoT implements government-level encryption in the software solution.</td>
</tr>
<tr>
<td>ii. PR.DS-2: Data-in-transit is protected</td>
<td>Data encryption requirements for all electronic information assets being transmitted over insecure networks or where such encryption is specified by legal agreements have been documented, implemented,</td>
<td>Reprivata CoT requires end users and attached devices to connect through the use of encrypted virtual private network tunnels.</td>
<td>Compliant with NIST CSF Control implemented in the Reprivata solution</td>
<td>No applicable external solutions are available since the Reprivata CoT implements government-level encryption in the software solution.</td>
</tr>
</tbody>
</table>
### iii. PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition

<table>
<thead>
<tr>
<th>Senior management is required to create and implement a computer and technology asset management program.</th>
<th>The Reprivata solution enables secure management of critical technology assets that are members of the CoT by ensuring security management and tracking of those assets.</th>
<th>Configuration management databases can provide device inventory reporting. Asset tracking and reporting software can enhance technology asset management and replacement.</th>
</tr>
</thead>
<tbody>
<tr>
<td>An information and technology asset refresh, removal, and replacement management program has been documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>Senior management is required to create and implement a computer and technology asset management program.</td>
<td>The Reprivata solution enables secure management of critical technology assets that are members of the CoT by ensuring security management and tracking of those assets.</td>
</tr>
<tr>
<td>Senior management is required to create and implement a computer and technology asset management program.</td>
<td>The Reprivata solution enables secure management of critical technology assets that are members of the CoT by ensuring security management and tracking of those assets.</td>
<td>Configuration management databases can provide device inventory reporting. Asset tracking and reporting software can enhance technology asset management and replacement.</td>
</tr>
<tr>
<td>A data leakage assessment and protection management program has been documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>Reprivata CoT implements multi-level encryption for data at rest. Reprivata CoT requires end users and attached devices to connect through the use of encrypted virtual private network tunnels. Reprivata CoT can integrate active network threat monitoring, identification, and mitigation both inside and outside the CoT through its</td>
<td>Compliant with NIST CSF</td>
</tr>
<tr>
<td>v. PR.DS-5: Protections against data leaks are implemented</td>
<td>vi. PR.DS-6: Protections against data leakage are implemented</td>
<td>vii. PR.DS-7: Protections against data leakage are implemented</td>
</tr>
<tr>
<td>A data leakage assessment and protection management program has been documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>Reprivata CoT implements multi-level encryption for data at rest. Reprivata CoT requires end users and attached devices to connect through the use of encrypted virtual private network tunnels. Reprivata CoT can integrate active network threat monitoring, identification, and mitigation both inside and outside the CoT through its</td>
<td>Compliant with NIST CSF</td>
</tr>
<tr>
<td>A data leakage assessment and protection management program has been documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>Reprivata CoT implements multi-level encryption for data at rest. Reprivata CoT requires end users and attached devices to connect through the use of encrypted virtual private network tunnels. Reprivata CoT can integrate active network threat monitoring, identification, and mitigation both inside and outside the CoT through its</td>
<td>Compliant with NIST CSF</td>
</tr>
<tr>
<td></td>
<td>PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity</td>
<td>A file and system integrity assessment and protection program has been documented, implemented, and communicated to both internal and external stakeholders.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td></td>
<td>PR.DS-7: The development and testing environment(s) are separate from the production environment</td>
<td>Separate production, quality assurance, and testing environments have been implemented and their usage requirements have been communicated to both internal and external stakeholders.</td>
</tr>
<tr>
<td></td>
<td>PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity</td>
<td>A file and system integrity assessment and protection program has been documented, implemented, and communicated to both internal and external stakeholders.</td>
</tr>
<tr>
<td></td>
<td>Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of</td>
<td></td>
</tr>
</tbody>
</table>

113
i. **PR.IP-1**: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)

A minimum baseline configuration program for all technology assets has been documented, implemented, and communicated to both internal and external stakeholders.

**Base configuration of Reprivata CoT solution are included in the software documentation prepared for the UL certification process.**

Compliant with NIST CSF

Control implemented in the Reprivata solution

Configuration management databases can provide device configuration reporting on compliance with internal and external configuration standards.

---

ii. **PR.IP-2**: A System Development Life Cycle to manage systems is implemented

A systems development, assessment, and management life cycle for all technology assets has been documented, implemented, and communicated to both internal and external stakeholders.

**Technology Management is required to create and implement a Systems Development Life Cycle for the software design, creation, and implementation functions.**

The Reprivata solution enables the segregation and segmentation of application systems under development to support a Systems Development Life Cycle (SDLC).

Companies can get assistance in creating and implementing a SDLC from software programming and development training companies as well as from external consulting firms.

---

iii. **PR.IP-3**: Configuration change control processes are in place

A change control management program for all technology assets has been documented, implemented, and communicated to both internal and external stakeholders.

**Technology Management is required to create and implement a change management and control function for tracking changes to applications, devices, and other technology assets.**

The Reprivata solution enables secure collaboration and data sharing by key management stakeholders when discussing the changes made to applications and other technologies managed by the company.

Change management software can provide this type of functionality.

---

iv. **PR.IP-4**: Backups of information are conducted, maintained, and tested

A backup and data archival management program for all technology assets has been documented, implemented, and communicated to both internal and external stakeholders.

**Technology management is required to create and implement a data backup and archival program to ensure the security of critical business data.**

The Reprivata solution enables critical data protection within the CoT so it can be archived and secured by the backup program.

Backup and data archival software can provide this type of functionality.

---

v. **PR.IP-5**: Policy and regulations

Physical security policies and Senior management is

The Reprivata solution enables Physical security management
<table>
<thead>
<tr>
<th></th>
<th>PR.IP-6: Data is destroyed according to policy</th>
<th>PR.IP-7: Protection processes are improved</th>
<th>PR.IP-8: Effectiveness of protection technologies is shared</th>
</tr>
</thead>
<tbody>
<tr>
<td>regarding the physical operating environment for organizational assets are met</td>
<td>procedures for ensuring security of facilities have been documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>required to create and implement a physical security management program that is consistent with the organization’s risk posture.</td>
<td>secure collaboration and data sharing by key management stakeholders when discussing the risks associated with the physical security management program.</td>
</tr>
<tr>
<td>vi.</td>
<td>Senior management is required to create and implement a data destruction program that is consistent with the organization’s risk posture.</td>
<td>The Reprivata solution enables secure collaboration and data sharing by key management stakeholders when discussing the risks associated with data destruction.</td>
<td>Data destruction programs can be created and evaluated by external consulting firms that specialize in physical security.</td>
</tr>
<tr>
<td>vii.</td>
<td>Information and technology asset protection policies and procedures are regularly reviewed to determine what enhancements are required to meet cybersecurity risk management requirements and any enhancements are documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>When included in the Reprivata Master Agreement, this enables compliance with NIST CSF.</td>
<td>The Reprivata Master Agreement is a legal document that can be customized as required by the CoT owner so the appropriate security, operational, and policy requirements are in place for all CoT users.</td>
</tr>
<tr>
<td>viii.</td>
<td>The use and management of information and technology protection controls have been documented, implemented.</td>
<td>When included in the Reprivata Master Agreement, this enables compliance with NIST CSF.</td>
<td>The Reprivata Master Agreements are designed to be easily updated by internal and/or external legal counsel as required by the CoT owner.</td>
</tr>
<tr>
<td>ix.</td>
<td>PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed</td>
<td>Cybersecurity event response and recovery programs for information and technology assets have been documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>When included in the Reprivata Master Agreement, this enables compliance with NIST CSF.</td>
</tr>
<tr>
<td>x.</td>
<td>PR.IP-10: Response and recovery plans are tested</td>
<td>Cybersecurity event response and recovery programs for information and technology assets have been tested and the results of those tests have been communicated to both internal and external stakeholders.</td>
<td>When included in the Reprivata Master Agreement, this enables compliance with NIST CSF.</td>
</tr>
<tr>
<td>xi.</td>
<td>PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening policies and procedures have been documented, implemented.)</td>
<td>Personnel screening policies and procedures have been documented, implemented.</td>
<td>Senior management is required to create and implement a personnel screening</td>
</tr>
<tr>
<td>xi. PR.IP-12: A vulnerability management plan is developed and implemented</td>
<td>A cybersecurity vulnerability risk assessment, testing, and management program for information and technology assets has been documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>Senior management is required to create and implement a system and application vulnerability management program that is consistent with the organization’s risk posture.</td>
<td>The Reprivata solution enables secure collaboration and data sharing by key management stakeholders when discussing the risks associated with the company’s personnel.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>e. Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.</td>
<td>A maintenance and management program for technology assets has been documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>Senior management is required to create and implement a device maintenance program that is consistent with the organization’s risk posture.</td>
<td>The Reprivata solution enables secure collaboration and data sharing by key management stakeholders when discussing the risks associated with device maintenance and repair.</td>
</tr>
<tr>
<td>i. PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools</td>
<td>A maintenance and management program for technology assets has been documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>Senior management is required to create and implement a device maintenance program that is consistent with the organization’s risk posture.</td>
<td>The Reprivata solution enables secure collaboration and data sharing by key management stakeholders when discussing the risks associated with device maintenance and repair.</td>
</tr>
<tr>
<td>ii. PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access</td>
<td>User and service remote access to technology assets have been documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>Senior management is required to create and implement a device maintenance program, to include remote access to those devices where applicable, that is consistent with the organization’s risk posture.</td>
<td>The Reprivata solution enables secure collaboration and data sharing by key management stakeholders when discussing the risks associated with remote device maintenance and repair.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>organization’s risk posture.</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>f.</td>
<td>Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>i.</td>
<td>PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy</td>
<td>Audit logs and records related to access and management of information and technology assets have been documented, implemented, and reviewed on a regular basis to help detect and prevent cybersecurity events.</td>
<td>When included in the Reprivata Master Agreement, this enables compliance with NIST CSF.</td>
</tr>
<tr>
<td>ii.</td>
<td>PR.PT-2: Removable media is protected and its use restricted according to policy</td>
<td>A data leakage assessment and protection management program has been documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>Technology management is required to create and implement a data leakage and loss prevention program, to include control over removable media, where applicable, that is consistent with the organization’s risk posture.</td>
</tr>
<tr>
<td>iii.</td>
<td>PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities</td>
<td>Technology asset roles and service requirements that ensure that the only minimum necessary configuration of technology</td>
<td>Base configuration of Reprivata CoT solution are included in the software documentation prepared for the UL certification process.</td>
</tr>
<tr>
<td>3. Detect – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events. (18 key controls)</td>
<td>assets is in place have been documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>evaluated by external consulting firms.</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>iv. PR.PT-4: Communication s and control networks are protected</td>
<td>Network architecture requirements to implement secure network design and connectivity have been documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>Reprivata CoT can integrate active network threat monitoring, identification, and mitigation both inside and outside the CoT through its Global Threat Intelligence capabilities.</td>
<td>Compliant with NIST CSF Control implemented in the Reprivata solution</td>
</tr>
<tr>
<td>v. PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations</td>
<td>Network architecture requirements to implement secure network design and connectivity have been documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>Technology management is required to create and implement network resiliency program that is consistent with the organization’s risk posture.</td>
<td>The Reprivata solution enables secure collaboration and data sharing by key management stakeholders when discussing the risks associated with network resiliency.</td>
</tr>
<tr>
<td>a. Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.</td>
<td>Network data flows and communication paths have been mapped for critical business functions. Data flows are included in all</td>
<td></td>
<td></td>
</tr>
<tr>
<td>i. DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>ii. <strong>DE.AE-2:</strong> Detected events are analyzed to understand attack targets and methods</td>
<td><strong>Global Threat Intelligence capabilities.</strong></td>
<td>well as by external consulting firms.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Reprivata CoT can integrate active network threat monitoring, identification, and mitigation both inside and outside the CoT through its Global Threat Intelligence capabilities.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Compliant with NIST CSF Control implemented in the Reprivata solution</strong></td>
<td><strong>Network data flow and event information reviews can be performed and evaluated by network threat management software companies as well as by external consulting firms.</strong></td>
<td></td>
</tr>
<tr>
<td>iii. <strong>DE.AE-3:</strong> Event data are collected and correlated from multiple sources and sensors</td>
<td><strong>Reprivata CoT can integrate active network threat monitoring, identification, and mitigation both inside and outside the CoT through its Global Threat Intelligence capabilities.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Compliant with NIST CSF Control implemented in the Reprivata solution</strong></td>
<td><strong>Network data flow and event information reviews can be performed and evaluated by network threat and incident management software companies as well as by external consulting firms.</strong></td>
<td></td>
</tr>
<tr>
<td>iv. <strong>DE.AE-4:</strong> Impact of events is determined</td>
<td><strong>Reprivata CoT can integrate active network threat monitoring, identification, and mitigation both inside and outside the CoT through its Global Threat Intelligence capabilities.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Compliant with NIST CSF Control implemented in the Reprivata solution</strong></td>
<td><strong>Network data flow and event information impact assessments can be performed and evaluated by network threat and incident management software companies as well as by external consulting firms.</strong></td>
<td></td>
</tr>
<tr>
<td>v. <strong>DE.AE-5:</strong> Incident alert thresholds are established</td>
<td><strong>Reprivata CoT can integrate active network threat monitoring, identification, and mitigation both inside and outside the CoT through its Global Threat Intelligence capabilities.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Compliant with NIST CSF Control implemented in the Reprivata solution</strong></td>
<td><strong>Network data flow and event information alerts and assessments can be performed and evaluated by network threat and incident management software companies as well as by external consulting firms.</strong></td>
<td></td>
</tr>
<tr>
<td>b. Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>i. DE.CM-1: The network is monitored to detect potential cybersecurity events</td>
<td>A network monitoring program for technology assets has been documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>Reprivata CoT can integrate active network threat monitoring, identification, and mitigation both inside and outside the CoT through its Global Threat Intelligence capabilities.</td>
<td>Compliant with NIST CSF Control implemented in the Reprivata solution.</td>
</tr>
<tr>
<td>ii. DE.CM-2: The physical environment is monitored to detect potential cybersecurity events</td>
<td>A physical security monitoring program has been documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>Senior management is required to create and implement a physical security monitoring program that is consistent with the organization’s risk posture.</td>
<td>The Reprivata solution enables secure collaboration and data sharing by key management stakeholders when discussing the risks associated with physical security monitoring.</td>
</tr>
<tr>
<td>iii. DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events</td>
<td>A personnel monitoring program for the use of information and technology assets has been documented, implemented, and</td>
<td>Reprivata CoT can integrate active network threat monitoring, identification, and mitigation both inside and outside the CoT through its</td>
<td>Compliant with NIST CSF Control implemented in the Reprivata solution.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Physical security monitoring programs can be created and evaluated by external consulting firms that specialize in physical security.</td>
</tr>
<tr>
<td>iv. DE.CM-4: Malicious code is detected</td>
<td>A secure coding and testing program for systems development has been documented, implemented, and communicated to both internal and external stakeholders. An anti-virus and malware protection program has been documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>Technology management is required to create and implement a malicious code detection and prevention program, to include secure coding training, where applicable, that is consistent with the organization’s risk posture.</td>
<td>The Reprivata solution enables secure collaboration and data sharing by key management stakeholders when discussing the risks malicious code detection and prevention. Malicious code detection and prevention and secure coding training programs can be created and evaluated by security application testing software companies, as well as by external consulting firms.</td>
</tr>
<tr>
<td>v. DE.CM-5: Unauthorized mobile code is detected</td>
<td>A secure coding and testing program for systems development has been documented, implemented, and communicated to both internal and external stakeholders. An anti-virus and malware protection program has been documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>Technology management is required to create and implement a malicious code detection and prevention program, to include secure coding training, where applicable, that is consistent with the organization’s risk posture.</td>
<td>The Reprivata solution enables secure collaboration and data sharing by key management stakeholders when discussing the risks malicious code detection and prevention. Malicious code detection and prevention and secure coding training programs can be created and evaluated by security application testing software companies, as well as by external consulting firms.</td>
</tr>
<tr>
<td>vi. DE.CM-6: External service provider activity is monitored to</td>
<td>An external support and service provider monitoring program for the Reprivata CoT can integrate active network threat monitoring, Compliant with NIST CSF Control implemented in</td>
<td>Network data flow and event monitoring alerts and assessments can be</td>
<td></td>
</tr>
<tr>
<td>c. Detection Processes (DE.DP): Detection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>vii. DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed</td>
<td>A personnel monitoring program for the use of information and technology assets has been documented, implemented, and communicated to both internal and external stakeholders. An external support and service provider monitoring program for the use of information and technology assets has been documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>Reprivata CoT can integrate active network threat monitoring, identification, and mitigation both inside and outside the CoT through its Global Threat Intelligence capabilities. Reprivata CoT enables access control permissions for end users and attached devices through the use of certificates. Reprivata CoT requires end users and attached devices to connect through the use of encrypted virtual private network tunnels.</td>
<td>Compliant with NIST CSF Control implemented in the Reprivata solution</td>
</tr>
<tr>
<td>viii. DE.CM-8: Vulnerability scans are performed</td>
<td>A vulnerability management, assessment, and remediation process is documented, implemented, and implemented. Senior management is required to create and implement a system and application vulnerability management program that is consistent with the organization’s risk posture.</td>
<td>The Reprivata solution enables secure collaboration and data sharing by key management stakeholders when discussing the risks associated with system and application vulnerabilities.</td>
<td>Vulnerability management programs can be created and evaluated by vulnerability management software firms as well as by external consulting firms that specialize in data management.</td>
</tr>
<tr>
<td>i. DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability</td>
<td>User identities, roles, permissions, and access requirements for personnel monitoring access and security events related to technology assets have been documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>When included in the Reprivata Master Agreement, this enables compliance with NIST CSF.</td>
<td>The Reprivata solution enables secure collaboration and communication of internal and external parties and their responsibilities for reviewing audit logs related to activities of CoT members.</td>
</tr>
<tr>
<td>ii. DE.DP-2: Detection activities comply with all applicable requirements</td>
<td>A threat intelligence assessment and review process is documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>Reprivata CoT technology designed and implemented to comply with NIST CSF.</td>
<td>Compliant with NIST CSF Control implemented in the Reprivata solution</td>
</tr>
<tr>
<td>iii. DE.DP-3: Detection processes are tested</td>
<td>The threat intelligence assessment and review process is tested regularly and the results of such tests are communicated to both internal and external stakeholders.</td>
<td>Reprivata CoT can integrate active network threat monitoring, identification, and mitigation both inside and outside the CoT through its Global Threat Intelligence capabilities. When included in the Reprivata Master Agreement, this enables compliance with NIST CSF.</td>
<td>Compliant with NIST CSF Control implemented in the Reprivata solution</td>
</tr>
<tr>
<td>iv. DE.DP-4: Event detection</td>
<td>A threat intelligence</td>
<td>When included in the Reprivata solution</td>
<td>The Reprivata solution enables</td>
</tr>
<tr>
<td>v.</td>
<td>DE.DP.5: Detection processes are continuously improved</td>
<td>Cybersecurity event detection policies and procedures for monitoring Information and technology assets are regularly reviewed to determine what enhancements are required to meet cybersecurity risk management requirements and any enhancements are documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>When included in the Reprivata Master Agreement, this enables compliance with NIST CSF.</td>
</tr>
</tbody>
</table>

<p>| 4. | Respond – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident. (19 key controls) | a. Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies). | | | |</p>
<table>
<thead>
<tr>
<th>i. RS.CO-1: Personnel know their roles and order of operations when a response is needed</th>
<th>Tactical and strategic responsibilities for responding to cybersecurity incidents have been documented, implemented, and communicated that information to the appropriate stakeholders.</th>
<th><strong>Senior management is required to create and implement an incident response plan that outlines the personnel roles and responsibilities and is consistent with the organization’s risk posture.</strong></th>
<th>The Reprivata solution enables secure collaboration and data sharing by key management stakeholders when discussing the risks associated with security incidents and events.</th>
<th>Incident response programs can be created and evaluated by external consulting firms that specialize in incident response.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ii. RS.CO-2: Incidents are reported consistent with established criteria</td>
<td>Incident reporting procedures and personnel assignments have been documented, implemented, and communicated that information to the appropriate stakeholders.</td>
<td>When included in the Reprivata Master Agreement, this enables compliance with NIST CSF.</td>
<td>The Reprivata solution enables secure collaboration and communication of internal and external parties and their responsibilities for security event detection and reporting related to activities of CoT members.</td>
<td>The Master Agreements are designed to be easily updated by internal and/or external legal counsel as required by the CoT owner. All CoT users are required to sign the Master Agreement before they can utilize the data sharing and collaboration capabilities of the CoT.</td>
</tr>
<tr>
<td>iii. RS.CO-3: Information is shared consistent with response plans</td>
<td>Incident reporting procedures and personnel assignments have been documented, implemented, and communicated that information to both internal and external stakeholders.</td>
<td>When included in the Reprivata Master Agreement, this enables compliance with NIST CSF.</td>
<td>The Reprivata solution enables secure collaboration and communication of internal and external parties and their responsibilities for security event detection and information sharing related to activities of CoT members.</td>
<td>The Master Agreements are designed to be easily updated by internal and/or external legal counsel as required by the CoT owner. All CoT users are required to sign the Master Agreement before they can utilize the data sharing and collaboration capabilities of the CoT.</td>
</tr>
<tr>
<td>iv. RS.CO-4: Coordination with</td>
<td>Incident reporting procedures and</td>
<td>When included in the Reprivata Master</td>
<td>The Reprivata solution enables secure</td>
<td>The Master Agreements are designed to be</td>
</tr>
<tr>
<td><strong>v. RS.CO-5:</strong> Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness</td>
<td>Incident reporting procedures with suppliers and other third parties have been documented, implemented, and communicated that information to both internal and external stakeholders.</td>
<td><strong>When included in the Reprivata Master Agreement, this enables compliance with NIST CSF.</strong></td>
<td>The Reprivata solution enables secure collaboration and communication of internal and external parties and their responsibilities for security event detection and information sharing related to activities of CoT members.</td>
<td>The Master Agreements are designed to be easily updated by internal and/or external legal counsel as required by the CoT owner. All CoT users are required to sign the Master Agreement before they can utilize the data sharing and collaboration capabilities of the CoT.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>b. Analysis (RS.AN):</strong> Analysis is conducted to ensure effective response and support recovery activities.</td>
<td>Cybersecurity event detection and investigation policies and procedures for monitoring Information and technology assets are documented, implemented, and communicated that information to both internal and external stakeholders.</td>
<td><strong>When included in the Reprivata Master Agreement, this enables compliance with NIST CSF.</strong></td>
<td>The Reprivata solution enables secure collaboration and communication of internal and external parties and their responsibilities for notifying relevant parties about security event detection related to activities of CoT members.</td>
<td>The Master Agreements are designed to be easily updated by internal and/or external legal counsel as required by the CoT owner. All CoT users are required to sign the Master Agreement before they can utilize the data sharing and collaboration capabilities of the CoT.</td>
</tr>
<tr>
<td><strong>i. RS.AN-1:</strong> Notifications from detection systems are investigated</td>
<td>Stakeholders occur consistent with response plans personnel assignments have been documented, implemented, and communicated that information to both internal and external stakeholders.</td>
<td>Agreement, this enables compliance with NIST CSF.</td>
<td>The Reprivata solution enables secure collaboration and communication of internal and external parties and their responsibilities for improving security event detection processes related to activities of CoT members.</td>
<td>The Master Agreements are designed to be easily updated by internal and/or external legal counsel as required by the CoT owner. All CoT users are required to sign the Master Agreement before they can utilize the data sharing and collaboration capabilities of the CoT.</td>
</tr>
<tr>
<td>ii. RS.AN-2: The impact of the incident is understood</td>
<td>Cybersecurity event evaluation policies and procedures for monitoring Information and technology assets are documented, implemented, and communicated that information to both internal and external stakeholders.</td>
<td>Senior management is required to create and implement incident response impact analyses that determine how incidents affect the organization and are consistent with the organization’s risk posture.</td>
<td>The Reprivata solution enables secure collaboration and data sharing by key management stakeholders when discussing the risks associated with the impacts of security incidents and events.</td>
<td>Incident response impact analyses can be performed and evaluated by external consulting firms that specialize in incident response metrics.</td>
</tr>
<tr>
<td>iii. RS.AN-3: Forensics are performed</td>
<td>Cybersecurity event investigation policies and procedures for monitoring Information and technology assets are documented, implemented, and communicated that information to both internal and external stakeholders.</td>
<td>When included in the Reprivata Master Agreement, this enables compliance with NIST CSF.</td>
<td>The Reprivata solution enables secure collaboration and communication of internal and external parties and their responsibilities for analyzing the numbers, types, impacts, and response results of security events related to activities of CoT members.</td>
<td>The Master Agreements are designed to be easily updated by internal and/or external legal counsel as required by the CoT owner. All CoT users are required to sign the Master Agreement before they can utilize the data sharing and collaboration capabilities of the CoT.</td>
</tr>
<tr>
<td>iv. RS.AN-4: Incidents are categorized consistent with response plans</td>
<td>Cybersecurity event evaluation policies and procedures for monitoring Information and technology assets are consistent with technology and operational risk management requirement and are documented, implemented, and communicated that information to both internal</td>
<td>When included in the Reprivata Master Agreement, this enables compliance with NIST CSF.</td>
<td>The Reprivata solution enables secure collaboration and communication of internal and external parties and their responsibilities for analyzing the numbers, types, impacts, and response results of security events related to activities of CoT members.</td>
<td>The Master Agreements are designed to be easily updated by internal and/or external legal counsel as required by the CoT owner. All CoT users are required to sign the Master Agreement before they can utilize the data sharing and collaboration capabilities of the CoT.</td>
</tr>
<tr>
<td></td>
<td>v. RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal testing, security bulletins, or security researchers)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Processes for utilizing externally-sourced vulnerability information to improve the vulnerability management program are documented, implemented, and communicated that information to both internal and external stakeholders.</td>
<td>When included in the Reprivata Master Agreement, this enables compliance with NIST CSF.</td>
<td>The Reprivata solution enables secure collaboration and communication of internal and external parties and their responsibilities for analyzing the numbers, types, impacts, and response results of security vulnerabilities related to activities of CoT members.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The Master Agreements are designed to be easily updated by internal and/or external legal counsel as required by the CoT owner.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>All CoT users are required to sign the Master Agreement before they can utilize the data sharing and collaboration capabilities of the CoT.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c. Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>i. RS.MI-1: Incidents are contained</td>
<td>Cybersecurity event response and recovery programs for information and technology assets have been documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>Reprivata CoT can integrate active network threat monitoring, identification, and mitigation both inside and outside the CoT through its Global Threat Intelligence capabilities.</td>
<td>Compliant with NIST CSF Control implemented in the Reprivata solution</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Incident response containment and mitigation reviews can be performed and evaluated by external consulting firms that specialize in incident response management.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ii. RS.MI-2: Incidents are mitigated</td>
<td>Cybersecurity event response and recovery programs for information and technology assets have been documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>Reprivata CoT can integrate active network threat monitoring, identification, and mitigation both inside and outside the CoT through its Global Threat Intelligence capabilities.</td>
<td>Compliant with NIST CSF Control implemented in the Reprivata solution</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Incident response containment and mitigation reviews can be performed and evaluated by external consulting firms that specialize in incident response management.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>iii. RS.MI-3: Newly identified</td>
<td>Cybersecurity event response and recovery</td>
<td>Reprivata CoT can integrate active network</td>
<td>Compliant with NIST CSF</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Vulnerability containment and mitigation</td>
<td></td>
</tr>
<tr>
<td>Vulnerabilities are mitigated or documented as accepted risks</td>
<td>Threat monitoring, identification, and mitigation both inside and outside the CoT through its Global Threat Intelligence capabilities.</td>
<td>Control implemented in the Reprivata solution</td>
<td>reviews can be performed and evaluated by external consulting firms that specialize in vulnerability management.</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>Programs for information and technology assets have been documented, implemented, and communicated to both internal and external stakeholders. Cybersecurity event evaluation policies and procedures for monitoring Information and technology assets are consistent with technology and operational risk management requirement and are documented, implemented, and communicated that information to both internal and external stakeholders.</td>
<td>Outcomes from cybersecurity event response and recovery exercises and incidents for information and technology assets have been documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>When included in the Reprivata Master Agreement, this enables compliance with NIST CSF.</td>
<td>The Reprivata solution enables secure collaboration and communication of internal and external parties and their responsibilities for analyzing the numbers, types, impacts, and response results of security incidents related to activities of CoT members.</td>
<td>The Master Agreements are designed to be easily updated by internal and/or external legal counsel as required by the CoT owner. All CoT users are required to sign the Master Agreement before they can utilize the data sharing and collaboration capabilities of the CoT.</td>
</tr>
<tr>
<td>d. Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>i. RS.IM-1: Response plans incorporate lessons learned</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ii. RS.IM-2: Response strategies are updated</td>
<td>Cybersecurity event detection policies and procedures for monitoring Information and technology assets are regularly reviewed to determine what enhancements are required to meet cybersecurity risk management requirements and any enhancements are documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>When included in the Reprivata Master Agreement, this enables compliance with NIST CSF.</td>
<td>The Reprivata solution enables secure collaboration and communication of internal and external parties and their responsibilities for updating incident response plans related to activities of CoT members.</td>
</tr>
</tbody>
</table>

| 5. | Recover – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident. (6 key controls) | | | | |

| a. | Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents. | | | | |

<p>| i. | RC.RP-1: Recovery plan is executed during or after a cybersecurity incident | Cybersecurity event response and recovery programs for information and technology assets have been documented, implemented, and communicated to both internal and external stakeholders. | When included in the Reprivata Master Agreement, this enables compliance with NIST CSF. | The Reprivata solution enables secure collaboration and communication of internal and external parties and their responsibilities for updating incident recovery plans related to | The Master Agreements are designed to be easily updated by internal and/or external legal counsel as required by the CoT owner. All CoT users are required to sign the Master Agreement before they can utilize the data sharing and collaboration capabilities of the CoT. |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th>activities of CoT members.</th>
<th>utilize the data sharing and collaboration capabilities of the CoT.</th>
</tr>
</thead>
<tbody>
<tr>
<td>b.</td>
<td>Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>i.</td>
<td>RC.IM-1: Recovery plans incorporate lessons learned</td>
<td>Cybersecurity event detection policies and procedures for monitoring Information and technology assets are regularly reviewed to determine what enhancements are required to meet cybersecurity risk management requirements and any enhancements are documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>When included in the Reprivata Master Agreement, this enables compliance with NIST CSF.</td>
</tr>
<tr>
<td>ii.</td>
<td>RC.IM-2: Recovery strategies are updated</td>
<td>Cybersecurity event detection policies and procedures for monitoring Information and technology assets are regularly reviewed to determine what enhancements are required to meet cybersecurity risk management requirements and any enhancements are documented, implemented, and communicated to</td>
<td>When included in the Reprivata Master Agreement, this enables compliance with NIST CSF.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>c. Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>i. RC.CO-1: Public relations are managed</td>
<td>Responsibilities for managing messaging and other communications during a cybersecurity event to ensure all appropriate parties are updated on a timely basis are documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>Senior management is required to create and implement public relations and reputation management programs that are consistent with the organization’s risk posture.</td>
<td></td>
</tr>
<tr>
<td>ii. RC.CO-2: Reputation is repaired after an incident</td>
<td>Procedures for managing reputational risks related to cybersecurity events for information and technology assets have been documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>Senior management is required to create and implement public relations and reputation management programs that are consistent with the organization’s risk posture.</td>
<td></td>
</tr>
<tr>
<td>iii. RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams</td>
<td>Cybersecurity event response and recovery programs for information and technology assets have been documented, implemented, and communicated to both internal and external stakeholders.</td>
<td>When included in the Reprivata Master Agreement, this enables compliance with NIST CSF.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Reprivata solution enables secure collaboration and data sharing by key management stakeholders when discussing the risks associated with managing the corporate reputation.</td>
<td>The Reprivata solution enables secure collaboration and data sharing by key management stakeholders when discussing the risks associated with managing the corporate reputation.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Public relation communication and impact analyses can be performed and evaluated by external consulting firms that specialize in corporate public relations management.</td>
<td>Reputational impact reviews can be performed and evaluated by external consulting firms that specialize in corporate reputation management.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Master Agreements are designed to be easily updated by internal and/or external legal counsel as required by the CoT owner.</td>
<td>The Master Agreements are designed to be easily updated by internal and/or external legal counsel as required by the CoT owner.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>All CoT users are required to sign the Master Agreement.</td>
<td>All CoT users are required to sign the Master Agreement.</td>
<td></td>
</tr>
</tbody>
</table>
Artifcat 3 – Recommendations for Enhancement of Reprivata Master Agreements for Implementing Community of Trust (CoT) Risk Management Solution

The Reprivata Master Agreements were created to provide a Community of Trust (CoT) owner with the ability to create business rules of engagement to govern the relationships and collaboration with those internal and external stakeholders that are part of the CoT network solution.

While the current Master agreements provide a good starting point for setting up these business rules and relationships, the researcher evaluated specific key controls in the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) version 1.1. After reviewing the key controls in the five Functional security areas covered by the NIST CSF, the following controls were identified as potential enhancements to the Master Agreements that would help enable cybersecurity maturity and improvement programs for all the CoT participants.

1. **NIST CSF Functional Area – Identify (ID) Controls Language to Include:**

<table>
<thead>
<tr>
<th>NIST CSF Key Controls</th>
<th>Rationale for inclusion in Master Agreements</th>
</tr>
</thead>
<tbody>
<tr>
<td>• ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.</td>
<td>• Documenting the cybersecurity roles and responsibilities of internal stakeholders and third parties, such as suppliers and business partners, enables the CoT owner establish access control, incident response reporting, user collaboration, and data sharing processes to meet the needs of the CoT as a whole.</td>
</tr>
<tr>
<td>• ID.BE-1: The organization’s role in the supply chain is identified and communicated</td>
<td>• The cybersecurity roles for event identification for the organization and its third parties like suppliers and partners that are CoT users should be legally defined in writing to make sure all obligations are understood.</td>
</tr>
<tr>
<td>• ID.GV-1: Organizational cybersecurity policy is established and communicated</td>
<td>• Compliance to cybersecurity policies by stakeholders should be specific and with assessment and reporting requirements for all CoT users.</td>
</tr>
<tr>
<td>• ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners</td>
<td>• Documentation of cybersecurity roles for all internal and external stakeholders should be documented and mutual collaboration and data sharing responsibilities outlined in writing for all CoT users.</td>
</tr>
<tr>
<td>• ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed</td>
<td>• Legal and regulatory compliance cybersecurity requirements should be clearly documented for all CoT users.</td>
</tr>
</tbody>
</table>
- ID.RA-6: Risk responses are identified and prioritized.
- Risk management collaboration requirements for all CoT users should be clearly defined and stakeholder obligations for risk review are documented.

- ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process
- Risk management and review obligations for third parties should be legally binding when collaborating in the CoT.

- ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization’s cybersecurity program and Cyber Supply Chain Risk Management Plan.
- Third party contracts should include provisions for measuring and managing cybersecurity risks and implementing cybersecurity controls for controlling related risks.

- ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.
- Cybersecurity audit and assessment provisions should be clearly documented and assessment reporting requirements specified.

- ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers
- Cybersecurity recovery and response plans should be required of all CoT users.

2. NIST CSF Functional Area – Protect (PR) Controls Language to Include:

<table>
<thead>
<tr>
<th>NIST CSF Key Controls</th>
<th>Rationale for Inclusion in Master Agreements</th>
</tr>
</thead>
<tbody>
<tr>
<td>• PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities</td>
<td>• See ID.AM-6 and ID.GV-2, which outline the rationale for inclusion in Master Agreements.</td>
</tr>
<tr>
<td>• PR.IP-7: Protection processes are improved</td>
<td>• Cybersecurity protection management process improvement and maturity requirements are documented for all CoT users.</td>
</tr>
<tr>
<td>• PR.IP-8: Effectiveness of protection technologies is shared</td>
<td>• Collaboration requirements for assisting CoT users to enhance their cybersecurity protection technologies and processes are documented.</td>
</tr>
<tr>
<td>• PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed</td>
<td>• Requirements for CoT users to implement cybersecurity response plans are documented.</td>
</tr>
<tr>
<td>• PR.IP-10: Response and recovery plans are tested</td>
<td>• Requirements for CoT users to share the results of cybersecurity response plan tests are documented.</td>
</tr>
<tr>
<td>• PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy</td>
<td>• Requirements for CoT users to implement technology logs on all networks, servers, and other devices and that the logs are handled and reviewed as part of a log management process are documented.</td>
</tr>
</tbody>
</table>
3. NIST CSF Functional Area – Detect (DE) Controls Language to Include:

<table>
<thead>
<tr>
<th>NIST CSF Key Controls</th>
<th>Rationale for Inclusion in Master Agreements</th>
</tr>
</thead>
<tbody>
<tr>
<td>• DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability</td>
<td>• The cybersecurity roles for event detection for the organization and its third parties like suppliers and partners that are CoT users should be legally defined in writing to make sure all obligations are understood.</td>
</tr>
<tr>
<td>• DE.DP-3: Detection processes are tested</td>
<td>• Requirements for CoT users to share the results of detection process and procedure tests are documented.</td>
</tr>
<tr>
<td>• DE.DP-4: Event detection information is communicated</td>
<td>• Documenting the cybersecurity event detection responsibilities of internal stakeholders and third parties, such as suppliers and business partners, enables the CoT owner to establish access control, incident response reporting, user collaboration, and data sharing processes to meet the needs of the CoT as a whole.</td>
</tr>
<tr>
<td>• DE.DP-5: Detection processes are continuously improved</td>
<td>• Cybersecurity detection process improvement and maturity requirements are documented for all CoT users.</td>
</tr>
</tbody>
</table>

4. NIST CSF Functional Area – Respond (RS) Controls Language to Include:

<table>
<thead>
<tr>
<th>NIST CSF Key Controls</th>
<th>Rationale for Inclusion in Master Agreements</th>
</tr>
</thead>
<tbody>
<tr>
<td>• RS.CO-2: Incidents are reported consistent with established criteria</td>
<td>• Requirements for CoT users to share the results of cybersecurity incidents and under what situations are documented.</td>
</tr>
<tr>
<td>• RS.CO-3: Information is shared consistent with response plans</td>
<td>• Collaboration requirements between CoT users on cybersecurity incidents are documented.</td>
</tr>
<tr>
<td>• RS.CO-4: Coordination with stakeholders occurs consistent with response plans</td>
<td>• How and when CoT users are required to work together on cybersecurity incidents are documented.</td>
</tr>
<tr>
<td>• RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness</td>
<td>• How the CoT will be used by users to share critical response and remediation data related to cybersecurity events is documented.</td>
</tr>
<tr>
<td>• RS.AN-1: Notifications from detection systems are investigated</td>
<td>• Responsibilities for CoT users to investigate and report cybersecurity events are documented.</td>
</tr>
<tr>
<td>• RS.AN-3: Forensics are performed</td>
<td>• Requirements for CoT users to utilize forensic tools and share the results of those investigations are documented.</td>
</tr>
<tr>
<td>NIST CSF Key Controls</td>
<td>Rationale for Inclusion in Master Agreements</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>RS.AN-4: Incidents are categorized consistent with response plans</td>
<td>How cybersecurity events are classified and what responses are required by specific event classes are documented.</td>
</tr>
<tr>
<td>RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)</td>
<td>Requirements for CoT users to utilize cybersecurity threat and vulnerability resources, such as research organizations or vendors, as part of their vulnerability management programs are documented.</td>
</tr>
<tr>
<td>RS.IM-1: Response plans incorporate lessons learned</td>
<td>Requirements to CoT users to share post mortem analyses of the results from cybersecurity response exercises or tests are documented.</td>
</tr>
<tr>
<td>RS.IM-2: Response strategies are updated</td>
<td>Requirements for CoT users to keep their cybersecurity response plans up-to-date are documented.</td>
</tr>
</tbody>
</table>

5. NIST CSF Functional Area – Recover (RC) Controls Language to Include:

<table>
<thead>
<tr>
<th>NIST CSF Key Controls</th>
<th>Rationale for Inclusion in Master Agreements</th>
</tr>
</thead>
<tbody>
<tr>
<td>RC.RP-1: Recovery plan is executed during or after a cybersecurity incident</td>
<td>The requirements for CoT users to utilize cybersecurity incident response plans when events are detected are documented.</td>
</tr>
<tr>
<td>RC.IM-1: Recovery plans incorporate lessons learned</td>
<td>See RS.IM-1, which outlines the rationale for inclusion in Master Agreements.</td>
</tr>
<tr>
<td>RC.IM-2: Recovery strategies are updated</td>
<td>See RS.IM-2, which outlines the rationale for inclusion in Master Agreements.</td>
</tr>
<tr>
<td>RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams</td>
<td>Documenting the cybersecurity event response responsibilities and activities of internal stakeholders and third parties, such as suppliers and business partners, enables the CoT owner to establish access control, incident response reporting, user collaboration, and data sharing processes to meet the needs of the CoT as a whole.</td>
</tr>
</tbody>
</table>
Artifact 4 – Definitions, Acronyms, and Abbreviations [from Reprivata Community of Trust documentation and NIST Glossary of Information Security Terms, 2018]

Access Control – The process of permitting or restricting access to applications at a granular level, such as per-user, per-group, and per-resources.

CA – A certificate authority (CA) is a trusted entity that issues electronic documents that verify a digital entity's identity on the Internet. The electronic documents, which are called digital certificates, are an essential part of secure communication and play an important part in the Public Key Infrastructure.

CoT – A Community of Trust (CoT) is a group of like-minded users and service providers that have created a private network using a combination of IPSec, TLS, and multiple encryption algorithms to protect the members of the Community of Trust. This can be accomplished by legally bounding a private network’s owner and members with a cyber demarcation point for end users, employees, and all interconnected third parties.

Collective Defense – A security arrangement in which each entity in the system accepts that the security of one is the concern of all, and therefore commits to a collective response to threats and breaches of the system.

Community Owner – Within a Community of Trust, the Community Owner is the entity that initiates the CoT with other third parties through the use of standardized service agreements and encrypted communications technologies that allows the members of the CoT to collaborate securely.

Community Services – Community Owner provides a suite of services to the End User. This allows an End User to establish a User Profile consisting of the End User’s PII and/or Non-PII, which is warehoused in the Central database for each Community. The End User determines what PII and/or Non-PII it is willing to share (if any) with other Members, providers, third parties, or selected third parties when using IPES. In some instances, an End User may be able to receive payment for sharing PII and/or Non-PII with certain third parties or receive subsidies for third-party provided IPES.

Defense in Depth – The coordinated use of multiple security controls and countermeasures to protect the integrity of a company’s information assets.

ECDH – Elliptic Curve Diffie–Hellman is an anonymous key agreement protocol that allows two parties, each having an elliptic curve public–private key pair, to establish a shared secret over an insecure channel. This shared secret may be directly used as a key, or to derive another key which can then be used to encrypt subsequent communications using a symmetric key cipher.


End User – An individual that uses “Community provided IPES Services” delivered via a Community Owner.

Interconnection Security Agreement – A document that regulates security-relevant aspects of an intended connection between an agency and an external system. It regulates the security interface between any two systems operating under two different distinct authorities. It includes a variety of descriptive,
technical, procedural, and planning information. It is usually preceded by a formal MOA/MOU that
defines high-level roles and responsibilities in management of a cross-domain connection.

**IPES** – Internet Protocol Enabled Services (IPES) means any services provided to the End User through a
Community Inter-connected Network or the Internet. Examples include web browsing, online gaming,
online educational games or instruction, Voice over Internet Protocol services, e-mail, texting or
messaging, and any other service delivered through a web browser, mobile app or through the use of a
personal computer, laptop, or a mobile device and the Internet.

**IPSec** – Internet Protocol Security is a protocol suite for securing IP communications by
authenticating and encrypting each IP packet of a communication session. IPSec includes protocols for
establishing mutual authentication between agents at the beginning of the session and negotiation of
cryptographic keys to be used during the session. IPSec can be used in protecting data flows between a
pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a
security gateway and a host (network-to-host). IPSec uses cryptographic security services to protect
communications over IP networks. IPSec supports network-level peer authentication, data origin
authentication, data integrity, data confidentiality (encryption), and replay protection. IPSec is an end-
to-end security scheme operating in the Internet Layer of the Internet Protocol Suite, while some other
Internet security systems in widespread use, such as Transport Layer Security (TLS) and Secure Shell
(SSH), operate in the upper layers at Application layer. Hence, only IPSec protects any application
traffic over an IP network. Applications can be automatically secured by IPSec at the IP layer.

**Master Agreement** – These agreements require members of a Community of Trust (CoT) to organize
and deploy their independent Communities of Trust using a process that will facilitate the reliable
implementation of security policy and technical interoperability between independent Communities of
Trusts and interconnected entities.

**Non-PII** – Non-personally identifiable information (non-PII) is data associated with an End User that is
not specific enough to identify an End User individually. Examples include: fist name, zip code, or
birthday.

**NSA Suite B** – A set of cryptographic algorithms promulgated by the National Security Agency as
part of its Cryptographic Modernization Program. It is to serve as an interoperable cryptographic base
for both unclassified information and most classified information. Suite B was announced on 16
February 2005. Suite B can be used to protect foreign releasable information, US Only information,
and Sensitive Compartmented Information (SCI).

**PII** – Personally Identifiable Information (PII) is defined as any information about an End User
maintained by an agency, including (1) any information that can be used to distinguish or trace an End
User’s identity, such as name, social security number, date and place of birth, mother’s maiden name, or
biometric records; and (2) any other information that is linked or linkable to an End User, such as
medical, educational, financial, and employment information. Examples include, but are not limited to
full name, mother’s maiden name, government issued identification numbers like social security number,
passport number, driver’s license number or financial account or credit card numbers, or biometric data
like fingerprint, handwriting, etc.

**PKI** – A Public Key Infrastructure (PKI) is a set of hardware, software, people, policies, and
procedures needed to create, manage, distribute, use, store, and revoke digital certificates. In
cryptography, a PKI is an arrangement that binds public keys with respective user identities by means
of a certificate authority (CA).
Private Communications CoT (PC CoT) Software CA – The Certificate Authority inside the IPSEC tunnel. This is to authenticate the keys used to initiate the IPSEC tunnel. TLS has another key and it uses the same Private Communications CoT (PC CoT) software CA inside the IPSEC tunnel. To encrypt packets, a ZRTP application layer for TwoFish encryption algorithm is implemented.

RFC 1918 – The document that helped create the standards by which networking equipment assigns IP addresses in a private network. A private network can use a single public IP address. The RFC reserves the following ranges of IP addresses that cannot be routed on the Internet: 10.0.0.0 - 10.255.255.255 (10/8 prefix).

Risk – A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (1) the adverse impacts that would arise if the circumstance or event occurs; and (2) the likelihood of occurrence.

Risk Adaptive Access Control – Access privileges are granted based on the combination of a user’s identity, mission need, and the level of security risk that exists between the system being accessed and a user. Risk Adaptive Access Control will use security metrics, such as the strength of the authentication method, the level of assurance of the session connection between the system and a user, and the physical location of a user, to make its risk determination.

Risk Analysis – The process of identifying the risks to system security and determining the likelihood of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management is synonymous with risk assessment.

Risk Assessment – The process of identifying the risks to system security and determining the likelihood of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management is synonymous with risk assessment.

SIP – The Session Initiation Protocol is a communications protocol for signaling and controlling multimedia communication sessions. The most common applications of SIP are in Internet telephony for voice and video calls, as well as instant messaging all over IP networks.

SRTP – A Real-time Transport Protocol (RTP) profile intended to provide encryption, message authentication and integrity, and replay attack protection to the RTP data in audio-visual applications.

Threat – Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.

Threat Analysis – The examination of threat sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment.

Threat Assessment – The process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat.

Third Party Testing – Independent testing by an organization that was not involved in the design and implementation of the object being tested (e.g., a system or device) and is not intended as the eventual user of that object.
**TLS** – Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols designed to provide communications security over a computer network.

**Tunnel Mode** – One of two modes of transport supported by IPSec. This mode encrypts the entire packet including the header, it then provides the packet with a new header.

**TwoFish** – A symmetric key block cipher with a block size of 128 bits and key sizes up to 256 bits.

**User Profile** – Means the End User’s PII that the End User populates in the Central Privacy Authority provided by a Community Owner database and the rules defining when certain subsets of PII may be disclosed to third party IPES providers, *i.e.*, any IPES that is not a Community Owner.

**Vulnerability** – A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

**Vulnerability Analysis** – The systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

**Vulnerability Assessment** – The formal description and evaluation of the vulnerabilities in an information system.

**ZRTP** – A cryptographic key-agreement protocol to negotiate the keys for encryption between two end points in a Voice over Internet Protocol (VoIP) phone telephony call based on the Real-time Transport Protocol. It uses Diffie–Hellman key exchange and the Secure Real-time Transport Protocol (SRTP) for encryption.
To whom it may concern:

In my capacity as Editor-in-Chief of the *Muma Business Review* and *Muma Case Review*, I am writing this letter to confirm that both journals allow the authors to retain the copyright under a Creative Commons BY-NC license. As a result, authors can reprint their work wherever it is desired provided they acknowledge the source.

In the case of Ed Fulford, he has two Muma Case review articles that have been accepted for publication, proofed and formatted accordingly. He can therefore include them as part of his dissertation.

If you have further questions, feel free to contact me by email or at my home (813-994-4511).

Yours Sincerely,

T. Gradon Gill, Professor and Academic Director
Doctor of Business Administration program
groundon@usf.edu
IMPLEMENTING A CYBERSECURITY COMMUNITY OF TRUST: REPRIVATA SEeks AN “EARLY ADOPTER”

Reprivata developed a cybersecurity solution which could fundamentally change how companies create private, trust-based interconnections with their third-party business partners. Now, how do they attract the right “early adopter” to implement it?

John “Tripp” Hardy, the Chief Executive Officer (CEO) of Reprivata, sat in the San Francisco airport waiting for his flight to Washington, DC. Tripp, an investment banker by training, had been approached by one of Reprivata’s founders, Scott Yeager, to join the young company and help it to productize its cybersecurity solution.

Tripp and Scott had known each other since 2014. Scott was a visionary in the networking field who had helped start Metropolitan Area Exchange - East (MAE-East), one of the first commercial and largest of the Internet Exchange Points (IXPs). By 2013, Scott, along with his partner David Cox (an expert in both networking and application development), had turned their talents to developing a cybersecurity solution to allow companies to build a Community of Trust (CoT). This CoT would enable the members to communicate and collaborate securely amongst themselves on business and cybersecurity issues. While addressing this problem, Scott and David had come to three conclusions. First, a technology was needed that would allow the businesses to securely communicate and collaborate over the Internet. Second, a generally-accepted cybersecurity standard was required to provide a methodology for businesses to mature their cybersecurity programs. Third, the business network connections between companies needed to be governed by legal language, similar to the Master Service Agreements that had been written in the 1990s for IXPs and ISPs to link their networks. With those three design elements in his mind, Scott and David had set to work.

After years in development, Scott had shown Tripp the initial solution. Excited about its potential and the opportunity to work with Scott to build Reprivata, Tripp decided it was the right time to join the company and help it take the CoT solution to market. As Tripp first began to present the Reprivata CoT solution to his Financial Services contacts, there was a significant amount of interest in the CoT concept. However, none of the organizations were willing to implement Reprivata’s solution and show its worth. As Tripp
reviewed his upcoming schedule of meetings in Washington, DC, he thought, “How do we overcome just one organization’s reluctance when they clearly see the value of our solution?”

**The Cybersecurity Problem Spaces**

Cybersecurity professionals had been diligently working to better understand the natures and impacts of the cyber risks. However, the funding and staffing of these efforts needed to change. The adoption of more pre-emptive and responsive global, national, and business cyber risk management behaviors lagged the number of cyber risks being identified by cyber risk managers—and being exploited by bad actors. Additionally, the number of effective cybersecurity solutions that could fix more than very specific technical vulnerabilities had not increased to a point that interrelated problem spaces could be addressed. The more aggressive implementation of effective risk measurement and mitigation programs, based on cybersecurity standards and methodologies, seemed likely to improve the management and assessment of cybersecurity problem and solution spaces. At this time, however, cybersecurity programs had not matured at a pace that could keep up with the numbers and varieties of cyber risks (Fulford, 2017).

The problem spaces that cybersecurity practitioners had been required to address were very similar, regardless of the industry or location they worked in. These problem spaces included:

- The Global Cybersecurity Problem Space
- The Government Cybersecurity Problem Space
- The Business Cybersecurity Problem Space
- The Cybersecurity Standard Problem Space

More details on the current and emerging issues related to these cybersecurity problem spaces can be found in “A Note on the Cybersecurity Problem Space in 2018”.

**The Drive Toward Broader Cybersecurity Collaboration and Maturity**

Cybersecurity practitioners had not been alone in working through the difficulties of achieving and protecting information sharing between diverse groups. A similar lack of communication had long plagued law enforcement.

**Building Communities of Trust Initiative**

As a means of addressing this, in 2010, the United States Department of Justice (U.S. Justice) launched The Building Communities of Trust (BCOT) Initiative, which focused on developing trust between law enforcement, fusion centers, and the communities they served, particularly immigrant and minority communities, so that crime and terrorism could be addressed. This initiative had been administered primarily by the Nationwide Suspicious Activity Reporting (SAR) Initiative (abbreviated as NSI). The NSI program provided law enforcement with a capacity for gathering, documenting, processing, analyzing, and sharing suspicious activity reports about behaviors that had a potential nexus to terrorism. The NSI recognized that each community’s collaboration to gather and share this type of information was critically important in the prevention of crime and terrorism, since law enforcement agencies were dependent on community members to report suspicious activity information to state, local, tribal, and territorial (SLTT) law enforcement officers. To help ensure that this reporting was taking place, it was essential that law enforcement and community members had strong, trusting relationships. As these relationships were developed and maintained, members of the community would be more likely to report crime and suspicious activities, which was the reason the NSI had worked with partners at the federal, state, and local levels—including United States Attorney’s Offices, public and privacy advocacy groups,
religious and faith leaders, and a diverse group of local community members—to implement the Building Communities of Trust initiative (Wasserman, 2010).

**Executive Order 13636: Improving National Cybersecurity Maturity**

On February of 2013, President Obama issued Executive Order (EO) 13636: Improving Critical Infrastructure Cybersecurity, which was aimed at strengthening the cybersecurity of the critical national infrastructure. Later in 2013, Edward Snowden, a National Security Agency (NSA) contractor with high level security clearance, copied and leaked classified information from the NSA without authorization. Snowden’s disclosures revealed numerous global surveillance programs, many run by the NSA and other intelligence agencies with the cooperation of telecommunication companies and European governments. Soon after that event, there was significant pressure from the White House to create a cybersecurity framework to meet the directives in the Executive Order. This led to NIST and industry participants, beginning work on what was known as the Cybersecurity Framework (CSF).

While the EO did not mandate the use of any particular cybersecurity standard, it did set in motion the joint government and industry collaboration that led to the development of the initial version of the CSF, which was released in 2014. As stated in the EO (House, 2013):

> It is the policy of the United States to enhance the security and resilience of the Nation’s critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards.

**Selected Cybersecurity Management Standards**

While Reprivata was researching the various cybersecurity standards to determine which one to base their solution on, two serious issues were noted: first, there were many cybersecurity standards already published and second, no two industries agreed on which of the standards took precedence. Seeing the White House’s directions on improving cybersecurity maturity as an opportunity, Scott and David had set out in search of that overarching cybersecurity standard that would embrace the concepts of collaboration and cyber maturity as guiding principles. Some of their findings were instrumental in leading them to a most interesting conclusion (see Exhibit 1).

**Industry-Specific Standards**

There were also a number of industry-specific standards such as the Payment Card Industry Data Security Standard (PCI DSS) for companies that process, transmit, and store credit card data, the North American Energy Reliability Corporation Critical Information Protection (NERC CIP) guidelines for the bulk power energy companies in North America, and the Health Information Portability and Accountability Act (HIPAA) Security Rule, which established national security standards to protect individuals’ electronic personal health information that was created, received, used, or maintained by a covered Healthcare entity. Adopting one of the more general industry-specific security frameworks above could be complementary to other similar methodologies. However, many companies were required to be compliant with several of these standards and to submit themselves to regular compliance assessments, so it became increasingly difficult for them to be fully compliant with all of the specific standards or regulations at any one time. Also, none of these regulations or standards required companies to measure the maturity of
their cybersecurity program, nor did they require companies to collaborate on solving mutually-held security issues.

**International Standards Organization 27000 Standards**

As perhaps the most widely known family of information security standards, the International Standards Organization (ISO) 27000 framework was a very mature one that focused on creating and enhancing an organization’s Information Security Management System (ISMS). The framework also provided requirements under which an ISMS could be audited and certified by an ISO registrar. At the time of this case study, the ISO 27000 series of standards included 45 individual guidelines across the functional areas that made up a company’s security program. As a very comprehensive set of standards, the ISO 27000 guidelines could be used across a wide range of industries and types of business environments. ISO 27000 was the security equivalent of the ISO 9000 quality management standards used by manufacturers to demonstrate operational excellence. Because ISO 27000 was very established with cybersecurity practitioners compared to other standards, countries had used it as a basis to create regulatory compliance requirements and related guidance about security as well as directions to organizations on how extend the use of the ISO standards in their enterprise risk management practices and programs. Because of the expanding scope of the ISO 27000 series of guidelines, an ISMS could be difficult to measure and challenging to get certified. As such, many smaller companies were reluctant to expend the necessary resources required to achieve accreditation, so there was a widely-held perception that ISO 27000 could be difficult to deploy and maintain. As with industry-specific standards, ISO 27000 did not require companies to measure the maturity of their cybersecurity programs, nor did it dictate that companies collaborated to work on the security challenges they faced.

**National Institute of Standards and Technology Cybersecurity Framework**

The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) had much in common with the NIST 800 series information security guidelines, which were created about 20 years ago and had evolved over that time. The original NIST 800 series of guidelines provided a starting point for other information security guidelines and methodologies. The CSF, as an extension of the original NIST 800 series, leveraged a wide range of information security standards and leading practices. While the NIST CSF was created recently relative to other information security standards, it was designed to be very comprehensive and was targeted for use by large enterprises, as well as those companies with business connections in the United States. It was found to be easily aligned to the ISO standards, such as ISO 27000 and ISO 9000. It was the only information security framework that defined specific measurements whereby companies could demonstrate their cybersecurity maturity. It also required companies to collaborate with their third-party business partners in cybersecurity issues that affected their business relationships. Because the NIST CSF contained a lot of very practical guidance, it could be adapted to smaller and non-US organizations without a great deal of effort and expense.

**General Data Protection Regulation**

The General Data Protection Regulation (GDPR) was adopted in 2016 as a personal data protection and privacy regulation in European Union (EU) law. GDPR was created as a new set of data security and management guidelines and was designed to give EU citizens more control over their personal data and to hold businesses that manage and process this personal data accountable for implementing and strengthening the security and privacy controls over this data. GDPR was aimed at simplifying the regulatory environment for businesses, so both citizens and businesses in the EU could benefit from the products and services offered by the growth of the digital economy. GDPR also addressed the movement,
export, and exfiltration of personally identifiable data outside of the EU and the European Economic Area (EEA). The EEA covered the EU countries of Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, and Sweden. The EEA also included Iceland, Liechtenstein and Norway, which allowed these countries to be part of the EU’s single market for trade and economic development. While Switzerland was neither an EU nor EEA member, it was part of the single EEA market. The United Kingdom, as part of its plans to leave the EU in 2019, implemented the Data Protection Act of 2018, which contained equivalent data security and privacy protection language to GDPR. As of 2019, the United Kingdom would become a third country for the purposes of the transfer of personal data outside the EU, which could require the EU to review the United Kingdom’s data protection framework to determine if the data security and privacy controls were equivalent to those required by GDPR.

Reprivata

David, I was there at MAE-East when we made up the rules for how companies interconnect to others on the Internet. Why don’t we just make up the rules now around how businesses collaborate privately and securely to meet our own needs? – Scott Yeager to David Cox (2013)

David Cox was a talented technologist who saw an increasingly serious security problem facing companies that did business over the Internet: there were few, if any, applications that were flexible and secure enough to enable interconnected businesses to communicate and collaborate together. In 2012, David began to build the first version of an encrypted collaboration and communication application. David’s solution was based on open source software and included the highest level of encryption available at the time.

The cybersecurity communication and collaboration application that David developed utilized a multi-layered encryption software approach. This created a secure encrypted connection while cloaking the accessibility of the edge devices connected to a defined set of network end points that required the ability to pass secured traffic through those interconnections. Traffic from all the edge devices inside the secured connections were policed, and anomalous or suspicious traffic flows were captured and stored in the Central Privacy Authority Intrusion Database (CPAID), which was a key component of the functionality of the application.

In 2013, David contacted Scott Yeager, who he had known from Scott’s work on MAE-East. After some discussion, David and Scott formed Reprivata to productize David’s application. Reprivata’s name was based on the Latin phrase “Res privata” which means private business. One of Reprivata’s strategic goals was to “re-privatize” how companies did business over the Internet.

David originally funded the start-up through his company MiMTiD, and Scott provided additional capital to begin work on creating the Reprivata CoT solution. Once Scott understood that the solution David had developed allowed a company to build secure private networks using the software, Scott realized that the problem of enabling secure communication and collaboration between connected business partners could be solved one private network at a time. He discussed this with David and they decided to create new rules around how a private network could become cyber secure and have interconnected entities play by the same set of rules.

One of the ideas for this new cybersecurity solution was to bound the edges of a private network, as built out of the software, with a new set of interconnection contracts, similar to those used in the early days of
the internet between IXPs, ISPs, and CDNs. Scott believed that creating these new legal demarcation points for a private network and bounding those demarcations for the network’s end users, employees and interconnected third parties would be the most prudent and successful approach.

Reprivata Community of Trust Conceptual Model
The Reprivata Community of Trust (CoT) Conceptual Model (see Exhibit 2) was developed to articulate the interactions of elements that influence successful cybersecurity CoT implementations using the Reprivata cybersecurity risk management solution. These elements helped determine and, in some cases, manage the resources within these projects as part of the overarching corporate business strategy which determined the cyber risk posture, and how that posture could be managed and measured. These were two distinct groups of elements: one composed of the cybersecurity frameworks and legal documents that provide structure to the CoT, and one that constituted the Internal and External Stakeholders of the CoT.

The CoT Governance element (see Exhibit 2) was based on the Master Agreements that are executed between the overall Community of Trust’s Internal Stakeholders and its External Stakeholders. The Master Agreements provided the legal guidance over its governance functions that the CoT members would utilize in interactions between themselves and were the basis for the on-going collaboration activities in the CoT. The IT risk assessment processes were defined, outlining the risk management requirements for each member, such as purchasing cyber insurance and the how the cybersecurity program maturity of the members would be evaluated against the CSF security controls framework. The contractual obligations of each member regarding their IT compliance, and how the technical and business interconnections were to be managed were also specified by this element. Finally, the risk metrics were defined, outlining the risk measurements and the frequency of reporting those measurements were stipulated.

The CoT Risk Management Strategy and the CoT Governance elements of the model augmented each other as required to implement the selected Cyber Risk Management methodology (see Exhibit 2). The provisions of CoT Governance empowered the company’s ability to measure risk and show the company’s overall risk posture was being managed effectively. If risk management requirements were changed, the company typically would reassess its risk posture and determine how any such changes would impact its operational stance within the CoT and under the conditions of the Master Agreement. In this way, the Proposed Conceptual Model would demonstrate that any changes in one or both of these elements would typically require a business to re-assess its cyber risk posture with respect to the overall change in its technology footprint it used to support the CoT and its strategic and operational decisions and initiatives. The effects on the corporation’s internal technology environment were ways that these elements influenced the direction and scope of the cyber-related management programs. These influencers provided both an internal and external context on how the CoT Risk Management Strategy was implemented, how its success would be measured, and how it would be evaluated against CoT Governance requirements (such as internal or external audits, external risk assessments, or regulatory reviews). These evaluations would influence the CoT Risk Management Strategy implementation by providing the legal and cybersecurity orientation for enhancing cyber risk management, as well as the key performance metrics and reporting required by management.

Defining the CoT Rules of Engagement
During his days in networking, Scott had worked on these types of legal and regulatory issues with Andy Lipman, a partner at the law firm of Morgan Lewis and one of the leading attorneys in the area of Telecommunications law. Earlier in his career, Andy had heavily influenced the interconnection language
that was incorporated in the Telecommunication Act of 1996. Scott and David went to Andy and discussed their proposed business model with him. Scott had been part of developing some of the original commercial rules of the Internet connectivity with Rick Adams, the founder of UUNET, and several other Internet pioneers. Scott thought that Reprivata could make up new rules for a private network and these new rules could be enforced by the owner of the private network without asking permission of any jurisdictional entity.

Andy found Scott’s approach to be unique and forward-thinking, and strongly encouraged David and Scott to continue maturing their solution. In addition, Andy confirmed to Scott and David that they could make up new rules for a private network and those rules could also be used to enforce cybersecurity maturity requirements via Master Agreements, using the notion of a demarcation point in the Master Agreement to create and enforce those rules across all interconnected users, employees and third parties.

Andy then reviewed Reprivata’s concepts and software design and was impressed by the ways the company was solving for some of the more impactful security issues facing interconnected companies doing business over the Internet. On his recommendation, Reprivata filed for two patents. The first one was for an Encrypted Community of Trust (CoT) using the Central Privacy Authority to warehouse data owned by End Users and to facilitate management of encryption keys controlled by the CoT owner. The second patent was for an Advertising Compliance Authority (ACA), based on functionality created through the use of Reprivata’s software.

Reprivata’s Cybersecurity Community of Trust

As Reprivata performed its early research into the key functionality required by its cyber risk management solution, Scott and David found that the Community of Trust (CoT) model, similar to one implemented by the U.S. Justice’s BCOT initiative (even though they had no knowledge of the U.S. Justice’s efforts at the time Reprivata was developing its strategy), was key to the broad-based adoption and success of the solution with clients. They then designed Reprivata’s CoT approach around several core concepts:

- The CoT members were required to meet a minimum cybersecurity standard that was uniform, repeatable, easy-to-understand, and measure.

- The CoT was implemented as a private network between its members with demarcation points documented both technically and legally through Master Agreements (standardized contracts) at the employee, end-user and independent third party (I3P) levels.

- The CoT agreements were required its members to obtain cyber insurance as a form of risk management and third-party monitoring control.

- The CoT agreements were defining the limits on liability for its members in case of a data breach or other major cybersecurity event.

- The CoT agreements were both defining and enabling secure information sharing and collaboration between the members on cybersecurity issues that impacted the community as a whole.

- The CoT should be able to provide members with the ability to monitor cybersecurity events related to the members’ business activities across servers, applications, devices, and data flows from all interconnected third parties. This notion was called a Community of Trust Privacy
Authority (CoTPA) and was defined and described in all the CoT Master Agreements, so information could be legally collected and agreed to by all parties in the private network. It allowed Personally Identifiable Information (PII) and other sensitive business data to be stored by the CoT owner as the custodian of the data, and also to be held privately in the CoTPA Privacy Authority and managed on behalf of all the members of the CoT in a secure and legal manner.

- The CoTPA also helped the CoT owner to collect data about the activities of members inside the private CoT and use it as needed to protect the overall cybersecurity posture and maturity of the CoT in a manner that protected all parties. This enabled the CoT owner to share data between themselves and the interconnected third parties, so that they could collaborate about cyber maturity matters across the demarcation set out in the Master Agreement.

**Selecting the Right Cybersecurity Standard**

With these guiding principles established and the initial technology platform designed, the Reprivata team began to review the different cybersecurity standards and frameworks that were used in various industries. One of the first things they learned was that there were actually many cybersecurity methodologies to choose from. After reviewing a number of the most widely used ones, the team realized that none of the standards met their needs. There seemed to be no good way to proceed at this point. The other standards, though comprehensive, did not facilitate collaboration between companies to solve mutually-held cybersecurity issues—a key part of the Reprivata’s technology and process-oriented solution. Then, Scott and David evaluated the NIST CSF and they recognized that they had found the right cybersecurity standard for their needs.

This decision was also influenced by David’s personal experiences. After returning from a trip abroad as part of a cybersecurity project team he initiated, David told Scott they should use the NIST CSF. The NIST CSF was a comprehensive set of cybersecurity requirements based on 23 control categories across 5 cybersecurity functional areas (see Exhibit 3). As such, the cybersecurity requirements offered a comprehensive framework on which companies could construct their cybersecurity programs. Also, the NIST CSF included a cybersecurity program maturity model that gave companies several ways to determine how they were performing as they implemented the framework’s security controls (see Exhibit 4).

To David’s way of thinking, a standard with cybersecurity and risk management control guidelines developed by industry, NIST, and other government agencies charged with protecting the U.S. critical national infrastructure was a match to Reprivata’s guiding principles. When Scott heard David’s reasoning, he agreed that the NIST CFF was the standard to use in the Master Agreements to help ensure consistent cybersecurity maturity across the clients’ private networks. Now, with the NIST CSF providing direction on how to implement and mature a cybersecurity program, the team incorporated these security controls and maturity requirements into the Master Agreements.

**Illustrating the Reprivata CoT Solution Space**

A shared framework such as the NIST CSF focused on the rapid identification and remediation of security control gaps relative to a generally accepted cybersecurity standard, as opposed to having to regularly recertify their cybersecurity posture to multiple information infrastructure protection guidelines or, at worst, against ad hoc security requirements. Reprivata realized that this approach to closing security control weaknesses required not only collaboration between the members of a CoT, but a very robust cybersecurity program as well.
Of particular interest for Reprivata and its CoT solution was NIST CSF Tier 3 (see Exhibit 4). NIST CSF Tier 3 required the organizations that adopted the framework as part of building a trusted commercial relationship with their interconnected business partners to implement cyber risk initiatives as part of an on-going cybersecurity process improvement program. Each organization in the CoT was required to incorporate cyber risk into its enterprise risk management policies and program. This enterprise approach to cyber risk meant that an organization-wide approach to managing cybersecurity risk could be adopted and applied to both internal and external stakeholders. By including stakeholders in the cybersecurity program, the company then began to recognize and document the interdependencies on third parties and the increased need for collaboration between all key stakeholders.

Another benefit of NIST CSF Tier 3 to the organization was that it could be readily mapped to government, international, and industry-specific standards, such as the ISO 27000 security requirements and others that are applicable to Financial Services, Healthcare, and other industries that needed to evaluate the cyber risks in their business and technology strategies.

In practice, NIST CSF Tier 3 could be implemented as a private network with demarcation points defined both technically and legally through the adoption of standardized Master Agreements or similar contracts at the employee, end-user and information and infrastructure protection levels. Such contracts defined limits of liability for all parties, in accordance to their technology footprint, interconnections, and identified risks. Another advantage of the standardized contracts was that risk mitigation measures such as cyber insurance were more easily integrated into the business partners’ overall cybersecurity posture as a form of mutually-approved risk management and third-party monitoring. By having such defined risk mechanisms, secure information sharing and broader collaboration between the partners was facilitated.

There were other advantages for the company that was the leader or “owner” of the CoT. The organization's cyber risk management practices had to be formally approved and expressed as policy, with appropriate NIST CSF key performance indicators included in enterprise risk management reporting. Under the framework, organizational cybersecurity practices were required to be regularly updated, based on the application of risk treatments. These treatments were defined in response to changes in internal and external strategic and tactical requirements as well as the changing threat and technology landscapes the business faced.

The proposed cyber risk evaluation solution artifacts were designed to be easily integrated into a company’s enterprise risk management program. The artifacts allowed the rapid application of tools and techniques such as gap analyses, compliance testing, threat surveillance, and incident response postmortems that were critical to the success of understanding cyber risks as they were discovered and assessed. These methods were consistent to the NIST CSF framework and could be shared with business partners to support their cybersecurity postures as well as to enable more thorough government and industry compliance reviews of security controls, which increased collaboration and cooperation between the partners.

In 2015, Scott had briefed the United States Department of the Treasury (U.S. Treasury) about the business interconnection issue. At the same time, he had started educating the American Bankers Association (ABA) about the NISF CSF and cyber insurance approach to enterprise risk management and cybersecurity maturity which were incorporated in the Master Agreements. Scott also contacted the National Association of Insurance Commissioners (NAIC) as an organization as well as each state insurance commissioner and met with them about the Reprivata CoT Master Agreements and related Reprivata’s decision to seek Underwriter’s Laboratory’s new cybersecurity certification on the Reprivata software suite. This was a major effort and took until the end of 2016.
The First Independently Certified Cybersecurity Software

In 2016, Reprivata decided to take a bold step. It approached the UL to certify the CoT solution under UL’s recently created Cybersecurity Assurance Program (UL CAP). Scott and David met members of the UL CAP program at a trade show and, after that meeting, Scott decided to engage UL CAP to perform a certification assessment on the Reprivata software. If the assessment was successful, Reprivata’s solution would be the first cybersecurity software to be certified under the UL CAP program. Reprivata knew that the UL certification could be a marketing advantage for them with potential clients, especially as a new company. Also, because UL certifications were well-respected in the insurance industry, a UL endorsement like this potentially helped clients get cyber insurance to cover losses from cyberattacks and to assist with getting the appropriate levels of coverage required to remediate from these events. Pursuing the UL CAP certification was truly an opportunity for Reprivata to distinguish itself as a leader in the development of robust cybersecurity solutions.

UL CAP assessors applied the UL 2900 series of cybersecurity standards to the certification process. To ensure David met the demanding certification requirements, Scott reached out to Nathan Gregory, who Scott had known from the MAE-East days of the 1990s. Initially, Nathan worked on documenting the software according to the UL CAP guidelines. As the certification process went on, Nathan also assisted David and the UL security testers to make sure that all issues found by the cybersecurity testing and evaluations were cleared. Nathan provided the UL testers with guidance on the software’s architecture functionality as they assessed the solution’s potential vulnerabilities and weaknesses in order to verify that its internal security capabilities and controls were implemented as designed.

Over several months, UL’s security assessment team tested the CoT solution and tried to break its cryptographic security, but was not able to do so. The application testing protocol was extensive, covering such areas as malformed input testing, software composition and runtime analysis, malware analysis, and penetration testing.

Finally, in July of 2016, the UL certification was awarded. Now, Reprivata had an innovative cybersecurity product that was the very first to be UL certified. Scott and David continued to look for an early adopter, but no company would commit to implement the product yet.

More details on the Reprivata software and CoT solution are included in the Technical Note accompanying this case study.

A Unique Opportunity to Test the Solution

Then, Reprivata got its first big break. David's work on the early versions of the Reprivata software for the intelligence community made him more well-known in the cybersecurity field. As a result, David was approached by the Kingdom of Saudi Arabia to implement some technology and policy approaches in the Kingdom’s cybersecurity operations center. As David started his work, it became clear implementing a CoT based on Reprivata’s software suite would be extremely useful to the program he was leading. While this was a chance to implement the Reprivata software in a cyber environment where it would be severely tested because of the number of attacks it would likely face, the agreement with the Saudi government also required David to be onsite in Saudi Arabia to manage the system. After much debate, Scott and David agreed that this was a situation they could not pass up. However, it also meant that finding a client in the United States would take more time in light of David’s move to Saudi Arabia to run the project.
Searching for an Early Adopter

In 2017, Scott and David discussed Reprivata’s future. They decided that it was time to find a hands-on Chief Executive Officer (CEO) who had deep connections with corporate executives and industry leaders and could help the company begin a more extensive marketing campaign to formally launch the CoT solution in the United States. Tripp Hardy was recruited to fill this role and the search for an “early adopter” in the United States accelerated.

Tripp’s first major act as CEO was to work with Scott and David on a white paper that addressed a U.S. Treasury request for comments on the cybersecurity issues related to business interconnections. This paper was the first time that Reprivata had presented anything in the public domain regarding the idea of a CoT with Master Agreements being a solution for companies that wanted to set boundaries on the risks inherent with third party business interconnections to their corporate networks. The paper, in addition to the awarding of the UL certification of their software, was a catalyst for Reprivata being asked to participate in meetings with several government agencies and also attracted the interest of companies in industries like Banking and Insurance. The pursuit of an early adopter was on in earnest.

In March of 2018, Tripp, Scott, and other members of the Reprivata senior management team had been engaged by potential clients at several high profile Federal and state government agencies in an attempt to sign up the first adopter of their cybersecurity solution. As a result of these meetings, the company had been asked to come to Washington, DC to perform a technical demonstration of a client-provided use case. Part of this demonstration included the integration of Microsoft Office into the solution to facilitate workgroup collaboration. Of particular interest to this agency was the concept of a “micro CoT”, essentially a small (10 to 100 user) private collaboration group that helped their internal departments change security and risk management behaviors immediately. This CoT implementation strategy also had the ability to make those groups compliant with NIST CSF Tier 3 requirements, taking small careful steps to raise the cyber maturity of the entire agency. However, this demonstration was not without potential obstacles and risks.

Challenges

There was growing acknowledgement within the company that additional development would be required before a client would agree to implement their solution. After they reviewed the company’s finances, Tripp and Scott met with the other members of the Reprivata management team to discuss next steps. Reprivata was a self-funded company; Scott and David had originally funded the startup and Tripp had become an investor when he joined the company. When he joined Reprivata as Chief Technology Officer, Nathan Gregory had also self-funded his considerable participation in Reprivata, especially his earlier efforts in documenting the Reprivata software suite as part of the requirements to obtain the UL certification for the solution and assisting the UL security testers during the software’s certification assessment.

Now, the company was at a crossroads and looking at potential funding options because of the number of organizations that had started taking interest in Reprivata and its solution. While all the management team had agreed that remaining self-funded was the direction they wanted to go, they also understood that they did not have sufficient funds to maintain the current capital burn rate. The management team had unanimously decided that the integration project for the upcoming product demonstration was critical to the future of the company, even though it would require them to spend most of the available cash. Without a real client yet, could Reprivata remain self-funded, complete the software integration,
successfully demonstrate the solution with a client use case, and close the deal—or would it need to pursue other funding options to execute its plans?

The Reprivata CoT solution had been built using open source software, tools, and applications for voice, video, file transfer, and text communications. Initially, no development efforts had been focused on integrating collaborative and office support tools like Microsoft Office and SharePoint into the solution. All the clients the Reprivata team had spoken with had either asked about or required this type of integration to enhance the solution’s native collaborative capabilities. While the Reprivata team believed that this integration would be feasible, they had become more certain that this functionality was a requirement for the solution’s broader acceptance in the market. Would a client want to risk implementing the Reprivata CoT solution without these capabilities?

Reprivata had not been able to pay sales people to reach out to potential clients. Scott, from his prior entrepreneurial experience, had a list of sales and marketing contacts that, after hearing about the Reprivata CoT solution, were eager to help set up meetings with potential clients. At this time, after 3 years with no real successes in finding an early adopter for the solution, the number of people who were either still interested in or willing to help Reprivata gain entrée into the right cybersecurity executives and influencers in companies had shrunk. Without sales people who considered taking a risk and continued to assist Reprivata without a near-term opportunity for compensation, could Reprivata find the next adopter of its solution—and the one after that—if they successfully closed the deal with their current client after the upcoming demonstration?

David Cox had been overseas for over a year. At a very critical time for Reprivata, with a software integration project and system demonstration in the offing for its first real U.S. client, David was supporting the cybersecurity operations center for the Kingdom of Saudi Arabia. The Kingdom of Saudi Arabia was a major target for cyberattacks and other security events. David was tapped for this project because of the development of a security and threat intelligence system that was part of the Reprivata CoT solution. With the technical abilities to help complete the integration project on time, David’s assistance ensured the client demonstration would be successful. Unfortunately, the client demonstration would soon be held in Washington, DC. Would David be able to participate in the preparation of the client demonstration and then be able to attend the formal presentation with the client in Washington, DC?

**Decisions**

All of the members of the Reprivata management team had spent a great deal of time, effort, and money to meet with potential clients in order to get an early adopter in the United States. Now, Scott and Nathan had both spent a significant amount of their own personal funds and could not easily raise additional money. David was not wealthy and did not have a great deal of available cash to help prop up the company’s finances in the short term. Tripp, being an investment banker working in the Silicon Valley area, had funded some of the companies’ activities since he joined the company, but he was a widowed father with 5 children to care for and could not contribute much more money at this time. That left the management team with several alternatives to consider.

Scott had always stated that his vision had already been to concentrate on the Master Agreements and let the clients define their own uses of a collaboration solution, even though they might not be the one Reprivata offered. Was the approach of allowing clients to determine how and if they wanted to implement a collaboration technology without using the Reprivata solution a prudent one?
There was quite a bit of discussion on how to fix the short-term money issues. Was it a good idea to go all in right now and spend most, if not all, of the remaining capital on the upcoming product demonstration, betting heavily on its success to secure the “early adopter” client the firm had been seeking?

With his investment banking background, Tripp had a number of high-level contacts with some of the leading venture capital firms and individual investors in Silicon Valley and New York that might be interested in investing in Reprivata. With a large client win potentially in the offing now, was it prudent to make an attempt to raise funds now? Also, if the Reprivata management team did that, what would they have to give, either in participation in the company or in ownership of its proprietary technology, to make such a deal?

Tripp and Scott had been attending security trade shows and conferences and had spoken with several cybersecurity vendors about the Reprivata solution. A number of the companies they met, including a few of the very large cybersecurity vendors, were interested in forming partnerships to bring a more comprehensive cybersecurity solution to market by integrating Reprivata’s technology. If they made such an arrangement, would Reprivata ultimately lose its identity and, more importantly, the potential for future earnings from its unique and innovative technology?

Tripp, Scott, and David had a number of conversations about the best way to productize the Reprivata solution. One way they discussed was to spin off the proprietary technology solution suite to form a software company. In fact, the technology was perhaps the most valuable asset the company held. However, Scott was adamant that Reprivata would not become a software development firm, which would require the hiring of programming, support, and sales people. Tripp made the argument that spinning the technology off into a separate company could give Reprivata a great opportunity to further mature the product and could provide more opportunities to integrate the software with other cybersecurity technologies and make the proprietary technology even more valuable. Did Reprivata really need such a development capability?

References


Biography

Ed Fulford is an executive in risk, information security, and compliance. He has more than 25 years of international experience assessing, building, and managing IT Security and Risk Management programs for companies such as CGI, CAPCO, RBS WorldPay, Fundtech Corporation, Cingular Wireless, and British Telecom. Fulford earned a Bachelor of Science in Business Administration from the University of Florida and a Master of Business Administration from Troy University. His professional certifications include the Payment Card Industry Professional, Certified Information Security Manager, Certified Information Systems Security Professional, Certified Fraud Examiner, and Certified Information Systems Auditor credentials.
### Exhibit 1: Comparison of Selected Cybersecurity Management Standards

<table>
<thead>
<tr>
<th>Comparison Criteria</th>
<th>Industry-Specific Cybersecurity Standards</th>
<th>ISO 27000 Standards</th>
<th>NIST Cybersecurity Framework</th>
<th>General Data Protection Regulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Includes Comprehensive Security Guidance and Leading Practices</td>
<td>Differs between standards</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Aligns with other Information Security and Business Standards</td>
<td>Alignment is relatively easy, but takes time to do</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Facilitates Compliance with other Information Security Standards</td>
<td>No, but there are some frameworks that use other standards as models for technical controls</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes, but requires compliance assessment to determine</td>
</tr>
<tr>
<td>Is Specific to a Single Country or Region</td>
<td>Yes, in most cases</td>
<td>No</td>
<td>Yes, but useful for foreign companies doing business in the United States</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes Cybersecurity Maturity Model</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Requires Collaboration between Business Partners</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

*Source: Developed by case writer*
Exhibit 2: Reprivata Community of Trust Conceptual Model

Source: Developed by case writer
### Exhibit 3: NIST CSF Functions & Control Categories for Assessment

<table>
<thead>
<tr>
<th>Functions</th>
<th>Categories</th>
</tr>
</thead>
</table>
| Identify (ID) | Asset Management (AM)  
Governance (GV)  
Risk Assessment (RA)  
Risk Management Strategy (RM)  
Supply Chain Risk Management (SC) |
| Protect (PR) | Identity Management, Authentication and Access Control (AC)  
Awareness and Training (AT)  
Data Security (DS)  
Information Protection Processes and Procedures (IP)  
Maintenance (MA)  
Protection Technologies (PT) |
| Detect (DT) | Anomalies and Events (AE)  
Security Continuous Monitoring (CM)  
Detection Processes |
| Respond (RS) | Response Planning (RP)  
Communications (CO)  
Analysis (AN)  
Mitigation (MI)  
Improvements (IM) |
| Recover (RC) | Recovery Planning (RP)  
Improvements (IM)  
Communications (CO) |

*Source: Developed by case writer*
## Exhibit 4: NIST CSF Implementation Tiers

<table>
<thead>
<tr>
<th>Maturity Tier</th>
<th>Definition and Characteristics</th>
</tr>
</thead>
</table>
| **1. Partial** | **Risk Management Process** – Organizational cybersecurity risk management practices are not formalized, and risk is managed in an *ad hoc* and sometimes reactive manner. Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements.  
**Integrated Risk Management Program** – There is limited awareness of cybersecurity risk at the organizational level. The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources. The organization may not have processes that enable cybersecurity information to be shared within the organization.  
**External Participation** – The organization does not understand its role in the larger ecosystem with respect to either its dependencies or dependents. The organization does not collaborate with or receive information (e.g., threat intelligence, best practices, technologies) from other entities (e.g., buyers, suppliers, dependencies, dependents, ISAOs, researchers, governments), nor does it share information. The organization is generally unaware of the cyber supply chain risks of the products and services it provides and that it uses. |
| **2. Risk Informed** | **Risk Management Process** – Risk management practices are approved by management but may not be established as organizational-wide policy. Prioritization of cybersecurity activities and protection needs is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.  
**Integrated Risk Management Program** – There is an awareness of cybersecurity risk at the organizational level, but an organization-wide approach to managing cybersecurity risk has not been established. Cybersecurity information is shared within the organization on an informal basis. Consideration of cybersecurity in organizational objectives and programs may occur at some but not all levels of the organization. Cyber risk assessment of organizational and external assets occurs, but is not typically repeatable or reoccurring.  
**External Participation** – Generally, the organization understands its role in the larger ecosystem with respect to either its own dependencies or dependents, but not both. The organization collaborates with and receives some information from other entities and generates some of its own information, but may not share information with others. Additionally, the organization is aware of the cyber supply chain risks associated with the products and services it provides and uses, but does not act consistently or formally upon those risks. |
| **3. Repeatable** | **Risk Management Process** – The organization’s risk management practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on the application of risk management |
processes to changes in business/mission requirements and a changing threat and technology landscape.

**Integrated Risk Management Program** – There is an organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities. The organization consistently and accurately monitors cybersecurity risk of organizational assets. Senior cybersecurity and non-cybersecurity executives communicate regularly regarding cybersecurity risk. Senior executives ensure consideration of cybersecurity through all lines of operation in the organization.

**External Participation** – The organization understands its role, dependencies, and dependents in the larger ecosystem and may contribute to the community’s broader understanding of risks. It collaborates with and receives information from other entities regularly that complements internally generated information, and shares information with other entities. The organization is aware of the cyber supply chain risks associated with the products and services it provides and that it uses. Additionally, it usually acts formally upon those risks, including mechanisms such as written agreements to communicate baseline requirements, governance structures (e.g., risk councils), and policy implementation and monitoring.

**4. Adaptive Risk Management Process** – The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators. Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing threat and technology landscape and responds in a timely and effective manner to evolving, sophisticated threats.

**Integrated Risk Management Program** – There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. The relationship between cybersecurity risk and organizational objectives is clearly understood and considered when making decisions. Senior executives monitor cybersecurity risk in the same context as financial risk and other organizational risks. The organizational budget is based on an understanding of the current and predicted risk environment and risk tolerance. Business units implement executive vision and analyze system-level risks in the context of the organizational risk tolerances. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities and continuous awareness of activities on their systems and networks. The organization can quickly and efficiently account for changes to business/mission objectives in how risk is approached and communicated.
**External Participation** - The organization understands its role, dependencies, and dependents in the larger ecosystem and contributes to the community’s broader understanding of risks. It receives, generates, and reviews prioritized information that informs continuous analysis of its risks as the threat and technology landscapes evolve. The organization shares that information internally and externally with other collaborators. The organization uses real-time or near real-time information to understand and consistently act upon cyber supply chain risks associated with the products and services it provides and that it uses. Additionally, it communicates proactively, using formal (e.g., agreements) and informal mechanisms to develop and maintain strong supply chain relationships.

*Source: Developed by case writer based on CSF version 1.1, 2018*
A NOTE ON THE CYBERSECURITY PROBLEM SPACE IN 2018

The Transmission Control Protocol/Internet Protocol (TCP/IP) used for Internet communications was designed so that traffic from one device connected to the Internet was visible to all other connected devices. This one attribute made it possible for bad actors and hackers to attack any company, country, or person from anywhere on earth across the Internet. For the first time in recorded history, a disgruntled individual, terrorist group, or rogue country wreaked havoc on other people, companies, countries, and--of even greater concern--the global economy. All that was required was a computer, an Internet connection, and one or more vulnerable endpoints attached to critical applications or networks also linked to the Internet.

The cybersecurity industry had long acknowledged that the Internet was not originally designed for electronic business. Also, it was never intended for the transmission of critical information, nor for the support of mission critical networks and infrastructure. As quoted from a 2002 research report produced by the CERT Coordination Center in connection with the Software Engineering Institute (SEI) at Carnegie Mellon University (CMU): “The Internet was not designed to resist highly untrustworthy users” (Lipson, 2002).

Recognizing this problem, the cybersecurity industry’s mindset was focused on defending against untrustworthy users. After all, this approach worked in the physical world. If one knew the weapon that an attacker was using and the direction from which the attack was coming, an effective defense could often be planned and implemented. However, this had not been the case when defending against cyberattacks on the Internet. There usually were many ways to stage an attack without being detected. In addition, the technologies that were used for masking such attacks had become more sophisticated, as

---

2 Copyright © 2018, Ed Fulford. This technical note was developed to provide background information in support of one or more case studies published by the Muma Case Review. It may be freely copied and shared for non-commercial purposes.
demonstrated by attackers’ abilities to anonymize themselves and their attack vectors, which made it much more difficult to isolate the sources of attacks. Also, remember that many of the recent cybersecurity solutions defended against an attack that had already occurred and offered no assurance that they could defend against the next attack.

Cybersecurity and risk management professionals had been working diligently to improve information security and risk management practices in order to reduce overall cybersecurity risks. While these efforts had managed to improve information security practices, they had done so without showing any significant or maintainable reductions in the numbers and types of cybersecurity risks. This situation had identified a variety of challenges that cybersecurity experts needed to address in a number of key problem areas.

The Cybersecurity Problem Space

Ely Kahn from Sqrrl, one of responders to the 2017 Passcode (The Christian Science Monitor's section on security and privacy) poll of cybersecurity practitioners, stated (Sorcher, 2017):

I think the most urgent cybersecurity challenge is the need for all organizations to fully understand the cyber risks they face, how those risks affect their mission, and what are the most cost-effective ways to mitigate those risks.

The cybersecurity practitioners’ struggles to stem the tide of cyber risks came at the increasing expense of the resources--tools, personnel, and support--needed to change the nature of global, national, and business behaviors that helped create this situation in the first place. The focus on creating cybersecurity solutions to fix more than point problems had not gained significant mindshare with cybersecurity practitioners, so they tried to transform current information security and risk management approaches to address broader and increasing more interrelated problem spaces. As a method of dealing with cybersecurity risks, information security might ultimately have had an indirect impact on the successful implementation of effective cybersecurity control programs over time. However, the management and assessment practices related to information security problem and solution spaces were not encompassing enough and were too inwardly focused to enable wide-reaching strategic and tactical enhancements to take place. As such, cybersecurity programs were not maturing quickly enough to deal with these risks. One significant reason for this situation was the lack of collaboration between companies that did business together. In many cases, these business partners did not discuss their common cybersecurity issues because of the lack of defined rules of engagement and secure communication capabilities.

For the purpose of this article, the following cybersecurity problem areas will be discussed:

- Global Cybersecurity Problems
- Government Cybersecurity Problems
- Business Cybersecurity Problems
- Cybersecurity Standards Problems

Global Cybersecurity Problems

Europol, the European Union Agency for Law Enforcement Cooperation, recently assessed the global impact of cybersecurity events like the ransomware epidemic. In their study, they found that their efforts had some successes in disrupting criminal groups that primarily operated online. However, they also determined that the economic impact was far reaching with cross-border implications as multinational banks and international corporations were attacked. Commenting on this situation in an October 2017

The global impact of huge cyber security events such as the WannaCry ransomware epidemic (a cryptoworm attack in 2017 which targeted computers running the Microsoft Windows operating system by encrypting data and then demanding the owners to make payments in the Bitcoin cryptocurrency to release the computer has taken the threat from cybercrime to another level.

Summing up the efforts of Europol and its law enforcement partners at the conclusion of the interview, Wainwright said that, even with the progress that had been made, “The collective response is still not good enough” (“The Global Impact,” 2017).

Over time, cybersecurity threats and attacks like the WannaCry incidents had become ever-present news items. As terrorist groups and rogue governments sought new ways to economically damage or strike fear in their enemies, the number and sophistication of cybersecurity incidents grew. The 2017 Internet Organized Crime Threat Assessment cited several examples of cyber events with a global reach that included:

- Ransomware eclipsed most other cyber-threats with global campaigns indiscriminately affecting victims across multiple industries in both the public and private sectors. Some attacks targeted and affected critical national infrastructures at levels that could have endangered lives. These attacks highlighted how network interconnectivity, poor digital hygiene standards and insufficient security practices allowed such threats to quickly spread and expand the attack vectors.

- The first serious attacks by botnets using infected insecure Internet of Things (IoT) devices occurred.

- Data breaches continued to result in the disclosure of vast amounts of data, with over 2 billion records related to European Union citizens reportedly being leaked over a 12-month period, often exacerbated by poor digital hygiene and security practices.

- The Darknet remained a key cross-cutting enabler for a variety of crime areas. It provided access to among other things:
  - The supply of drugs such as Fentanyl and new psychoactive substances which directly led to many fatalities internationally
  - The supply of firearms that were used in terrorist acts
  - Compromised payment data which enabled bad actors to commit various types of payment fraud
  - Fraudulent documents which facilitated various types of fraud, trafficking in human beings, and illegal immigration activities

- Offenders continued to abuse the Darknet and other online platforms, sharing and distributing child sexual abuse material, and engaging with potential victims, often coercing or sexually extorting vulnerable minors.

- Payment fraud affected almost all industries, having the greatest impact on the Retail, Airline and Accommodation sectors. Several sectors had been targeted by these fraudsters as the services they
provided could be used for the facilitation of other crimes, including trafficking in human beings or drugs, and illegal immigration.

- Direct attacks on bank networks manipulated card balances, took control of ATMs or directly transferred funds, known as payment process compromise, represented one of the serious emerging threats in this area. (“The Global Impact,” 2017).

While governments began to allocate more money and personnel to defend their countries, many companies were not financially able to defend themselves, and affected individuals were even less able to do so. Even with the regulatory and industry requirements placed on them, neither companies nor individuals could adequately defend themselves from cyber-attacks and were not likely to have the training, competence, or capability to do so. The best that could be expected was that companies would continue to strive to maintain a heightened degree of operational resilience, business continuity, and disaster recovery in their strategic and tactical plans.

As outlined in the cybersecurity industry report mentioned above, international and business boundaries had been all but eliminated by electronic commerce, which put more pressure on governments and companies to be more vigilant in their own cybersecurity controls to prevent or limit the impacts from cyber incidents. Practitioners in the cybersecurity field actively discussed if it was more prudent to implement, maintain, and monitor the effectiveness of security controls around their supply chains or their networks. Ultimately, however, these cybersecurity professionals determined that more work was required. In many cases, the international supply chains were intertwined with transnational computer networks, which made the deployment and monitoring of these security control mechanisms and systems much more difficult. As discussed previously, the lack of cybersecurity program maturity in governments and international companies, in addition to the absence of consistent collaboration between these groups based on prescribed rules for doing so, limited their abilities to coordinate actions to deal with cybersecurity issues that arose on a seemingly daily basis.

The consequences from the set of circumstances outlined above were far-reaching. For example, the rising hostility of threat actors was often misunderstood and not foreseen before attacks took place, which lessened the time and ability for governments or companies to respond, thus costing them financially and operationally as well as negatively impacting their reputations. The other effects from such events included critical systems and services not being available or functioning as designed during emergencies and the civil conflicts that resulted from prolonged service outages.

**Government Cybersecurity Problems**

Government agencies had helped safeguard very sensitive information on their country’s citizens as well as data about their actions and programs that affected the public welfare. This had made them particularly attractive targets for cyberattacks. Unfortunately, governments had often lagged behind businesses in the implementation of cybersecurity controls and protection systems. This became a serious concern as the cyberattacks and the terrorists who launched them became more sophisticated. The Heritage Foundation, in its January, 2018 report on Federal cyber breaches, found that there were over 30,000 cybersecurity incidents that affected the United States government in 2016, with 16 rising to the level of a being a major incident (Walters, 2018). Both the Obama and Trump Administrations issued Executive Orders mandating the United States government to implement modern, focused, responsive, and proactive cybersecurity programs that had the ability to adapt to the threat environment and to provide better measurements of the cyber risks faced. At this point, it was not readily apparent that the government had
begun to dedicate the appropriate resources to do this and to meet these cyber challenges in an aggressive way.

Cybersecurity practitioners both inside and outside the government questioned what intelligence and law enforcement agencies had done to deploy effective cyber defense technologies. Of particular concern were the abilities of agencies charged with cybersecurity monitoring as well as identifying and remediating security breaches. For example, when Wikileaks released what it believed to be a list of CIA hacking tools in March, 2017, these abilities were seriously questioned. This incident exposed a list of cybersecurity hacking applications known as “Year Zero” or “Vault 7,” which were reportedly acquired by Wikileaks while the information passed between government employees and contractors in an “unauthorized manner.” A month later in April, 2017, a group known as the Shadow Brokers continued releasing what it claimed were NSA hacking tools. One of the tools included in this release, known as EternalBlue, was associated with a number of cyberattacks, including those involving WannaCry ransomware, which occurred throughout the summer of 2016 and into 2017. The Shadow Brokers claimed to have stolen these tools from a team, known as the “Equation Group,” which was reportedly associated with the NSA (Walters, 2018).

Also, state and local governments had been even more at risk from such cyberattacks. Few had the money to invest in the technologies and the appropriately trained personnel to provide needed services in network security, threat intelligence, risk-based analytics, and data encryption. The ransomware attack that crippled the government support systems of the City of Atlanta, Georgia for over a week in March, 2018 was further indication that local governments had been woefully underprepared from a technical capability perspective and a personnel standpoint to deal with these types of cyberattacks when they occurred (Hutcherson, 2018).

Government agencies at all levels had not been able to effectively create cyber defense capabilities in their organizations, primarily due to the fact that their cybersecurity strategies had often been “silied” in one functional area. As such, these agencies had not concentrated on bringing their entire organization up to a baseline level of compliance to cybersecurity standards such as those created by the National Institute of Standards and Technology (NIST). By assessing their current cybersecurity strategies and competencies against these standards, agencies determined what gaps existed in their processes and practices as well as in their technical capabilities. This began to help them determine how exposed their information assets were and the best ways to resolve those security control issues.

From a functional standpoint, government agencies needed to build more robust security-focused cultures that monitor, measure, and manage cybersecurity behaviors. Once this had been initiated, agencies then concentrated on pushing out cyber risk management activities to the rest of their organizations. Providing the right visibility to, and understanding of, cyber risks to the broader organization was found to be critical to success in mitigating them quickly and minimizing their impacts.

Collaboration and communication of potential and real cybersecurity events and attack scenarios showed that such activities facilitated agencies working better together. This information sharing assisted agencies in better understanding cyber incidents that had the potential to affect agencies and other public organizations. By identifying critical points of failures, decision criteria, and barriers to progress, government agencies had developed better cyber defense strategies that speeded remediation from breaches and prevented similar events from occurring in the future. In the Heritage Foundation’s report, one of the key takeaways was that the United States government should continue to focus on securing its own networks while collaborating with the private sector and international communities on better understanding cyber risks. (Walters, 2018).
In order to change the behaviors in government agencies, the numbers and types of cybersecurity threats and vulnerabilities had been evaluated in more detail, including the activities of foreign and domestic cyber threat actors and their attendant risks. This had shown the potential to speed up the implementation of cyber risk management technologies to defend against these actors. This had also assisted with better aligning cybersecurity strategies with those of the agencies’ operational missions. Government agencies had not consistently created and tested cyber defense readiness plans. When done proactively, these programs had success in ensuring that incident response and escalation procedures were widely communicated and tested for their effectiveness. Additionally, this facilitated collaboration between agencies to show how they jointly managed cyber incidents. In the law enforcement arena, programs like the Department of Justice’s Building Communities of Trust initiative improved how federal and local law enforcement groups worked together. (Wasserman, 2010).

Finally, government agencies had not had the appropriate levels of internal expertise required to make better cybersecurity investment and program management decisions. Agencies needed to examine their cybersecurity investments against leading practices and benchmarks, but this had not been done consistently. In order to ensure agencies allocated their resources with a risk-based approach, they had utilized mission objectives, benchmarks, and cybersecurity directions as guides. Government agencies had approached their cybersecurity postures as an evolving landscape of increasing potential threats—one that had required the ability to adapt to those risks. Proactive and mature cybersecurity programs had needed the commitment from leaders to be able to invest wisely, create a culture of cyber innovation, and maintain relevant and continuous training and awareness programs.

**Business Cybersecurity Problems**

Cybersecurity had become one of the most important issues facing businesses today. According to the World Economic Forum’s 2018 Global Risks Report, both large-scale cyberattacks and major data breaches or fraud were ranked among the top five most likely risks in the next decade (“The Global Risks Report,” 2018). At the time of the case, companies had been required to deal with cybersecurity problems head on because those issues have had significant impacts on the overall business operations as well as the Information Technology (IT) infrastructure. This had become even more critical for those businesses that were interconnected with third parties such as partners and suppliers. These interconnections exposed all the business partners to cyber threats that had become more severe and frequent. As the numbers of security risks had risen, businesses learned, to their dismay, that they faced more threats and more attacks than ever before, many of which required more and faster cyber response and remediation capabilities than were already in place.

As businesses expanded their interconnections and shared more information, the number of networks and devices that required more comprehensive security controls increased as well. In recent years, 63 percent of breaches were traced to third-party vendors, according to the Soha System’s 2016 survey on third-party risk management (“Soha Systems' Survey,” 2016). The security of mobile telephones, tablet computers, and other networkable devices had lagged in the implementation of cybersecurity controls too. Additionally, new technology advances such as artificial intelligence and machine learning enabled threat actors to create more malicious and sophisticated tools to use in their attacks.

If the statistics from recent global security breaches had been accurate indicators, the impacts of these incidents clearly affected businesses and their partners as a group as well as individually. In a November, 2017 article on ComputerWeekly.com, incidents affecting infrastructure hosted by a third party cost small businesses £106K on average, while large enterprises lost nearly £1.5M as a result of breaches affecting suppliers they shared data with, and saw another £1.2M in expenditures because of insufficient levels of
protection from providers of Infrastructure as a Service (IaaS) (Ashford, 2017). The threat environments had changed, with hacking software and hackers themselves becoming much more advanced in both capability and reach. Cyber terrorists had progressed in more economically-focused directions including industrial espionage, corporate disinformation, market and financial manipulation, and disruption of critical public and private infrastructures. They had done so without slowing their previous activities such as data exfiltration, system ransom and extortion, and digital vandalism. Mitigating these threats had required businesses to re-think the cybersecurity and business risk postures. In many cases, organizations developed a more inclusive approach to enterprise risk management. Current thinking in business strategies had required companies to reconsider how cyber risks affected the company as a whole, including stakeholders like customers, partners, suppliers, industry groups, and regulators. The ComputerWeekly.com article quoted Alessio Aceti, head of the enterprise business division at Kaspersky Lab, a multinational Internet security and anti-virus provider, who stated (Ashford, 2017):

> While cyber security incidents involving third parties prove to be harmful to businesses of all sizes, their financial impact on a company had the potential to result in twice as much damage.

Because cybersecurity had been considered a business risk as well as a technology risk, integrating monitoring for both of these risks into the company’s cybersecurity risk management program had become essential. Cyber risks had impacted entire businesses operationally and financially, and seriously damaged their reputations in the process. In such situations, businesses needed to continue evaluating, updating, and communicating their cybersecurity policies, practices, business rules, training programs, and other procedures to cause the requisite cultural changes required for better cybersecurity hygiene. When done in a holistic way, cyber risk management had become a strategic weapon for better protecting the company’s environment while maturing its cybersecurity capabilities at the same time. Companies had approached this challenge by creating better new rules of engagement with their interconnected business partners, such as contractual agreements in which both the company and its partners were required to improve their cybersecurity programs and provide ways to demonstrate the maturity of the programs. However, this change had not been adopted widely, and many businesses had not started to collaborate with their partners in this area. A key reason was that businesses had not had technologies that enabled them to communicate securely with their internal and external stakeholders to deal with mutual cybersecurity risks.

In its 2016 Global 1000 survey, CGI, a leading independent information technology and business process services firm, found that organizations that viewed security not only as a mandatory part of operations, but also as an enabler to growth and change, maximized the benefits of digital transformation efforts. At the same time, only 14% of clients who responded to the Global 1000 survey stated that they were at a level of maturity where cybersecurity was a key part of their value propositions (CGI, 2016). In order to move forward, companies had begun to take input from regulatory, industry, consumer, and other stakeholder groups in order to mature their cybersecurity strategies and risk management systems. By approaching cybersecurity as a business problem first, companies had been better able to create more resilient operational frameworks that would improve their abilities to identify, respond to, and remediate cyberattacks and mitigate any business interruptions more quickly and cost effectively.

**Cybersecurity Standards Problems**

Cybersecurity practitioners had reviewed security and control-related guidelines and standards to determine which ones of the various government, industry, and independently developed guidelines would be the best ones for them to utilize as they continued development on their cybersecurity programs. Companies had been increasingly challenged by regulators, industry groups, and business partners to
become savvier in the areas of maturing their cybersecurity programs and understanding their cyber risks. However, as determined by a review of the academic literature (Fulford, 2017), there were a significant number of cybersecurity and risk management frameworks used by cybersecurity practitioners that ranged from rudimentary ones based on manual questionnaires using qualitative techniques to those that were very complex utilizing strong quantitative and statistical measures. In January, 2018 the IT Governance web site published a review of the most frequently adopted cybersecurity frameworks (Watson, 2018):

- Payment Card Industry Data Security Standard (PCI DSS) – 47%
- International Standards Organization (ISO) 27001/27002 – 35%
- Center for Internet Security (CIS) Critical Security Controls – 32%
- National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Security – 29%

While all of these frameworks had large numbers of adopters, the newer NIST Cybersecurity Framework (NIST CSF) successfully combined qualitative and quantitative methods in an easy-to-use and understandable format. This methodology, which was created in part from the older NIST 800 series security and risk management approach, was found to map directly to most of the control requirements and most of the other security frameworks, which would make it relatively easy to implement for many companies and government agencies. To many companies, the ability to measure and understand cyber risks on several levels internally and externally had become daunting challenges to companies’ enterprise risk management programs. A framework, like the NIST CSF, that enabled companies to assess each other’s cyber maturity and define collaboration in disseminating ways to better deal with risks across their business ecosystem, regardless of industries involved or the technologies they used to interconnect and exchange products, services, and—most importantly—information.

Current directions in cyber risk evaluation had been seeking a way for companies to “get credit” for the work they were doing to mature their cybersecurity programs while simultaneously identifying cyber risks and related security control gaps. This type of approach had helped senior executives rationalize their investments in their technology footprints and attendant cybersecurity governance and management practices. An overarching cybersecurity implementation and risk management methodology which enabled companies in different industries and business practices to have common vocabulary and taxonomy for discussing and understanding their cyber risks would be extremely beneficial to a variety of industry and government organizations.

Such a methodology had assisted companies in standardizing and streamlining the implementation of cyber risk management controls that were required by the establishment and operation of new business technology interconnections. This had helped businesses to eliminate redundancies in security controls and to increase the understanding of how effectiveness of those controls was measured. Companies had a duty to be more cyber mature, including improving understanding the cyber risks related to their internal and external technology interconnections, as well as their indirect interconnections (such as the interconnections of their business partners’ partners).

References


Biography

Ed Fulford is an executive in risk, information security, and compliance. He has more than 25 years of international experience assessing, building, and managing IT Security and Risk Management programs for companies such as CGI, CAPCO, RBS WorldPay, Fundtech Corporation, Cingular Wireless, and British Telecom. Fulford earned a Bachelor of Science in Business Administration from the University of Florida and a Master of Business Administration from Troy University. His professional certifications include the Payment Card Industry Professional, Certified Information Security Manager, Certified Information Systems Security Professional, Certified Fraud Examiner, and Certified Information Systems Auditor credentials.