JOURNAL OF INFORMATION SYSTEMS APPLIED RESEARCH

Volume 14, Issue. 2
June 2021
ISSN: 1946-1836

In this issue:

iscap
Information Systems & Computing Academic Professionals

The **Journal of Information Systems Applied Research** (JISAR) is a double-blind peer reviewed academic journal published by ISCAP, Information Systems and Computing Academic Professionals. Publishing frequency is three to four issues a year. The first date of publication was December 1, 2008.

JISAR is published online (https://jisar.org) in connection with CONISAR, the Conference on Information Systems Applied Research, which is also double-blind peer reviewed. Our sister publication, the Proceedings of CONISAR, features all papers, panels, workshops, and presentations from the conference. (https://conisar.org)

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the conference. At that point papers are divided into award papers (top 15%), other journal papers (top 30%), unsettled papers, and non-journal papers. The unsettled papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the JISAR journal. Currently the target acceptance rate for the journal is about 40%.

Questions should be addressed to the editor at editor@jisar.org or the publisher at publisher@jisar.org. Special thanks to members of ISCAP/EDSIG who perform the editorial and review processes for JISAR.

2021 ISCAP Board of Directors

Eric Breimer Siena College President	James Pomykalski Susquehanna University Vice President	Jeffry Babb West Texas A&M Past President/ Curriculum Chair
Jeffrey Cummings Univ of NC Wilmington Director	Melinda Korzaan Middle Tennessee State Univ Director	Niki Kunene Eastern CT St Univ Director/Treasurer
Michelle Louch Carlow University Director	Michael Smith Georgia Institute of Technology Director/Secretary	Lee Freeman Univ. of Michigan - Dearborn Director/JISE Editor
Tom Janicki Univ of NC Wilmington Director/Meeting Facilitator	Anthony Serapiglia St. Vincent College Director/2021 Conf Chair	

Copyright © 2021 by Information Systems and Computing Academic Professionals (ISCAP). Permission to make digital or hard copies of all or part of this journal for personal or classroom use is granted without fee provided that the copies are not made or distributed for profit or commercial use. All copies must bear this notice and full citation. Permission from the Editor is required to post to servers, redistribute to lists, or utilize in a for-profit or commercial use. Permission requests should be sent to Scott Hunsinger, Editor, editor@jisar.org.

JOURNAL OF INFORMATION SYSTEMS APPLIED RESEARCH

Editors

Scott Hunsinger
Senior Editor
Appalachian State University

Thomas Janicki
Publisher
University of North Carolina Wilmington

2021 JISAR Editorial Board

Ulku Clark
University of North Carolina Wilmington

Ed Hassler
Appalachian State University

Muhammed Miah
Tennessee State University

James Pomykalski
Susquehanna University

Christopher Taylor
Appalachian State University

Karthikeyan Umapathy
University of North Florida

Jason Xiong
Appalachian State University

Towards a Leader-Driven Supply Chain Cybersecurity Framework

Manoj Vanajakumari
Business Analytics
manojuv@uncw.edu

Sudip Mittal
Computer Science
mittals@uncw.edu

Geoff Stoker
Information Systems
stokerg@uncw.edu

Ulku Clark
Information Systems
clarku@uncw.edu

University of North Carolina Wilmington
Wilmington, NC 28403

Kasey Miler
Kcmiller1@nps.edu
Naval Postgraduate School
Monterey, CA 93943

Abstract

Supply chains (SC) often span multiple cultures, countries, and time zones with security concerns that, at a high level, can be grouped into two broad areas: 1) products/assets; 2) information technology (IT). SCs can achieve higher operational efficiency if participating entities are highly connected since rapid information transfer helps SC participants be agile, adaptable, and aligned. To be antifragile, a key requirement of highly interconnected systems is strong overall cybersecurity. We posit that individual partners independently enhancing their security may not sufficiently improve the overall SC cybersecurity posture; rather, what is required is that coordinated cybersecurity efforts be driven by the SC's most powerful member. We propose a conceptual framework for the leader in the SC that involves two broad elements: 1) supplier/member selection; 2) continuous training, development, and risk assessment of SC members from a cybersecurity perspective. A use case is provided to expound on the presented ideas.

Keywords: Supply Chain, Cybersecurity, Framework, Powerful Member

©2021 ISCAP (Information Systems and Computing Academic Professionals)

1. INTRODUCTION

The National Institute of Standards and Technology (NIST) states that:

> Supply chains are complex, globally distributed, and interconnected sets of resources and processes between multiple levels of organizations. Supply chains begin with the sourcing of products and services and extend from the design, development, manufacturing, processing, handling, and delivery of products and services to the end user (NIST, 2018b, p. 15).

Supply Chain (SC) entities include suppliers, manufacturers, wholesalers/distributors, and retailers. SCs that focus exclusively on speed and cost often break down over time, so to be resilient and effective, SCs require agility, adaptability, and alignment (Lee, 2004). Agility is needed to accommodate sudden changes in supply and demand; adaptability helps SCs respond to market changes; and better alignment is gained via strong collaboration among SC members. These traits develop among SC entities during long-term relationships during which they share information on a timely basis and adapt new technology as needed.

Power asymmetries exist in SCs (Munson, Rosenblatt, & Rosenblat, 1999). Certain characteristics confer organizational power of one SC member over the others e.g., a partner has reward power if it can help other SC members achieve their goals. Other types include expert, referent, coercive, and legitimate power. For example, Walmart has huge financial clout and can require suppliers to do packaging, RFID tagging, and delivery in the way that best suits Walmart, even if some suppliers would have to operate sub-optimally. Often the power of one member is sufficiently transcendent that the SC is recognized by that member's name, e.g. Walmart, Target, Boeing, etc. We will generically refer to the partner with the most organizational power as the *powerful member*. The terms leader and powerful member are equivalent in the context of this paper, and we will use powerful member from this point forward.

A cybersecurity disruption to any partner can cause dysfunction along the entire SC. Securing the information and information technology (IT) along the SC is extremely difficult given the degree of complexity involved and suggests several questions:

- Who has overall responsibility for SC cybersecurity?
- What do those responsibilities entail?
- How would a cybersecurity risk assessment of the SC be done?

As we will discuss in Section 2, the SC powerful member has an important role to play in SC cybersecurity. That role involves including cybersecurity considerations when selecting new SC members and maintaining a healthy SC ecosystem. Cybersecurity-specific risk assessments involve considerations of people, process, and technology.

Figure 1 depicts a typical stylized SC model. Products/material flow (solid, black arrows) from upstream to downstream. Money and information flow (dotted, gold, two-headed arrows) both upstream and downstream. To facilitate communication and information sharing, SC entities use technologies that link the various partners in an SC forming a chain of cyber-physical systems.

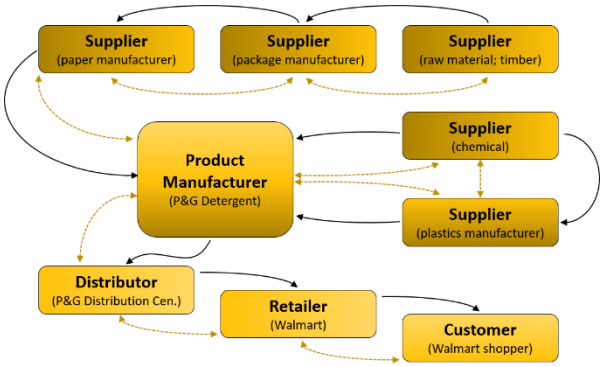

Figure 1 –SC stylized diagram (*products/material: black arrows; funds/information: dotted, gold arrows*)

SC security encompasses both the physical systems (products/assets) and the information technology (IT). Smith, et al., identify the cyber system portion of SCs as a network of IT infrastructures used to connect partners and further define:

> Supply Chain Information Security Risk (SCISR) as degradation or disruption to a supply chain's infrastructure or structural resources resulting from the successful exploitation of IT vulnerabilities by threats within an organization, within the supply chain network, or in the external environment (Smith, Watson, Baker, & Pokorski, 2007).

In this research, we examine the SCISR in the context of cybersecurity risk management.

There have been many reports of large-scale cybersecurity incidents (McCandless & Evans, 2020). Examples include the 2013 Target breach where network credentials were stolen from a third-party HVAC vendor (Krebs, 2014); the 2017 Verizon breach where a software and data firm partner misconfigured a cloud-based repository (UpGuard, 2017); and the 2017 Equifax breach where an open-source software component available from a third-party contained a five-year old flaw (Gutzmer, 2017). A recent survey of companies in the USA, UK, Switzerland, Mexico, and Singapore found that 92% of respondents had suffered a SC-partner-related breach in the previous 12 months (BlueVoyant, 2020).

Mulligan & Schneider report that several past cybersecurity doctrines such as prevention, risk management, and deterrence through accountability did not bear fruit (Mulligan & Schneider, 2011). They recommend viewing cybersecurity as a collective interest like public health and suggest that incentive mechanisms must be in place to prompt system developers, operators, and users to improve information system security.

We suggest that for cybersecurity risk assessment and management to succeed, the powerful member of the SC must take special initiative. The other SC members (non-powerful members – *note: we use this term to differentiate only, not to imply that the other members have no power per se*) are often smaller firms that do not possess the same resources to conduct cybersecurity activities to protect their cyber systems from cyber threats as the powerful member, as well, they often lack perspective on the *bigger picture*.

The vulnerabilities introduced to the SC ecosystem by the least cybersecurity-capable companies weaken the cybersecurity posture of the entire SC since the chain is only as strong as the weakest link. A rigorous analysis of potential SC partners before selection is essential. After selection, the contracts between SC partners need to detail the management of third-party risk in addition to other SC requirements. One example, the Department of Defense's (DoD) Cybersecurity Maturity Model Certification (CMMC) framework addresses vendor accreditation for cybersecurity and helps determine if contractors are doing due diligence to protect sensitive data that resides on their networks (Webmaster A&S, 2020).

In this paper, we introduce a framework designed to help businesses with SC partner selection and management processes to reduce the risk of cyber-attacks on SC partners' cyber systems. Our framework proposes guidelines on how the powerful member manages the process to mitigate the risks in the SC to an acceptable level.

Failure to protect SC cyber systems could lead to loss of revenue, reputation, and customers. With emerging technologies being integrated into the industrial processes, we are now in the era of Industry 4.0, which is enabled by Artificial Intelligence, Big Data Analytics, Autonomous Robots, Horizontal and Vertical Integration, Internet of Things, Augmented Reality, Additive Manufacturing, Cloud, and Cybersecurity. As empowering as these technologies are for businesses, they make the cyber-systems more complex. The more complex they are, the more vulnerable they are.

Examples of interconnected IT systems for the sake of efficiency are everywhere. Walmart's Retaillink system enables suppliers to successfully support Vendor Managed Inventory initiatives. Through this system, suppliers can see the store-level inventory at any time. Target gives access rights to HVAC vendors to remotely monitor energy consumption at its stores. Lean manufacturing systems require firms to carry as little inventory as possible to support a production schedule. Raw material suppliers have access to shop-floor inventory levels to support Just-in-Time production. It is imperative that the professionals who manage cyber-SC systems have a well-established risk management system in place. The interdependencies between SC partners create additional attack vectors that need to be addressed. A breach that leads to data theft or other unauthorized activity in the systems of any SC component could potentially compromise data of other SC players.

The rest of the paper is organized as follows. In Section 2 we propose a framework for SC cybersecurity. Section 3 provides a short use-case. Our conclusion remarks are in Section 4.

2. CYBERSECURITY FRAMEWORK FOR SUPPLY CHAIN STAKEHOLDERS

2.1 Building the Framework

Efficient suppliers are integral to SC profitability. As discussed above, they also play an important role in keeping the SC secure. The Japanese manufacturing philosophies like Just-in-Time and Toyota Production System view suppliers as long-term partners. Hence, it is critical to identify the right suppliers to join the SC. Building a long-term relationship not only helps the SC meet customer demand effectively, but it also helps secure the SC. Knowing that there is a long-term association with the SC powerful member, the other partners will be more willing to adopt process and technology recommendations to secure the SC.

NIST's Cyber Supply Chain Risk Management (C-SCRM) program started in 2008. The program defines C-SCRM as "the process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of IT/OT [information and operational technology] products and service supply chains" (NIST, 2020). Within NIST's Framework for Improving Critical Infrastructure (FICI), it elaborates that C-SCRM is

> the set of activities necessary to manage cybersecurity risk associated with external parties. More specifically, cyber SCRM addresses both the cybersecurity effect an organization has on external parties and the cybersecurity effect external parties have on an organization (NIST, 2018b, p. 16).

It goes on to explicitly state that the examples provided for how it can be used "are not intended to address C-SCRM comprehensively," thus leaving room for flexible use and extension by practitioners. Our proposed framework is complementary to and fits within the larger FICI and is currently called Stakeholder Cyber Supply Chain Risk Management (SC-SCRM). The elements of the framework are shown in Figure 2.

The framework has two main parts, the Supplier Selection process and what happens after a supplier is selected to become a SC member which is comprised of four key components: Training, Development, Technology, and Risk Assessment (TDTR) – all informed by the Supply Chain Cybersecurity Strategy (SCCS). Readers familiar with concepts like Kaizen (Imai, 1986) may find it helpful to think about the TDTR in the same terms. The SC powerful member can lead SC-SCRM with well-established TDTR components for SC members and by integrating a sound SCCS. The SCCS should be primarily derived from the goals of the powerful member, but with an eye towards synergistic benefit to all SC members. Below, we explain the framework in more detail.

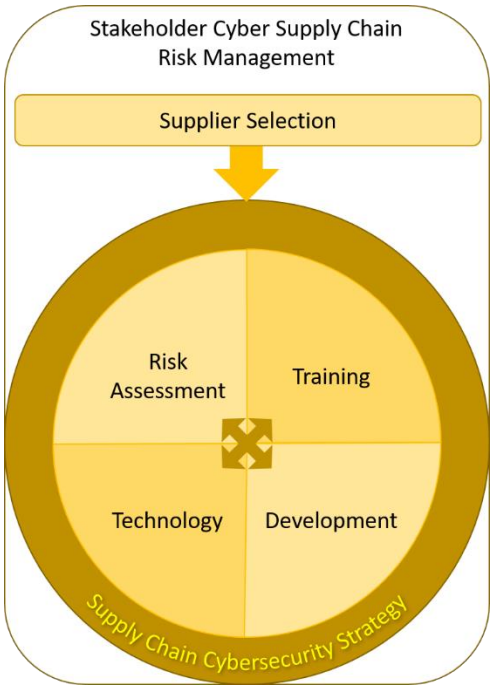

Figure 2 – Framework for Stakeholder Cyber Supply Chain Risk Management (SC-SCRM)

2.2 Supplier Selection Process

The supplier selection process is pivotal in ensuring a working SC-SCRM. To get to these details, we will need first to briefly run through the broad strokes of the larger framework encompassing SC-SCRM.

The risk management process (RMP) has variously been defined by many organizations such as NIST and the International Standards Organisation (ISO). NIST enumerates four components of the RMP as follows (NIST, 2011):

- frame risk – establish the context for risk-based decisions
- assess risk
- respond to risk
- monitor risk, continuously over time

The NIST RMP and information/communication flows among the components are depicted in Figure 3.

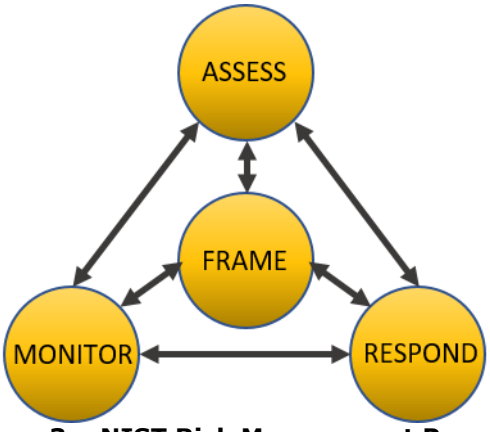

Figure 3 – NIST Risk Management Process; arrows indicated information and communications flows (NIST, 2011, p. 8)

Within NIST's FICI, the framework core expands on the above-mentioned elements to enumerate five functions: Identify, Protect, Detect, Respond, and Recover (Figure 4).

Further, they enumerate four implementation tiers to "provide context on how an organization views cybersecurity risk and the processes in place to manage that risk" (NIST, 2018, p. 8). These tiers range from Partial (Tier 1), which is informal and reactive, to Adaptive (Tier 4), which is agile and risk-informed, and are briefly summarized as follows:

Tier 1, Partial. Cybersecurity risk is managed in an ad hoc/reactive manner; practices are not formalized; generally unaware of cyber SC risks of the products/services provided and used.

Tier 2, Risk Informed. Cybersecurity risk management practices are approved by management; practices may not be organizational-level policy; generally aware of cyber SC risks, but does not act consistently or formally.

Tier 3, Repeatable. Cybersecurity risk management practices are formally approved and organizational policy; generally aware of cyber SC risks and acts formally upon the risks.

Tier 4, Adaptive. Cybersecurity risk management practices are adaptive and informed by previous and current cybersecurity activities; aware of SC risks, contributes to the SC community's understanding of risks; communicates proactively to maintain strong SC relationships.

Figure 4 – Five Functions of NIST's Framework for Improving Critical Infrastructure (NIST, 2018a)

A firm must consider which Tier a potential SC partner needs to occupy before it could become a SC member. This is somewhat analogous to setting ISO certification as a basic qualifier to be a supplier. To mitigate risks to acceptable levels, if the determined prerequisite Tier is lower than Tier 4, a road map for a SC member to gradually reach Tier 4 would minimize the exposure factor of the SC ecosystem. It is important to note that tiers assist in risk management of the power player and do not correspond to the maturity levels (NIST, 2018b).

An extensive list of criteria can be considered during a supplier selection process (Thanaraksakul & Phruksaphanrat, 2009). The list is quite comprehensive but can be broadly classified into five perspectives: (i) Financial (ii) Customer (iii) Internal Business Process, (iv) Learning and Growth, (v) Corporate Social Responsibility. The financial aspect is related to the ability of a vendor to have long term profitability. The customer aspect is related to the ability of the vendor to provide goods and services quickly as the firm's customer requirement changes. The internal business process relates to the vendor's ability to provide quality products and services at the right time and in the right quantities. The learning and growth measure is the flexibility of the vendor to adapt to changing market conditions. And, the corporate social responsibility is the ability of the vendor to be a good citizen company adhering to legal, societal, and environmental commitments.

In addition to the factors listed above, we propose that cybersecurity has reached sufficient importance, that a supplier selection process should explicitly incorporate criteria relevant to the key layers of cybersecurity – people, processes, and technology – explained as follows:

- People refers to having cybersecurity experts with appropriate qualifications in key positions as well as periodically training employees and testing their knowledge in cybersecurity awareness.
- Processes are there to ensure that SC risk tolerance and business objectives are aligned.
- The technology layer refers to having proper technology and tools in place, and that these tools are utilized in the way that would be aligned with the cybersecurity strategy of the powerful member.

An example scorecard template is in Table 1 and would help to rank potential SC participants (we provide a scored example for the use case in section 3). The specific criteria beneath the three key parts are examples and not meant to be comprehensive or specifically required in keeping with the spirit of the flexibility of FICI.

Organizations will want to craft the scorecard with items of specific importance to them and informed by their cybersecurity policy. Good sources for scorecard criteria are the categories and subcategories of the FICI framework core. Evaluating the criteria based on implementation tiers and then summing the result can provide a quantitative manner of comparison where higher scores would indicate a better potential SC partner from a cybersecurity perspective.

2.2 Training

The training component of the framework focuses on the powerful member's strategy on education, training, and awareness of the SC partners in all areas of the selection process: people, processes, and technology. The minimal tier requirement for each SC partner determined by the powerful member provides guidance on the minimal acceptable cyber hygiene levels for the SC ecosystem. Aligned cybersecurity policy and procedures of the SC ecosystem would be a means to make sure that every SC partner maintains the expected minimal cybersecurity posture.

The policies and procedures should detail important items like incident handling, incident monitoring, incident response plan, etc. Each SC partner doing periodic audits of their systems and users is necessary for the integrity of the system and user provisions. Any exploits found through the audits need to be addressed by every partner of the SC with the lead of the powerful member. The policies and procedures should address the management of data and user access for the partners leaving the SC ecosystem.

SC-SCRM Evaluation Scorecard	
People	Tier
CISO	
Network Security Engineer	
Security Analyst	
Etc. …	
Processes	Tier
Cyber Incident Response Plan	
Endpoint Monitoring	
Vulnerability Management	
Etc. …	
Technology	Tier
Email Security	
Firewalls	
Security Log Maintenance	
Etc. …	

Table 1 – Cybersecurity-focused Evaluation Scorecard template for potential SC partners

The training component would address improving the security posture of SC partners. If a partner is at the minimum acceptable tier at selection time, the training, coupled with development process of the framework progressively work towards bringing the partner as close as possible to Tier 4. It is important to note that some supply chain partners may never reach Tier 4 based on their firm size and available resources.

2.3 Development

Supplier development includes activities like site visits and personnel training with the goal of improving the capabilities and performance of the supplier. Since this requires financial investment in suppliers, Talluri, et al. propose optimization models for allocating resources among multiple suppliers to minimize risk and maintain an acceptable level of return (Talluri et al., 2010).

In the context of SC cybersecurity, natural questions to ask include: should the investment be made based on security weakness or should it be done based on the organization's ability to scale up the technological capabilities. Both are important since management may have to optimize the investment in both areas. The dynamic nature of the market requires the

entities to evolve on a continuous basis. The role of the powerful member cannot be emphasized enough to achieve the continuous improvement of the SC. As the business evolves, the organizational goals evolve for the powerful member. When the organizational goals evolve, the cybersecurity strategy evolves as well. This may require that suppliers move up the Tier structure of FICI. The powerful member should take an active role in developing the road map for other members to achieve the required Tier.

2.4 Technology

Industry 4.0 utilizes emerging technologies to improve efficiencies in SCs. Most of the emerging technologies come with unidentified cybersecurity risks. When an emerging technology is introduced to the SC ecosystem, the powerful member should vet the technology and outline the acceptable configuration/use of it for the other partners of the SC before it becomes embedded into the SC.

As an example, when considering embedded automotive network parts, researchers have identified the need to design and implement key security mechanisms to improve the cybersecurity posture of the parts, and, ultimately, the automobiles being produced, specifically: communication encryption, anomaly detection, and embedded software integrity (Studnia et al., 2013). It is likely that this category can be extended to other industries as well, especially where embedded electronic components are used.

One extension is the use of blockchain technology to provide decentralized secure ledgers for SC partners. Blockchain technology is a promising driver of common digital SC standards, but is not currently something that even the largest companies can impose on others and will require real collaboration to make it work end-to-end in a SC (Korpela et al., 2017). As SCs continue to digitize and integrate, many SMBs lack key functionalities (e.g. standards, transaction timestamps, secure information flow) that are already designed into blockchain technology.

There are many benefits that blockchain technology could bring to SCs including:

- tracing the origin (provenance) of the product/process, that is verifiable, thus preventing counterfeits
- improved trust among the members because every member has the same verified information
- improvement in data integrity because any incorrect information can be easily traced to the member who entered it
- IoT (Internet of Things) devices can be easily connected to the SC and the data is available throughout the SC thus ensuring the products conform to the requirements (e.g., pick and pack dates, storage temperatures, etc.)
- financial transactions happen quickly
- helps to achieve JIT production.

The impact of blockchain technology just on reducing counterfeit products could be tremendous. According to a 2018 report, the value of counterfeit goods in 2017 was estimated at $1.2 trillion and is likely to rise 50% to $1.82 trillion by 2020 (Research and Markets, 2017).

2.5 Risk Assessment

Managing SC risk requires a collaborative effort among the members to identify, evaluate, mitigate, and monitor events that may adversely affect the functioning of the SC (Ho et al., 2015). Cybercriminals usually exploit the weakest link in the SC. One study attempting to differentiate sources of security incidents indicates that 23% of SC security incidents involve current partners while 45% involve former partners (PwC, 2014). Hence, the risk management strategies in an SC context must include all partners.

SCs face a myriad of security threats to products/assets as well as information systems. The National Cyber Security Center (NCSC) classifies cybersecurity threats into un-targeted and targeted attacks (NCSC, 2016). Targeted attacks are directed towards a specific entity. Examples include distributed denial of service (DDoS), subverting the supply chain (attacking equipment or software used by the organization), and spear-phishing. Ransomware, phishing, spoofing, and water holing are examples of untargeted attacks as they don't have a specific target. The organizations need to know the weak points in their SCs to ensure a robust risk mitigation strategy (Smith et al., 2007). Ghadge, et al. classify these weak points into three dimensions: technical, human, and physical (Ghadge et al., 2019). Boone suggests that the strength of an SC's defense against cyber threats is only as good as the most susceptible member in the supply chain (Boone, 2017).

Now, we suggest a scorecard for conducting a cybersecurity risk assessment of SC members

assessed from the perspective of the SC powerful member.

NIST has defined risk as

> a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence (NIST, 2012, p. 6).

This definition implies:

$$\boldsymbol{impacts} * \boldsymbol{likelihood} = \boldsymbol{risk}$$

Switching the term order, substituting consequences for the word impacts, and further understanding likelihood as the combination of a threat exploiting a vulnerability (NIST, 2012), we can extrapolate to the well-known formula:

$$(\boldsymbol{threat} * \boldsymbol{vulnerability}) * \boldsymbol{consequence} = \boldsymbol{risk}$$

Driving one of the variables in the formula to zero will make the risk go away; however, a zero value for any variable may well require infinite resources and is generally impractical. Hence, the SC members will generally expend resources in a balanced manner to minimize the value of each of the variables.

Table 2 shows the general structure of the proposed risk assessment matrix template integrating the key layers of cybersecurity within the organization of the powerful member, current SC partners, and former partners.

The people aspect ensures that each SC partner employs key, qualified cybersecurity personnel and implements a thorough cybersecurity awareness training program to address one of the biggest threats: insiders. Process evaluation ensures that any changes to SC partner structure do not impact the alignment of that partner within the SC ecosystem. Also, if any changes happen to the powerful member's cybersecurity processes, due to the introduction of new tools for example, the alignment is updated appropriately for each partner. The technology layer ensures that partners update their tools and monitor their use IAW guidelines provided by the powerful member.

	Threat	Vulnerability	Consequence	Risk
Organization 1. People 2. Process 3. Technology				
Current Partners 1. People 2. Process 3. Technology				
Former Partners 1. People 2. Process 3. Technology				
			Total Risk	

Table 2 – Risk Assessment Matrix Template

The primary risk assessment by the powerful member does not preclude each SC partner also conducting assessments in this manner. The most cybersecurity-mature SC will encourage this and have key personnel meet periodically to more thoroughly evaluate the overall cybersecurity risk of the SC ecosystem.

3. SUPPLY CHAIN SUPPLIER SELECTION USE CASE

This lightweight use case is presented as a thought experiment and motivated in part by the 2013 Target breach and the 2017 breach of a casino (DarkTrace, 2017). Hackers stole 40,000,000 credit card numbers and cost Target $202 million after they were able to steal network credentials from a vendor that Target used to provide and monitor refrigeration and HVAC systems. An unnamed casino had its list of wealthy patrons stolen through a compromised "smart" fish tank thermometer used to monitor and regulate temperature, salinity, and feeding schedules.

We imagine a company, BigAg, selling agricultural products wholesale to supermarkets. Considering current pandemic conditions, BigAg wants to adjust their business practices to gain better visibility on the daily health of the workers throughout their SC. One way they would like to do this is to have worker temperatures regularly reported to the BigAg HQ.

BigAg looks for a new SC partner to handle the gathering of the worker temperatures and reduces the viable candidates to three different companies with different solutions. ManualTemp (MT) company hires local health care workers part-time to take worker temperatures. The data is collected periodically throughout each day in a

traditional manner and reported via apps that workers download to their personal phones. HatTemp (HT) manufactures hats designed to take worker temperatures at time intervals as often as every five minutes and is collected wirelessly. TempStation (TS) installs contactless infrared thermometers at strategic locations around company facilities capable of taking temperatures from up to 15 feet away. The stations can be wired into a network or a wireless access point for wireless transmission of data.

From this sketch, we will present a portion of the process envisioned with the framework as the powerful member considers the supplier selection process and the follow-on TDTR. Table 3 shows a hypothetical abbreviated and consolidated SC-SCRM evaluation scorecard for a few of the very many areas that would be assessed during the selection process.

In this truncated example, we will consider two criteria as exemplars for how the scorecard will be used. First, in the People section of the scorecard, we find that MT does not have anyone formally assigned to the position of a CISO, though someone is handling some of the duties normally associated with that position; HT established the position within the past year; and TS has had the position in place for several years. Second, from the Processes section, we note that Endpoint Monitoring is done by MT in an ad-hoc manner (employees whose phones act up are directed to contact tech support); HT and TS have an established and repeatable process for monitoring their hats and infrared thermometers, respectively.

Assuming the full scorecard is like the snippet (Table 3), we expect TS to be selected as the new SC partner due to higher tier scores across the board. (*NOTE: this evaluation is strictly cybersecurity-based; it is entirely reasonable that the selection might be different for other reasons e.g., budget constraints.*)

Carefully considering TempStation's cyber-security posture during selection does not complete the SC-SCRM process, but merely ensures it is well-begun. As long as TS is a SC member, they will need to regularly cycle through the bottom portion of the SC-SCRM (Figure 2) to ensure that training, development, technology, and risk assessment (TDTR) are informed by BigAg's SC cybersecurity strategy and continually improved.

SC-SCRM Evaluation Scorecard			
People	Tier		
	MT	HT	TS
CISO	1	2	3
Network Security Eng	2	2	3
Processes	MT	HT	TS
Cyber Incident Response Plan	1	3	3
Endpoint Monitoring	1	3	3
Technology	MT	HT	TS
Intrusion Detection System	2	3	3
Security Log Maintenance	2	3	4

Table 3 – Abbreviated and Consolidated Example Selection Evaluation Scorecard Comparing ManualTemp, HatTemp, and TempStation.

BigAg training might include adding the TS CISO to a peer group of all SC partner CISOs to meet quarterly for general professional development as well as table-top evaluations of the SC cybersecurity risk. The development example reads more like technology to me than development. Maybe something in line with the following might fit better: Development activities might include tracking the efforts made by TS to obtaining a higher tier in the various categories evaluated during selection. Cybersecurity efforts related to technology could involve coordinating improvements in wireless security (e.g. ensuring all SC partner WLANs incorporate WPA2). Finally, conducting regular cybersecurity-focused risk assessments should require annual formal evaluation with the use of a tool like the matrix in table 2 to identify risks to the overall SC.

4. CONCLUSIONS

Cybersecurity has been attracting a lot of attention for the past 20 years and that attention seems to be only intensifying based on the increasing need for cybersecurity professionals ((ISC)2, 2019). Suggested tools and techniques for dealing with SC cybersecurity have generally lagged other areas as evidenced by NIST not adding a Supply Chain category to the FICI until 2018.

SCs are often characterized by power asymmetries. We have argued that the onus of responsibility for overall SC cybersecurity falls on the shoulders of the *powerful member*. Naturally, the question arises as to what role the powerful member plays and to what degree. We

suggest that they begin the cybersecurity focus when identifying the right members to include in the SC. To this end, we formulated a Stakeholder Cyber Supply Chain Risk Management (SC-SCRM) framework which includes: Supplier Selection and four components intended for use as a continuous improvement process – Training, Development, Technology, and Risk Assessment (TDTR). The TDTR are all informed by the Supply Chain Cybersecurity Strategy (SCCS). We present the above framework in order to set the stage for future studies to determine where leader-driven decision makes the most sense and how to quantify it in application.

5. REFERENCES

BlueVoyant. (2020). *Global Insights: Supply Chain Cyber Risk* [Brochure]. New York, New York: Opinion Matters.

Boone, A. (2017, February). Cyber-security Must be a C-suite Priority. Computer Fraud & Security 2017(2), pp. 13-15. DOI: https://doi.org/10.1016/S1361-3723(17)30015-5

Darktrace. (2017). *Global Threat Report 2017, Selected Case Studies* (Rep.). Retrieved from https://cdn2.hubspot.net/hubfs/2784256/1_nat_2017_recap/Presentations/Darktrace%20-%20Global%20Threat%20Report%202017.pdf?t=1528334118161

Ghadge, A., Weiß, M., Caldwell, N.D. & Wilding, R. (2019), Managing Cyber Risk in Supply Chains: A Review and Research Agenda. Supply Chain Management, 25(2), pp. 223-240. Retrieved from https://dspace.lib.cranfield.ac.uk/bitstream/handle/1826/14843/Managing_cyber_risk_in_supply_chains-2019.pdf?sequence=4

Gutzmer, I. (2017, September 26). Equifax Announces Cybersecurity Incident Involving Consumer Information. Retrieved from https://www.equifaxsecurity2017.com/2017/09/07/equifax-announces-cybersecurity-incident-involving-consumer-information/

Ho, W., Zheng, T., Yildiz, H. & Talluri, S. (2015). Supply Chain Risk Management: A Literature Review. International Journal of Production Research, 53:16, 5031-5069. DOI: 10.1080/00207543.2015.1030467

(ISC)2. (2019). Strategies for Building and Growing Strong Cybersecurity Teams, (ISC)2 Cybersecurity Workforce Study, 2019. Retrieved from https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=1827084508A24DD75C60655E243EAC59ECDD4482

Imai, M. (1986). The Key to Japan's Competitive Success. McGraw-Hill.

Korpela, K., Hallikas, J., & Dahlberg, T. (2017). Digital Supply Chain Transformation toward Blockchain Integration. Retrieved from http://128.171.57.22/bitstream/10125/41666/paper0517.pdf

Krebs, B. (2014, February 5). Target Hackers Broke in Via HVAC Company. Retrieved from https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

Lee, H.L. (2004, October). The Triple-A Supply Chain. *Harvard Business Review*, 82 102-12, 157. Retrieved from https://hbr.org/2004/10/the-triple-a-supply-chain

McCandless, D., & Evans, T. (2020, December 09). World's Biggest Data Breaches & Hacks. Retrieved from https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Mulligan, D.K. & Schneider, F.B. (2011). Doctrine for Cybersecurity. *Daedalus*, 140(4), 70-92.

Munson, C.L., Rosenblatt, M.J., & Rosenblatt, Z. (1999). The Use and Abuse of Power in Supply Chains. *Business Horizons*. 42. 55-65. Retrieved from https://www.researchgate.net/publication/4884612_The_Use_and_Abuse_of_Power_in_Supply_Chains

National Institute of Standards and Technology (NIST). (2018a, August 10). Cybersecurity Framework: The Five Functions. Retrieved from https://www.nist.gov/cyberframework/online-learning/five-functions

National Institute of Standards and Technology (NIST). (2020, June 22). Cyber Supply Chain Risk Management: C-SCRM. Retrieved from https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management

National Institute of Standards and Technology (NIST). (2018b, April 16). Framework for Improving Critical Infrastructure Cybersecurity. Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

National Institute of Standards and Technology (NIST). (2012, September). Guide for Conducting Risk Assessments. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

National Institute of Standards and Technology (NIST). (2011, March). Managing Information Security Risk. Retrieved from https://nvlpubs .nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

PwC. (2014, September 30). Managing Cyber Risks in an Interconnected World. Retrieved from https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf

Research and Markets. (2017, December). Global Brand Counterfeiting Report, 2018. Retrieved from https://www.researchandmarkets.com /reports/4438394/global-brand-counterfeiting-report-2018

Ross, R., Pillitteri, V., Dempsey, K., Riddle, M., & Guissanie, G. (2020, February). Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. Retrieved from https://nvlpubs.nist.gov /nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

Smith, G.E., Watson, K.J., Baker, W.J., & Pokorski II, J.A. (2007) A Critical Balance: Collaboration and Security in the IT-Enabled Supply Chain, International Journal of Production Research, 45:11, 2595-2613, DOI: 10.1080/00207540601020544

Studnia, I., Nicomette, V., Alata, E., Deswarte, Y., Kaâniche, M. & Laarouchi, Y. (2013). Survey on Security Threats and Protection Mechanisms in Embedded Automotive Networks. 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop. Retrieved from https://hal .archives-ouvertes.fr/hal-00852244/file /Studniaetal.pdf

Talluri, S., Narasimhan, R. & Chung, W. (2010, November 16). Manufacturer Cooperation in Supplier Development Under Risk. European Journal of Operational Research, 207(1), pp 165-173.

Thanaraksakul, W. & Phruksaphanrat, B. (2009). Supplier Evaluation Framework Based on Balanced Scorecard with Integrated Corporate Social Responsibility Perspective. Proceedings of the International MultiConference of Engineers and Computer Scientists (IMECS). Retrieved from http://www.iaeng.org/publication/IMECS2009/IMECS2009_pp1929-1934.pdf.

UpGuard. (2017, July 12). Cloud Leak: How A Verizon Partner Exposed Millions of Customer Accounts: UpGuard. Retrieved from https://www.upguard.com/breaches/verizon-cloud-leak

Webmaster, A&S. (2020, December 10). Cybersecurity Maturity Model Certification (CMMC). Retrieved from https://www.acq .osd.mil/cmmc/