USF | Muma Case Review
A publication of the Muma College of Business | University of South Florida

Volume 3 Number 7 09 MAY 2018

ED FULFORD

IMPLEMENTING A CYBERSECURITY COMMUNITY OF TRUST: REPRIVATA SEEKS AN "EARLY ADOPTER"[1]

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?"

Editor: T. Grandon Gill, DBA

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 re-certify 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 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

Fulford, E. (2017). What factors influence companies' successful implementations of technology risk management systems? *Muma Business Review, 1*(13), 157-169. Retrieved from http://pubs.mumabusinessreview.org/2017/MBR-2017-157-169-Fulford-TechnologyRisk.pdf

House, W. (2013). Executive order (eo13636): *Improving critical infrastructure cybersecurity.* Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

Wasserman, R. (2010). *Building communities of trust.* Retrieved from https://nsi.ncirc.gov/documents/e071021293_BuildingCommTrust_v2.pdf

Biography

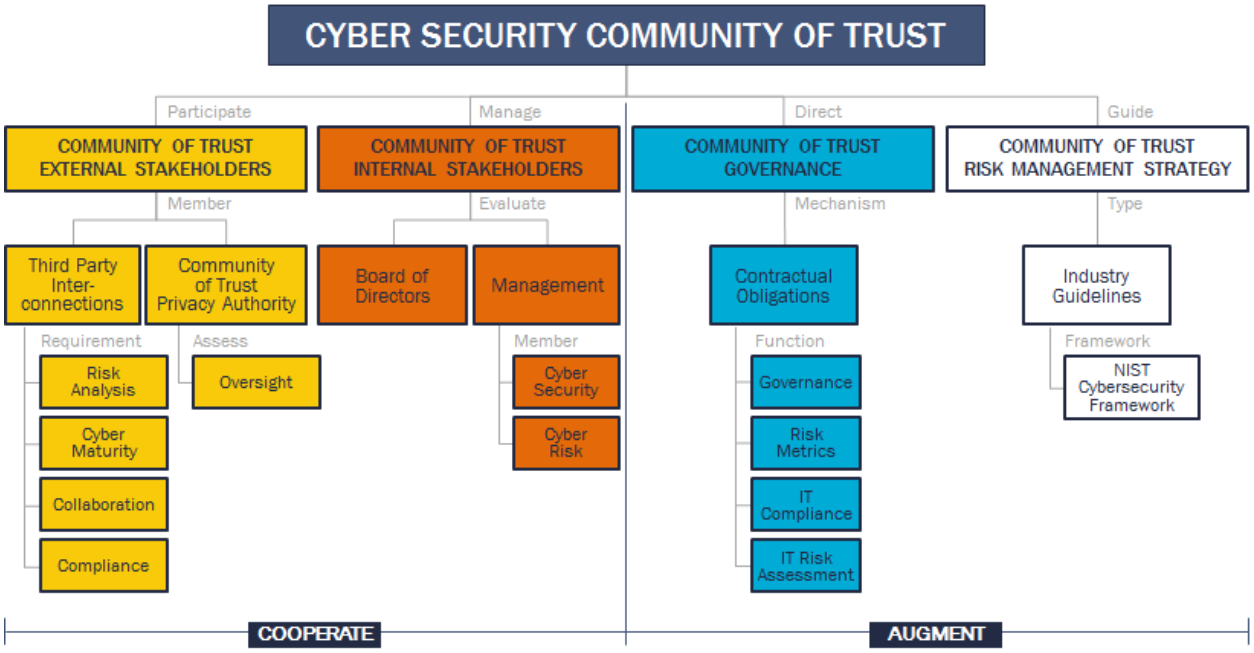
Ed Fulford is an executive in risk, information security, and compliance. He has more than 25 years of international experience assessing, building, and managing IT Security and Risk Management programs for companies such as CGI, CAPCO, RBS WorldPay, Fundtech Corporation, Cingular Wireless, and British 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

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

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

Functions	Categories
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)

Source: Developed by case writer

Exhibit 4: NIST CSF Implementation Tiers

Maturity Tier	Definition and Characteristics
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