Technology Innovation Management Review

April 2015

Cyber-Resilience in Supply Chains

Welcome to the April 2015 issue of the *Technology Innovation Management Review*. This month's editorial theme is Cyber-Resilience in Supply Chains. We welcome your comments on the articles in this issue as well as suggestions for future article topics and issue themes.

Carleton UNIVERSITY

www.timreview.ca

Publisher

The *Technology Innovation Management Review* is a monthly publication of the Talent First Network.

ISSN

1927-0321

Overview

The *Technology Innovation Management Review* (TIM Review) provides insights about the issues and emerging trends relevant to launching and growing technology businesses. The TIM Review focuses on the theories, strategies, and tools that help small and large technology companies succeed.

Our readers are looking for practical ideas they can apply within their own organizations. The TIM Review brings together diverse viewpoints – from academics, entrepreneurs, companies of all sizes, the public sector, the community sector, and others – to bridge the gap between theory and practice. In particular, we focus on the topics of technology and global entrepreneurship in small and large companies.

We welcome input from readers into upcoming themes. Please visit timreview.ca to suggest themes and nominate authors and guest editors.

Contribute

Contribute to the TIM Review in the following ways:

- Read and comment on articles.
- Review the upcoming themes and tell us what topics you would like to see covered.
- Write an article for a future issue; see the author guidelines and editorial process for details.
- Recommend colleagues as authors or guest editors.
- Give feedback on the website or any other aspect of this publication.
- Sponsor or advertise in the TIM Review.
- Tell a friend or colleague about the TIM Review.

Please contact the Editor if you have any questions or comments: timreview.ca/contact

About TIM

The TIM Review has international contributors and readers, and it is published in association with the Technology Innovation Management program (TIM; timprogram.ca), an international graduate program at Carleton University in Ottawa, Canada.

Editorial: Cyber-Resilience in Supply Chains

Chris McPhee, Editor-in-Chief
Omera Khan, Guest Editor

From the Editor-in-Chief

Welcome to the April 2015 issue of the *Technology Innovation Management Review*. The editorial theme of this issue is **Cyber-Resilience in Supply Chains**, and I am pleased to welcome our guest editor, **Omera Khan**, Professor of Operations Management at the Technical University of Denmark.

We hope you enjoy this issue of the TIM Review and will share your comments online. In May, we will be publishing a general, unthemed issue, which will be followed by an issue on **Cybersecurity** in June.

For future issues, we welcome your submissions of articles on innovation management, entrepreneurship, and other topics related to the launching and growing of technology companies. Please contact us (timreview.ca/contact) with article topics and submissions, suggestions for future themes, and any other feedback.

Finally, some of our readers may be interested to know that La Salle – Ramon Lull University in Barcelona, Spain, will be holding a doctoral consortium on the theme of "Digital Innovation" from July 2nd to 3rd, 2015. The deadline for the submission of abstracts is April 30th. For details, please see the Innova Institute blog: tinyurl.com/lbtp5qp

Chris McPhee
Editor-in-Chief

From the Guest Editor

It is my pleasure to be the invited guest editor for this month's issue on Cyber-Resilience in Supply Chains. Our growing interconnectivity in cyberspace has exposed us to new and greater vulnerabilities, and we have recently witnessed the catastrophic damage that cyber-attacks can cause to a firm's reputation and shareholder value. Supply chain cyber-resilience can be defined as the capability of a supply chain to maintain its operational performance when faced with cyber-risk.

Response measures to cyber-risks are being developed and researched, and the World Economic Forum has been at the forefront of advocating for the importance of addressing cyber-resilience. However, few if any, methods are currently robust enough to support cyber-resilience in supply chains.

Supply chain cyber-resilience has received less attention compared to cyber-risk, security, and resilience generally. An explanation for this could be because naturally we view information technology (IT) as solely responsible for cyber-related issues. This compartmentalization of disciplines is at the heart of the problem and must be overcome to achieve supply chain cyber-resilience. Cyber-attacks are crippling the world's most sophisticated supply chains, thereby causing losses that run into billions of dollars, but a disconnect between IT professionals and supply chain professionals means that determining accountability for this risk could take far longer than tackling the issue itself. A more coordinated approach between IT and supply chain professionals, led by an organizational culture that seeks to build resilience rather than just react to cyber-attacks, may have higher chances of survival as it adapts and aligns to a dynamic defense strategy against a growing threat.

The aim of the collection of articles presented in this issue is to highlight the significance of this topic and develop a shared understanding of the definition, theory, and managerial implications of cyber-risk and cyber-

Editorial: Cyber-Resilience in Supply Chains

Chris McPhee and Omera Khan

resilience in supply chains. And, in doing so, the issue seeks to develop an agenda for future research that provides solutions to the challenges of developing a supply chain cyber-resilience strategy, the tools and methods to respond to cyber-breaches in the supply chain, and case studies of best practice.

In the first article, **Omera Khan** and **Daniel Alberto Sepúlveda Estay**, a Professor and a PhD Student from the Technical University of Denmark, set the scene by developing a research agenda for future research after exploring the critical frameworks that exist in the supply chain risk management domain. The article concludes with prescriptions for academics and practitioners that must be taken to expand our understanding of supply chain cyber-resilience.

Next, **Luca Urciuoli**, Associate Research Professor in the Zaragoza Logistics Center in Spain, describes the challenges of implementing information and communication technologies to support the resilience of complex global supply chains, which could have an adverse effect if not addressed correctly. The article sheds light on the managerial strategies to improve cyber-resilience such as combining current technologies and services to achieve cyber-resilience.

In the third article, **Adrian Davis**, Managing Director of the Europe, Middle East, and Africa (EMEA) region at (ISC)2 in the United Kingdom, provides practical solutions to the challenges of achieving supply chain cyber-resilience, suggesting an information-centric approach to protect information early on in the supply chain. The key point here is to integrate information into the procurement cycle to build cyber-resilience, and a list of actions is provided to facilitate this.

Then, **Hugh Boyes**, Principal Fellow at WMG at the University of Warwick, United Kingdom, applies a model for cybersecurity for both product and service supply chains that is adapted from the Parkerian hexad to explore the security and trustworthiness facets of supply chain operations that may impact cyber-resilience. This model is particularly relevant to complex, time-critical, and cyber-physical systems and is currently being documented for use in the construction industry.

In the fifth article, **Lars Jensen**, CEO and Co-Founder of CyberKeel, an international maritime cybersecurity company based in Copenhagen, Denmark, explores cyber-resilience challenges in the maritime industry, which, as this article reveals, has seen a significant increase in levels of cyber-attacks. After describing the nature and characteristic of cyber-threats, the article argues for an urgent response by the maritime industry to rapidly develop a set of best practice guidelines to reduce the risk profile and increase cyber-resilience.

Finally, **Richard Wilding**, Professor and Chair of Supply Chain Strategy at Cranfield School of Management in the United Kingdom, and **Malcolm Wheatley**, a Visiting Fellow at Cranfield School of Management, answer the question "how can I secure my digital supply chain?" by providing insights into understanding and addressing the challenges of securing the supply chain. The authors identify five areas that chief executives and directors of manufacturing and supply chains must focus on securing.

We hope you enjoy reading this month's issue on supply chain cyber-resilience. The articles in this issue present us with an introduction and explanation of the nature of supply chain cyber-resilience, and in doing so, they provide both academics and practitioners with key insights and challenges that may help them to address the growing threat from cyberspace.

Omera Khan
Guest Editor

Editorial: Cyber-Resilience in Supply Chains

Chris McPhee and Omera Khan

About the Editors

Chris McPhee is Editor-in-Chief of the *Technology Innovation Management Review*. He holds an MASc degree in Technology Innovation Management from Carleton University in Ottawa, Canada, and BScH and MSc degrees in Biology from Queen's University in Kingston, Canada. Chris has over 15 years of management, design, and content-development experience in Canada and Scotland, primarily in the science, health, and education sectors. As an advisor and editor, he helps entrepreneurs, executives, and researchers develop and express their ideas.

Omera Khan is a Full Professor of Operations Management at the Technical University of Denmark. She works with leading organizations on a range of supply chain and logistics issues and is advisor to many universities developing courses in logistics, supply chains, and operations management. She has led and conducted research projects commissioned by government agencies, research councils, and companies in supply chain resilience, responsiveness, sustainability, and the impact of product design on the supply chain. Her latest area of research focuses on cyber-risk and resilience in the supply chain. Omera is an advisor to many organizations and provides specialist consultancy in supply chain risk management. She is a highly acclaimed presenter and is regularly invited as a keynote speaker at global conferences and corporate events. She has published her research in leading journals, contributed to several book chapters, and is lead author of *Handbook for Supply Chain Risk Management: Case Studies, Effective Practices and Emerging Trends*. She founded and was Chair of the Supply Chain Risk and Resilience Research Club and the Product Design and Supply Chain Special Interest Group. She has also been a visiting professor at a number of leading business schools.

Citation: McPhee, C., & Khan, O. 2014. Editorial: Cyber-Resilience in Supply Chains. *Technology Innovation Management Review*, 5(4) 3–5.
http://timreview.ca/article/884

Keywords: supply chains, cyber-resilience, resilience, cybersecurity, cyber-attacks, cyber-risk

Supply Chain Cyber-Resilience: Creating an Agenda for Future Research

Omera Khan and Daniel A. Sepúlveda Estay

> *"Resilience is all about being able to overcome the unexpected. Sustainability is about survival. The goal of resilience is to thrive."*
>
> Jamais Cascio
> Writer and futurist specializing in design strategies

Supply chains have become more vulnerable in recent years, and high-profile cyber-attacks that have crippled the supply chains of well-known companies reveal that the point of entry for hackers is often through the weakest link in the chain. Exacerbated by growing complexity and the need to be visible, these supply chains share vital streams of information every minute of the day, thereby becoming an easy and highly lucrative target for talented criminals, causing financial losses as well as damaging brand reputation and value. Companies must therefore invest in supply chain capabilities to withstand cyber-attacks (i.e., cyber-resilience) in order to guard against potential threats. They must also embrace the reality that this often-unknown dimension of risk is the "new normal". Although interest on this topic has grown in the business world, less has been reported by the academic community. One reason for this could be due to the convergence of two different disciplines, information technology and supply chains, where supply chain cyber-risk and cyber-resilience appear to have a natural fit. The topic of cyber-resilience in supply chains is still in early stages of development, and this is one of the first journals to focus a special issue on it. Currently, the closest academic literature is within the realms of supply chain risk and resilience, where numerous models and frameworks exist. In this article, this literature is explored to identify whether these models can incorporate the dimension of cyber-risk and cyber-resilience. In doing so, we create a research agenda for supply chain cyber-resilience and provide recommendations for both academia and practice.

Introduction

Supply chain management has become dependent on electronic systems; since the 2000s, we have seen the emergence of information technology solutions to support business operations, to share information, to connect businesses, and to generate greater visibility along supply chains in order to gain knowledge and control of processes. On the other hand, although supply chains have pursued aspects such as the standardization of business processes, increased communication, connectivity, and data exchange, the vulnerability of these systems to cyber-attacks is nevertheless increasing. Why is this? In modern supply chains, information is shared digitally more than any other way, and supply chains are so reliant on good quality information that, without it, supply chain managers cannot make decisions on forecasts, production, distribution, etc. Equally importantly, poor data leads to poor decisions and performance. So, even with the most efficient and responsive supply chain, performance will be greatly compromised without good quality information.

For supply chains to thrive, managers must recognize that cyber-attacks are becoming common occurrences and that the "new normal" operating environment is one that is increasingly impacted by unknown risks. A key lesson for supply chain managers is that cyber-attacks do not always "come through the front door"; a business can be greatly impacted by an attack on the weakest link in their supply chain. A key difficulty with cyber-attacks is that often a business will not know the

Supply Chain Cyber-Resilience: Creating an Agenda for Future Research

Omera Khan and Daniel A. Sepúlveda Estay

types of cyber-risks to which it has exposure, until it realizes that it is being attacked. Therefore, businesses must develop cyber-resilience to protect their supply chains.

Cyber-attacks can cause considerable economic costs to the companies that suffer these breaches, although the costs may not be noticed until after the damage is done. Estimates of the annual costs from cyber-crimes range from $375 billion to $575 billion (USD) (Intel Security, 2014), with significant effects on supply chains and resulting business performance with customers. Missing or erroneous data and information in supply chains, as a result of cyber-attacks, can lead to undesirable effects as diverse as intellectual property breaches, sub-standard or interrupted operations, sensitive data custody breaches, and decreases in service level to final customers. For example, some estimates indicate annual losses of £9.2bn from the theft of intellectual property and a further £7.6bn from industrial espionage.

Businesses that are able to understand what data is critical, where it is, who has access to it, and who is responsible for it, as well as where potential risks are in terms of information and data in the supply chain, are those that will be able to correctly communicate these risks to the supply chain in order to implement actions to mitigate them.

However, there has been a lack of managerial action to acknowledge the relevance and impact of cyber-crime (Burnson, 2013; Deloitte, 2012, 2013). It has been stated that "only a few CEOs realize that the real cost of cyber-crime stems from delayed or lost technological innovation" (Bailey et al., 2014) and companies have likely underestimated their risk (Intel Security, 2014). This is, either by delayed decision making or by a lack of awareness, the resulting inaction is leading to higher organizational costs from cyber-crimes.

This inaction is compounded by the increasing complexity of global supply chains and the speed and connectivity of operations required by companies to stay competitive. Furthermore, the growing skill of the attackers to find novel ways of accessing crucial data (Reuters, 2012), and the limited information and tools available to manage these threats, requires organizations to be more resilient to cyber-attacks that can cripple their supply chains.

Companies can prepare for potential attacks by applying appropriate supply chain risk-management tools and techniques both to reduce the likelihood of an intrusion and to deal with any disruption should an attack be successful. Every business that depends on a supply chain needs to build in cyber-resilience. But what exactly is cyber-resilience in the context of supply chains, and how can it be incorporated into current supply chain risk-management approaches?

Cyber-risk has been defined by the Institute for Risk Management (IRM, 2015) as "any risk of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its information technology systems". The ISO 27005:2008 defines information security risk as "the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization" (BSI, 2008). Both of these terms are being widely used in industry, and this article will consider these terms as equivalent.

We define supply chain cyber-resilience "as the capability of a supply chain to maintain its operational performance when faced with cyber-risk".

In light of the above challenges, the purpose of this article is to create an agenda for future research that could help supply chain and IT personnel to recognize and take a proactive team-based approach to supply chain cyber-resilience. More specifically, the aims of this study are to:

1. Explore current supply chain risk and resilience frameworks

2. Analyze these frameworks and determine whether they incorporate cyber-risk

3. Create a research agenda for cyber-risk and cyber-resilience.

The remainder of this article is structured as follows. First, the process used to find and review the key literature is explained. Next, the main findings of the literature review are discussed. Finally, a research agenda for supply chain cyber-resilience is proposed, including recommendations for both academia and industry.

Methodology

A systematic literature review was conducted, based on documented guidelines (Tranfield et al., 2003) through which a comprehensive, explicit, and reproducible method is followed. This method consists of ten steps that can be grouped into five main phases:

Supply Chain Cyber-Resilience: Creating an Agenda for Future Research

Omera Khan and Daniel A. Sepúlveda Estay

1. **Planning:** The planning phase focused on defining a review question to guide the search: "Do the current supply chain risk and resilience frameworks incorporate cyber-risk?"

2. **Searching:** The searching phase was guided by the identification of the relevant databases where the search was to be done, the keywords to be used during these searches, and the appropriate timeframe for the resulting documents to be included in the research. We searched for literature using the following databases: Scopus, Web of Science, ProQuest, and Google Scholar. The search keywords were determined from a knowledge domain analysis around the concept of cyber-resilience for the supply chain (see Figure 1). The three main knowledge domains to be scanned were identified as "supply chain management", "information technology management", and "risk (& resilience) management".

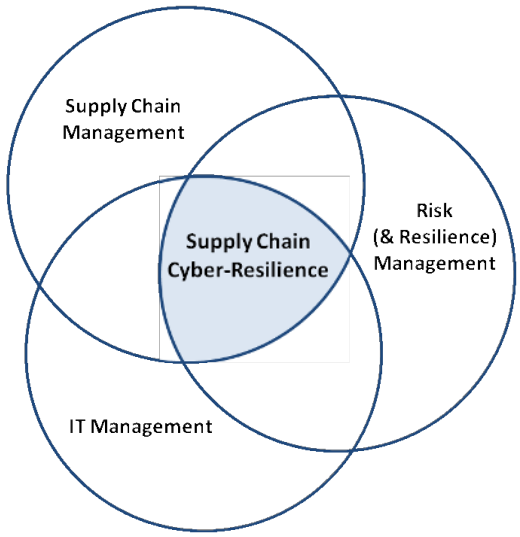

Figure 1. Main knowledge domains in supply chain cyber-risk management

3. **Screening:** After the initial, broad literature search was carried out, we conducted a preliminary analysis of the document titles and abstracts, if available. This step was followed by a more detailed analysis of the document abstracts, in the case of papers, and extended content in other cases. We applied explicit inclusion and exclusion criteria (e.g., document type, themes covered, research approaches) to identify a refined selection of documents for this analysis. Finally, the references of this refined set of articles were reviewed to identify relevant documents that might not have been identified through our initial broad search. Our final list consisted of 213 documents (24 articles, 137 peer-reviewed journal papers, 51 reports by specialized agencies, and 1 thesis). The documents covered the areas of supply chain risk management (131 documents), supply chain cyber-risk management (SCCRM), and information technology risk management (44 documents), ranging from the years 1998 to 2015.

4. **Extracting and synthesizing:** The documents were analyzed and synthesized using a spreadsheet format that allowed us to categorize the documents according to methodological approaches, contexts, outcomes, etc.

5. **Reporting:** In the next section, we report on our findings from the literature review.

Findings

Some of the earliest evidence of supply chain resilience can be found in the work of Christopher and Peck (2004), which was derived from earlier research on supply chain agility as a way of counteracting for uncertainty in the demand (Christopher & Towill, 2001), This perspective emerged after the foot-and-mouth disease event in the United Kingdom and the 9/11 terrorist attacks in United States, both of which occurred in 2001. Christopher and Peck proposed a reference model for the characterization of resilience in the supply chain, and the main aspects contributing to supply chain resilience were identified as re-engineering, organizational culture, agility, and collaboration.

Sheffi and Rice (2005) presented a disruption model based a proposed disruption theory for production systems (Asbjornslett, 1999), where this model was represented as a transient decrease in process performance. The Sheffi and Rice model identified eight sequential phases describing a disruption event: preparation, disruptive event, first response, initial impact, time of full impact, preparation for recovery, recovery, and long-term impact. Based on this model, Sheffi and Rice propose an enterprise "vulnerability map" through which the different disruption event probabilities and consequences are compared and ranked for prioritization.

Sheffi and Rice (2005) also identified product demand as the main source of uncertainty in the supply chain and acknowledged the increase in global uncertainty due to increased customer expectations, more global competition, longer and more complex supply chains, greater product variety, and shorter product lifecycles.

Supply Chain Cyber-Resilience: Creating an Agenda for Future Research

Omera Khan and Daniel A. Sepúlveda Estay

They considered organizational resilience as a strategic initiative to reduce vulnerability and therefore reduce the likelihood of occurrence of a disruption. Finally, they identified three important factors for building resiliency in an organization: redundancy, flexibility, and cultural change.

A number of other resilience frameworks have been suggested in literature. Linkov and colleagues (2013) proposed a resilience matrix of four steps representing a process for the event management cycles of disruptions: i) plan/prepare, ii) absorb, iii) recover, and iv) adapt. Each of these steps are described for different domains within the organization (i.e., physical, information, cognitive, and social). These authors have further suggested how to measure resilience according to this matrix.

Based on the framework proposed by Christopher and Peck (2004) as well as an empirical research study to identify vulnerabilities and capabilities within organizations, Pettit, Fiskel, and Croxton (2010) proposed the supply chain resiliency assessment and management (SCRAM) framework. This framework identifies an active relationship between the capabilities and the vulnerabilities in an organization, and its resulting resilience. They argue that the level of resilience that a company has to aim for is a balance between developing too many vulnerabilities (due to a lack of investment in capabilities), which could result in disruptions with undesirable economic effects, and investing in too many capabilities, which would erode profitability. Hence, they highlight an economic tradeoff between investment (capabilities) and risk (vulnerabilities).

Blackhurst, Dunn, and Craighead (2011) proposed a global resiliency framework based on systems theory and the framework proposed by Sheffi and Rice (2005). They distinguish between "resilience enhancers" and "resilience reducers", which are organizational attributes that either increase or decrease the ability of a firm to recover quickly and efficiently from a disruptive event. They identified 13 resilience enhancers and seven resilience reducers, each within three categories. Their work derives these attributes from an industrial setting and therefore can serve as basis for further research in the empirical confirmation of these or other resilience attributes.

The World Economic Forum (WEF, 2013) presented a resilience framework as part of its Supply Chain Risk Initiative. This framework attempts to quantify the risk to an organization's physical and intangible assets through a combination of effects from the existing risks to the organization and its vulnerabilities. The World Economic Forum's (WEF, 2013) resilience report also provides four recommendations for organizations to build resilient supply chains: i) put in place strong policies for the creation and adoption of resilience standards; ii) develop agile and adaptable strategies in organizations; iii) use data-sharing platforms for risk identification and response; and iv) enter into partnerships that involve all stakeholders in the risk assessment process.

Cyber-risks within the supply chain resilience framework

Our literature review did not find any supply chain resilience framework that incorporated the phenomenon of cyber-risk or information risk explicitly. However, our analysis revealed that the most influential sources for the development of cyber-resilience policy are the insurance industry, governmental requirements, and international organizations such as the World Economic Forum.

In 2012, the World Economic Forum created an initiative called "Partnering for Cyber-Resilience", led by Elena Kvochko, as a response to the increasing importance of cybersecurity. With more than 100 organizations involved, this initiative has created a series of reports describing principles for cybersecurity, recognizing interdependence, leadership, integrated risk management, and uptake by partners in the supply chain, as crucial aspects for resilience building. Additionally Kvochko has recently published an initial framework for the measurement of cyber-threats, through the calculation of a cyber-risk value and by combining eight factors grouped in three categories: vulnerability, assets, and attacker profile (WEF, 2015).

At a government level, there are several initiatives in place concerning cyber-risk and cybersecurity. In 2003, the United States government published the "National Strategy to Secure Cyberspace" (White House, 2003), and as part of a wider strategy from the Department of Homeland Security as a response to the 9/11 terrorist attacks and in line with Presidential Directive 63, which provides a framework for the protection of critical infrastructure (White House, 1998). In 2005, Germany started the "National Plan for Information Infrastructure Protection", with its main objectives being prevention, preparedness, and sustainability of the information infrastructure through the setting of international standards (German Federal Ministry of the Interior, 2005). By 2015, all EU member states except Portugal had published national cybersecurity strategies, with Estonia

Supply Chain Cyber-Resilience: Creating an Agenda for Future Research

Omera Khan and Daniel A. Sepúlveda Estay

having been the first in 2008 (ENISA, 2015; Keegan, 2014). In 2013, the United States government released Presidential Policy 21 and Executive Order 13636 to focus national attention on cyber-infrastructure resilience. In particular, Executive Order 13636 establishes a risk-based standard to protect critical infrastructure against cyber-threats. However, standards based on risk assessment do not necessarily create resilience (Linkov et al., 2013).

Conclusions and Recommendations

Our systematic literature review highlights that there is limited literature and no specific frameworks for cyber resilience in the supply chain, despite the increasing importance of the topic. The main supply chain resilience theories were proposed in the early 2000s, and the main advancements to those theories have been through the empirical identification of organizational attributes that increase or decrease resilience, as well as theoretical relationships between organizational vulnerabilities and capabilities as related to resilience. Additionally, we found that the existing supply chain resilience frameworks could be extended to consider cyber-risks through aspects such as cultural change (Sheffi & Rice, 2005) or collaboration and organizational culture (Christopher & Peck, 2004). Cyber resilience theory can also be advanced through the empirical quantification of the cyber-resilience of an organization, through case studies and stress testing of organizations with techniques such as non-invasive games (Gerencser et al., 2003).

A key contribution of this article is a definition for supply chain cyber-resilience: "the capability of a supply chain to maintain its operational performance when faced with cyber-risk". Furthermore, as a result of this study, we offer the following recommendations for academia with the goal of developing a future research agenda for supply chain cyber-resilience:

1. **Develop theory to demystify cyber-risk and cyber-resilience in supply chains:** Academics should conduct in-depth (systematic) literature reviews that confirm or expand on this study to devise methods of incorporating cyber-resilience with existing frameworks in supply chain resilience and indeed develop new models and frameworks. Finally, and fundamentally, they should align supply chain thinking and personnel with information technology issues and personnel to develop a team approach to supply chain cyber-resilience.
2. **Develop applicable tools and techniques:** There is a need for models (e.g., models of dynamic behaviour, machine-learning models for real-time monitoring of performance conditions) and practitioner workbooks (e.g., to evaluate the likelihood of detection or the probability of attack), to help practitioners better manage the causes and effects of cyber-risk to the supply chain.
3. **Generate case studies:** In-depth and longitudinal case studies within different industrial sectors are required to increase our understanding of the occurrence, detection, and reaction to cyber-attacks. Such case studies will enable researchers to validate theory and conceptual frameworks and models.
4. **Investigate the different types of cyber-attacks:** Studies should examine the attack goals (e.g., data theft, data modification, data falsification), the technical nature of attacks (e.g., tools, physical or digital barriers, verification procedures, data integrity), as well as human dimensions (e.g., cyber-attacker motivation, incentives).
5. **Propose strategic ways of managing cyber risks:** For example, academia may suggest portfolio investment to hedge risk by diversifying the business structure, where different areas counterbalance the effect of cyber-attacks. Furthermore, academia may suggest establishing appropriate key performance indicators or reviewing organizational culture and leadership, which should be empowered for proactive management of supply chain cyber-resilience.

For industry, we offer the following recommendations:

1. **The search for solutions to cyber-risks must be approached in terms of distributed accountability, instead of centralized authority:** The increasingly complex supply arrangements are creating conditions for "malevolent actors to recruit, coordinate and inflict harm across the whole network" (WEF, 2012). This challenge will require companies to adjust the current paradigm of centrally controlling risk management with routine evaluation processes (Deloitte, 2012).
2. **Re-arrange resources and develop contingency plans when necessary:** Organizations that thrive are those that can quickly recognize unusual operating conditions. It is no longer possible to prepare for every possible threat scenario. Instead, organizations

Supply Chain Cyber-Resilience: Creating an Agenda for Future Research

Omera Khan and Daniel A. Sepúlveda Estay

should prepare by encouraging team members to speak up when they detect an anomaly, having strategies in place to create customized contingency plans as necessary, and using automatic detection systems (e.g., machine learning) to identify real-time suspicious variations in performance indicators. There is a need for a new level of coordination in organizations for risk management and security response. In environments with high volatility, central controls are not sufficient and "structural integration is key to addressing uncertainties" (Boyson, 2014).

3. **Include recovery costs in the cost evaluation of cyber-attacks:** Recovery costs can surpass the direct organizational losses from cyber-attacks (Ponemon, 2014). Including recovery costs in the evaluations will highlight the real economic implications of delayed action.

4. **Create a cyber-crisis team within each organization:** Such teams should be empowered to work across organizational silos.

5. **Collaborate with academic institutions:** Academics can assist companies through training programs in cyber-resilience, by introducing new tools for the evaluation of cyber-resilience, or by providing methods for the real-time monitoring of conditions (e.g., through machine-learning methods) to detect potential threats.

6. **Promote a proactive culture:** Organizations should provide incentives for early-bird alerts on anomalous operating conditions, which promote flexibility and a proactive response in the face of an unforeseen threat.

About the Authors

Omera Khan is a Full Professor of Operations Management at the Technical University of Denmark. She works with leading organizations on a range of supply chain and logistics issues and is advisor to many universities developing courses in logistics, supply chains, and operations management. She has led and conducted research projects commissioned by government agencies, research councils, and companies in supply chain resilience, responsiveness, sustainability, and the impact of product design on the supply chain. Her latest area of research focuses on cyber-risk and resilience in the supply chain. Omera is an advisor to many organizations and provides specialist consultancy in supply chain risk management. She is a highly acclaimed presenter and is regularly invited as a keynote speaker at global conferences and corporate events. She has published her research in leading journals, contributed to several book chapters, and is lead author of *Handbook for Supply Chain Risk Management: Case Studies, Effective Practices and Emerging Trends*. She founded and was Chair of the Supply Chain Risk and Resilience Research Club and the Product Design and Supply Chain Special Interest Group. She has also been a visiting professor at a number of leading business schools.

Daniel A. Sepulveda Estay is a PhD researcher at the Technical University of Denmark, where he researches cyber-risk and security in the global supply chain. He has worked in the engineering and supply divisions of a number of multinational companies, both in strategic/leadership and operational roles for over 11 years, having partially led initiatives such as the implementation of lean manufacturing in Coca-Cola Company Latin America and supply rationalization in BHP Billiton´s copper projects division. Daniel has a BSc in Mechanical Engineering from the Federico Santa Maria Technical University in Valparaiso, Chile, an MSc degree in Industrial Engineering from the Pontifical Catholic University of Chile in Santiago, Chile, and an MSc degree in Management from the MIT Sloan School of Management, in Boston, United States.

Supply Chain Cyber-Resilience: Creating an Agenda for Future Research

Omera Khan and Daniel A. Sepúlveda Estay

References

Asbjornslett, B. E. 1999. Assess the Vulnerability of Your Production System. *Production Planning & Control,* 10(3): 219–229. http://dx.doi.org/10.1080/095372899233181

Bailey, T., Miglio, A. Del, & Richter, W. 2014. The Rising Strategic Risks of Cyberattacks. *McKinsey Quarterly,* 2 (2014): 17–22.

Blackhurst, J., Dunn, K. S., & Craighead, C. W. 2011. An Empirically Derived Framework of Global Supply Resiliency. *Journal of Business Logistics,* 32(4): 374–391. http://dx.doi.org/10.1111/j.0000-0000.2011.01032.x

Boyson, S. 2014. Cyber Supply Chain Risk Management: Revolutionizing the Strategic Control of Critical IT Systems. *Technovation,* 34(7): 342–353. http://dx.doi.org/10.1016/j.technovation.2014.02.001

BSI. 2008. *BS ISO/IEC 27001:2008 Information Technology – Security Techniques – Information Security Risk Management.* London: British Standards Institution.

Burnson, P. 2013. Supply Chain Cybersecurity: A Team Effort. *Supply Chain Management Review,* June (2013): 6–8.

Christopher, M., & Peck, H. 2004. Building the Resilient Supply Chain. *International Journal of Logistics Management,* 15(2): 1–14. http://dx.doi.org/10.1108/09574090410700275

Christopher, M., & Towill, D. 2001. An Integrated Model for the Design of Agile Supply Chains. *International Journal of Physical Distribution & Logistics Management,* 31(4): 235–246. http://dx.doi.org/10.1108/09600030110394914

Deloitte. 2012. *Aftershock: Adjusting to the New World of Risk Management.* London: Deloitte Development LLC.

Deloitte. 2013. *The Ripple Effect: How Manufacturing and Retail Executives View the Growing Challenge of Supply Chain Risk.* London: Deloitte Development LLC.

ENISA, 2015. National Cyber Security Strategies in the World. *European Union Agency for Network and Information Security.* Accessed April 1, 2015: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

Gerencser, M., Weinberg, J., & Vincent, D. 2003. *Port Security War Game: Implications for U.S. Supply Chains.* Booz & Company.

German Federal Ministry of the Interior. 2005. *National Plan for Information Infrastructure Protection.* Berlin: Bundesministerium des Innern.

Intel Security. 2014. *Net Losses: Estimating the Global Cost of Cybercrime.* Santa Clara, CA: Intel Security

IRM. 2015. Cyber Risk and Management. *Institute for Risk Management.* Accessed April 1, 2015: https://www.theirm.org/knowledge-and-resources/thought-leadership/cyber-risk/

Keegan, C. 2014. Cyber Security in the Supply Chain: A Perspective from the Insurance Industry. *Technovation,* 34(7): 380–381. http://dx.doi.org/10.1016/j.technovation.2014.02.002

Linkov, I., Eisenberg, D. A., Bates, M. E., Chang, D., Convertino, M., Allen, J. H., Flynn, S. E., & Seager, T. P. 2013. Measurable Resilience for Actionable Policy. *Environmental Science and Technology,* 47(18): 10108–10110. http://dx.doi.org/10.1021/es403443n

Pettit, T. J., Fiksel, J., & Croxton, K. L. 2010. Ensuring Supply Chain Resilience: Development of a Conceptual Framework. *Journal of Business Logistics,* 31(1): 1–21. http://dx.doi.org/10.1002/j.2158-1592.2010.tb00125.x

Ponemon. 2014. 2014 *Global Report on the Cost of Cyber Crime.* Traverse City, MI: Penemon Institute.

Reuters. 2012. *Cyber Crime - How Can Firms Tackle This Fast-Emerging Invisible Menace?* London: Thomson Reuters.

Sheffi, Y., & Rice, J. B. 2005. A Supply Chain View of the Resilient Enterprise. *MIT Sloan Management Review,* 47(1): 41–48.

Tranfield, D., Denyer, D., & Smart, P. 2003. Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review. *British Journal of Management,* 14(3): 207–222. http://dx.doi.org/10.1111/1467-8551.00375

WEF. 2012. *Risk and Responsibility in a Hyperconnected World - Pathways to Global Cyber Resilience.* Geneva, Switzerland: World Economic Forum.

WEF. 2013. *Building Resilience in Supply Chains.* Geneva, Switzerland: World Economic Forum.

WEF. 2015. *Partnering for Cyber Resilience: Towards the Quantification of Cyber Threats.* Geneva, Switzerland: World Economic Forum.

White House. 1998. *Presidential Decision Directive NSC-63 on Critical Infrastructure Protection.* Washington, DC: The White House.

White House, 2003. *The National Strategy to Secure Cyberspace.* Washington, DC: The White House.

Citation: Khan, O., & Sepúlveda Estay, D. A. 2015. Supply Chain Cyber-Resilience: Creating an Agenda for Future Research. *Technology Innovation Management Review,* 5(4): 6–12. http://timreview.ca/article/885

Keywords: resilience, supply chain management, cyber-risk, cybersecurity, theoretical foundation

Cyber-Resilience: A Strategic Approach for Supply Chain Management

Luca Urciuoli

> *"Business is all about risk taking and managing uncertainties and turbulence."*
>
> Gautam Adani
> Business magnate

Risk management and resilience strategies in supply chains have an important role in ensuring business continuity and reliability in a cost-efficient manner. Preventing or recovering from disruptions requires access and analysis of large amounts of data. Yet, given the multiple stakeholders, operations, and environmental contexts in which a global supply chain operates, managing risks and resilience becomes a challenging task. For this reason, information and communication technologies (ICT) are being developed to support managers with tailored tools and services to monitor disruptions, enhance instantaneous communication, and facilitate the quick recovery of supply chains. Hence, the objective of this article is to shed light on managerial strategies to improve the resilience of supply chains and thereby to point out how these could be automated by means of innovative ICT systems. In particular, this article concludes by warning about existing challenges to implementing such systems. If these challenges are not correctly addressed by managers, there is a major risk of further jeopardizing supply chains.

Introduction

Recent catastrophic events, such as terrorist attacks, natural disasters, and pandemics, have drawn attention to the vulnerability of global supply chains to risks (Jüttner, 2005). Vulnerability means that supply chains are susceptible to disruptions, meaning interruptions in business operations that result in undesirable consequences such as delayed deliveries or lost sales (Svensson, 2002). For example, the earthquake that hit Taiwan in September 1999 had a severe impact on the personal computer industry worldwide – 10% of the world's computer chips and 80% of the world's motherboards were produced in Taiwan – resulting in lost revenues of more than 200 million dollars due to production shut-downs (McGillivray, 2000). Supply chain trends such as globalization, specialization, complexity, and lean processes have been largely indicated as the main drivers of these risks (Pfohl et al, 2010; WEF, 2012). Hence, in such a scenarios, supply chain managers are asked to improve their risk management skills in terms of identifying, analyzing, mitigating, and finally monitoring risks.

Supply chains are often described as sets of organizations joining a virtual network through which flows of services/products, information, and money are moved and exchanged. The common goal of these networks is to transform raw materials into components and products that are delivered to final consumers, at the right time, quantity, quality, and place. In these networks, strategies to manage risks and resilience have an important role in ensuring business continuity, delivery reliability, responsiveness, etc.

To ensure the optimal management of risks and resilience, managers of supply chains need to identify, access, and analyze large amounts of data through different information technology platforms and sources. In particular, specific ICT systems based on a combination of push and pull services are indicated as the most promising approaches to support risk management and resilience in a cost-effective manner. The principle behind these systems is very simple: such systems consists of web-services providing common and consistent access to data for all the different actors in

Cyber-Resilience: A Strategic Approach for Supply Chain Management

Luca Urciuoli

the supply chain (e.g., suppliers, transport providers, manufacturers, distributors, importers, retailers) but also for governmental agencies worldwide (Williams et al., 2002). Yet, given their novelty, there is still much uncertainty about how these systems should be best integrated in companies.

Hence, the objective of this article is to provide a general overview of resilience strategies applied in supply chains and thereby shed light on how ICT systems can be exploited. By understanding and putting into practice these conceptual links, this article aims to contribute a visionary perspective of cyber-resilience in supply chains, illustrating how resilience in supply chains can be enhanced through the exploitation of innovative information technology services.

The article is structured in a manner to build up and lead to the cyber-resilience topic: after the introduction, it provides an overview of risk management and resilience strategies in supply chains. Next, it enumerates known challenges of these approaches, and thereafter it sheds light on the role of ICT in cyber-resilience. Finally, the article concludes by providing managerial implications and recommendations.

Risk Management and Resilience Strategies in Supply Chains

Besides risk management strategies, both researchers and practitioners point out that particular attention has to be given to strategies improving the resilience of supply chains, that is, the capability of supply chains to bounce back to stable conditions after a disruption. Resilience is important for two reasons: first of all, sooner or later, companies will have to face unexpected risks, for which no mitigation strategies have been planned in advance. Hence, the capabilities to respond to these events need to be built into the management of the companies. Second, the reactions of governmental agencies triggered after large catastrophes (e.g., terrorist attacks, earthquakes, hurricanes) may also give rise to unexpected events that supply chain companies need to deal with in order to ensure business continuity and survival (Sheffi, 2001).

Looking at the literature, diverse strategies to manage resilience have been enumerated. Some of those are:

- **Diversification of suppliers:** The access to a wider supply base enables firms to exploit additional production lines and quickly shift volumes and production in case of a disruption (Sheffi, 2006; Tang, 2006; Tomlin, 2006). In addition, companies may use flexible contract agreements, inspections to qualify suppliers, and make-and-buy strategies to split production across different factories (Sheffi, 2006).

- **Inventory management:** Safety stocks can be increased in order to avoid stock-outs in case of missed demand. Inventory redundancy may build additional capacity in firms, yet they are well known to generate additional costs as obsolescence, product lifecycles, and inventory holdings (Sheffi, 2006; Tang, 2006; Tomlin, 2006).

- **Ensure additional transport capacity and multiple consignment routes:** Plan in advance possibilities to transport cargo by means of multiple transportation modes, multiple carriers or providers, and consequently multiple routes and distribution channels (Tang, 2006; Tomlin, 2006). Additional transport capacity can also be ensured by investing in and maintaining a dedicated transportation fleet (Sheffi, 2006).

- **Product-centric design:** Aligning the design of the products with the supply chain efficiency targets. This process cannot happen in isolation, but it implies vertical cooperation and early involvement of suppliers in product concept development and design (Khan et al., 2012; Zsidisin et al., 2000). Multiple designs of products can become useful in emergency situations, for example, in case a specific raw material or component is unexpectedly not accessible (Sheffi, 2006).

- **Information sharing:** Information sharing may improve flexibility of supply chains or enable monitoring of risks and the establishment of preventive actions (Skipper & Hanna, 2009; Tomlin, 2006).

Challenges in Managing Risks and Resilience

Given the multiple stakeholders, operations, and environmental contexts in which a global supply chain operates, managing risks and resilience is a challenging task. These challenges are especially acute in the domain of cross-border trade, where the organizations in the virtual network need to be managed as single entities across national borders, and where several regulatory compliance frameworks exist. In practice, this means that supply chain companies need to deal with different cultures, geopolitical and organizational issues, regulatory compliance frameworks, and ultimately with different ICT systems, standards, and technologies operated by different actors and under different business logics (Urciuoli et al., 2013).

Cyber-Resilience: A Strategic Approach for Supply Chain Management

Luca Urciuoli

The latest R&D initiatives are putting their efforts on the development of ICT tools that may support companies with this complex process. These tools aim to enhance visibility of risks along the supply chain by enabling information collection through sensor technologies, sharing of data, and application of advanced business intelligence rules to analyze data; in particular, data are not being shared merely between the supply chain companies, but also between the supply chains and the governmental agencies. This practice is fundamental to reduce the administrative costs that cross-border supply chains entail (Urciuoli et al., 2013).

To give a sense of the burden experienced by companies, it can be reminded that, to import goods into a country, companies have to produce export and import declarations, with licenses and other permits to be attached, in order to demonstrate compliance with customs regulatory frameworks. In Europe alone, customs administrations are processing almost 200 million declarations every year; for example, in 2007, it was 183 million (IBM, 2008). Each of these declarations consists of roughly 40 typologies of documents and in total about 200 data elements need to be exchanged between business and governmental entities, resulting in highly complex and costly data transfer, processing, and storage challenges (ADB, 2005).

The Role of ICT: Towards Cyber-Resilient Supply Chains

Cyber-resilience may be achieved by smartly combining technologies and services that exist today on the marketplace or that are being developed in R&D projects. These are presented in this section as ICT systems for B2B (Business to Business) and B2G (Business to Government) information sharing and analysis.

B2B information sharing

Several IT companies are struggling to develop multiple data interfaces in order to guarantee full interoperability and access to data to supply chains stakeholders. Data is actually being shared between companies in a supply chain, however, often in paper and sometimes in electronic format. In particular, the usage of paper-based information exchange has been indicated as not effective, because of the risk for mistakes, data loss, as well as redundant transfer and collection of the same data. Hence, the usage of sophisticated electronic systems to collect, store in a common repository ecosystem, and analyze data has received a lot of attention because of the abundant cost savings that could be earned. For instance, in an international shipment, files of data containing bills of lading, invoices, packing lists, country of origin, cargo quantity and type, etc. need to be shared by supply chain companies in order to improve the prediction of estimated times of arrival (ETAs). According to ETA estimations, transportation and diverse resources can be optimally scheduled and allocated, market campaigns can be punctually started to strategically retain major market shares, etc. Likewise, customs declarations in import and export countries can be submitted simultaneously by different stakeholders (Urciuoli et al., 2011).

Nowadays, web-services based on service-oriented architectures (SOAs) seem to be widely exploited to ensure connectivity of the supply chain in a plug-and-play fashion. These services enable electronic data sharing, and with it may reduce the risk for mistakes or incomplete data. In addition, web-based push and pull services can be exploited to avoid data redundancy and speed up response procedures in case of unexpected disruptions:

- **B2B pull services:** Data may be pulled by a supply chain company in order to obtain the current status of a consignment/container or to interrogate the inventory levels of suppliers, distribution centres/wholesalers, retailers, transport infrastructure capacity, traffic conditions, etc.

- **B2B push services:** Push services are instead used to trigger alerts to companies whenever the status of inventory levels, demand, containers conditions. or position change in an unexpected manner. In other words, the service is able to sense whenever data outrange previously established upper and lower control limits (UCLs and LCLs). These data ranges can be determined by means of advanced business intelligence techniques.

The combination of the above push and pull services enables full visibility and control in the supply chain. By pulling key data, managers may monitor, in real time, inventory levels, shipping statuses, environmental conditions of cargo and containers, arrival time at specific nodes in the supply chain network, etc. This information improves decision making in terms of optimizing inventory levels, scheduling and planning transport assignments, allocating resources, designing networks, etc. On the contrary, push services are more suitable to handle risks and manage resilience. Hence, in case of deviations from planned routines, alerts may be triggered to recover or activate response procedures. Examples of push services could be alerts triggered by

Cyber-Resilience: A Strategic Approach for Supply Chain Management

Luca Urciuoli

environmental sensors in containers, alarms installed in vehicles, panic buttons, geofences, timefences, etc.

B2G information sharing
Nowadays, to enable resilience strategies, supply chain companies work with different contract typologies and portfolios of suppliers located in various countries across the globe. However, despite contracts being in place, in case of a disruption, companies will suddenly need to deal with several different regulatory frameworks and customs procedures. Not only that, different countries require different data formats or usage of different information technology interfaces, implying higher costs in terms of translation and adaptation efforts needed to bridge between different national systems. Experts believe that future information technology systems will ensure that companies' systems can easily connect to customs administrations' web-platforms (i.e., e-Customs) and facilitate filing of customs declarations or provide easy access to international trade-related documentation (Urciuoli et al., 2013). In addition, push and pull services developed in prototype platforms may play a fundamental role in managing resilience:

- **B2G pull services:** Pull services connected to e-Customs platforms may be used to control existing trade regulations, necessary documentation for import/export procedures, status of release and clearance of containers, customs declarations, licenses, etc.

- **B2G push services:** Push services are instead planned to include alerts in case of changed trading regulations, tariffs or taxes, deviations of containers inspections and release, etc. These systems may eliminate unnecessary delays, reduce paper redundancy, and in this way, reduce costs to companies and governments.

Conclusion

ICT has already been indicated as playing a major role in controlling and managing more complex value networks in a cost-efficient manner. However, additional capabilities, mainly aiming to improve cyber-resilience, may be exploited to ensure quick response to risks and disruptions in supply chains. These capabilities are supported by the development of common repository IT ecosystems where B2B or B2G push and pull web services are created and contemporarily accessed by supply chain actors, but also governmental agencies.

Enabling B2B and B2G data sharing may allow companies to access an unimaginable amount of data and services that can enhance the cyber-resilience of the whole supply chain. For instance, companies will be able to easily manage and control portfolios of suppliers online, make more accurate ETA estimations, monitor in real time the transport infrastructure capacity, learn and apply any sudden changes in trading regulations, rapidly submit electronic orders and comply with regulatory frameworks, etc.

Despite the promising future visions, there is still much work to be done in order to ensure that these ICT systems will be fully accepted and integrated into supply chain companies. Many challenges are being encountered and need to be solved in order to move a step forward towards cyber-resilient supply chains. These are, in sequential order, the following:

1. **Exploit/develop reliable and robust information collection and sharing (both B2B and B2G).** Collection and sharing of information is still a major concern, especially for small companies, both in terms of technical development, know-how, and monetary investments.

2. **Exploit business intelligence rules.** Develop tailored push and pull web services that enable cyber-resilience. Yet, to develop reliable business intelligence rules, resources need to be allocated to identifying, modelling, and assessing risks in a systematic manner.

3. **Ensure public–private partnerships.** Partnerships should focus on the implementation of ICT systems to exchange data with public agencies and aim at developing up-to-date standards and legislative frameworks.

4. **Solve potential data confidentiality issues.** Sharing information implies that data will need to be held in repositories or remote locations. For obvious reason, this requirement is not accepted by many business companies that fear their business strategies will be disclosed to competitors.

5. **Ensure cybersecurity.** In several instances, it has been pointed out that, although the information technology layer of supply chains is relevant to optimizing supply chain management, it may also expose companies to criminal actions (e.g., theft, fraud, forgery, industrial espionage) or sabotage, hackers, and terrorists aiming to promote ideological issues and hurt the economy of a nation or a single industry (e.g., hacktivism, sabotage). Hence, this risk naturally implies that cyber-resilience strategies should be followed by information technology security management systems.

Cyber-Resilience: A Strategic Approach for Supply Chain Management

Luca Urciuoli

In conclusion, it is strongly believed that, without common data access, managers may struggle to fully develop, apply, and coordinate resilience operations in companies. Resilience becomes even more challenging in global supply chains, where managers need to deal with threats and recovery operations outside their companies and in different and multi-faceted environmental contexts. Current R&D initiatives are demonstrating that ICT systems for B2B and B2G data exchange, when combined with business intelligence techniques, may provide supply chain managers with advanced capabilities to improve resilience. Hence, supply chain companies could be only "a click away" from fully automated cyber-resilience.

Acknowledgements

The author of this paper would like to thank the CORE project (Consistently Optimised Resilient Secure Global Supply Chains, Grant Agreement No. 603993), a project funded under the European Union's Seventh Framework Programme for research, technological development, and demonstration. This publication reflects the views only of the author, and the EU Commission cannot be held responsible for any use which may be made of the information contained therein.

About the Author

Luca Urciuoli is an Associate Research Professor in the MIT International Logistics Program within the Zaragoza Logistics Center in Spain, where he teaches and performs research in supply chain network design, supply chain risk, and security management. He holds an MSc degree in Industrial Engineering from Chalmers University of Technology in Gothenburg, Sweden, and a Doctorate in Transportation Security from the Engineering University of Lund, Sweden. He has been working at the research unit of the Volvo group as a project manager developing on-board transport and telematics services. He also led the research of the Cross-border Research Association in Switzerland and collaborated in several FP7 research and consultancy projects, with a focus on topics such as e-Customs, trade facilitation, supply chain security, waste security, and postal security. He is also an editorial board member for the *Journal of Transportation Security*, and he has published his research in several scientific and practitioner journals.

Contact: lurciuoli@zlc.edu.es

References

ADB. 2005. *ICT for Customs Modernization and Data Exchange.* Manila, Philippines: Asian Development Bank.

IBM. 2008. *Implementing e-Customs in Europe: An IBM Point of View.* Somers, NY: IBM Corporation.

Jüttner, U. 2005. Supply Chain Risk Management: Understanding the Business Requirements from a Practitioner Perspective. *International Journal of Logistics Management,* 16(1): 120–141. http://dx.doi.org/10.1108/09574090510617385

Khan, O., Christopher, M., & Creazza, A. 2012. Aligning Product Design with the Supply Chain: A Case Study. *Supply Chain Management,* 17(3): 323–336. http://dx.doi.org/10.1108/13598541211227144

McGillivray, G. 2000. Commercial Risk Under JIT. *Canadian Underwriter,* 67(1): 26–30.

Pfohl, H.-C., Köhler, H., & Thomas, D. 2010. State of the Art in Supply Chain Risk Management Research: Empirical and Conceptual Findings and a Roadmap for the Implementation in Practice. *Logistics Research,* 2(1): 33–44. http://dx.doi.org/10.1007/s12159-010-0023-8

Sheffi, Y. 2001. Supply Chain Management under the Threat of International Terrorism. *International Journal of Logistics Management,* 12(2): 1–11. http://dx.doi.org/10.1108/09574090110806262

Sheffi, Y. 2006. Resilience Reduces Risk. *Logistics Quarterly,* 12(4): 12–14.

Skipper, J. B., & Hanna, J. B. 2009. Minimizing Supply Chain Disruption Risk through Enhanced Flexibility. *International Journal of Physical Distribution and Logistics Management,* 39(5): 404–427. http://dx.doi.org/10.1108/09600030910973742

Svensson, G. 2002. A Conceptual Framework of Vulnerability in Firms' Inbound and Outbound Logistics Flows. *International Journal of Physical Distribution & Logistics Management,* 32(2): 110–134. http://dx.doi.org/10.1108/09600030210421723

Tang, C. S. 2006. Robust Strategies for Mitigating Supply Chain Disruptions. *International Journal of Logistics Research and Applications,* 9(1): 33–45. http://dx.doi.org/10.1080/13675560500405584

Tomlin, B. 2006. On the Value of Mitigation and Contingency Strategies for Managing Supply Chain Disruption Risks. *Management Science,* 52(5): 639–657. http://dx.doi.org/10.1287/mnsc.1060.0515

Urciuoli, L., Hintsa, J., & Ahokas, J. 2013. Drivers and Barriers Affecting Usage of E-Customs — a Global Survey with Customs Administrations Using Multivariate Analysis Techniques. *Government Information Quarterly,* 30(4): 473–485. http://dx.doi.org/10.1016/j.giq.2013.06.001

Cyber-Resilience: A Strategic Approach for Supply Chain Management

Luca Urciuoli

Urciuoli, L., Zuidwijk, R., & van Oosterhout, M. 2011. Adoption and Effects Extended SICIS. In *Proceedings of the 2011 Hamburg International Conference of Logistics (HICL).*

WEF. 2012. *New Models for Addressing Supply Chain and Transport Risks.* Geneva, Switzerland: World Economic Forum.

Williams, L. R., Esper, T. L., & Ozment, J. 2002. The Electronic Supply Chain: Its Impact on the Current and Future Structure of Strategic Alliances, Partnerships and Logistics Leadership. *International Journal of Physical Distribution & Logistics Management,* 32(8): 703–719. http://dx.doi.org/10.1108/09600030210444935

Zsidisin, G. A., Panelli, A., & Upton, R. 2000. Purchasing Organization Involvement in Risk Assessments, Contingency Plans and Risk Management: An Explorative Study. *Supply Chain Management,* 4(4): 187–197. http://dx.doi.org/10.1108/13598540010347307

Citation: Urciuoli, L. 2015. Cyber-Resilience: A Strategic Approach for Supply Chain Management. *Technology Innovation Management Review*, 5(4): 13–18. http://timreview.ca/article/886

Keywords: IT, ICT, supply chain management, cross-border trade, cyber-resilience, risk management

Building Cyber-Resilience into Supply Chains

Adrian Davis

> *"Today's CISO focuses on tier 1 or direct suppliers. Tomorrow's CISO will need to focus on the supply chain."*
>
> Chief information security officer (CISO) of a major international bank

The article discusses how an organization can adopt an information-centric approach to protect its information shared in one or more supply chains; clearly communicate the expectations it has for a direct (Tier 1) supplier to protect information; and use contracts and measurement to maintain the protection desired. Building on this foundation, the concept of resilience – and that of cyber-resilience – is discussed, and how an information-centric approach can assist in creating a more cyber-resilient supply chain. Finally, the article concludes with five steps an organization can take to improve the protection of its information: i) map the supply chain; ii) build capability; iii) share information and expertise; iv) state requirements across the supply chain using standards, common frameworks, and languages; and v) measure, assess, and audit.

Introduction

Supply chains – and the organizations involved in them – are now targets for hackers. There are several reasons behind this: one is that supply chains contain a wealth of information that may be sold or may embarrass one or more organizations in the supply chain; another is that one organization can be used as a route to attack another organization in the same supply chain, as was seen in the 2013 attack on the retailer Target in the United States (Krebs, 2014).

Information, just like the physical components of supply chains, is vital for the continued efficient operation of supply chains. Indeed, for some supply chains to operate, the constituent organizations may need to share trade secrets, proprietary data, and other sensitive information. However, the role and protection of information in supply chains has received less attention than the physical aspects of those supply chains. That situation is changing.

Much effort has been invested in reducing the risks associated with the physical aspects of supply chains – and improving their resilience overall – but less attention has been paid to the overall resilience and security of the cyber-related aspects of supply chains. This article will examine that key issue: how an organization can protect its information in one or more supply chains, and use that as the basis to build cyber-resilience across one or more of its supply chains.

The information-centric approach, which provides an organization with a powerful tool to protect the information it does and does not share, is presented as a solution to this key issue. How the approach can be adopted and used with direct – or Tier 1 – suppliers is discussed. From this foundation, the article looks at the concept of resilience and how cyber-resilience can be defined: the role of the information-centric approach is highlighted as a component of cyber-resilience. Finally, five steps an organization can take to build both an information-centric approach and cyber-resilience are listed and described.

Protecting Information in the Supply Chain

The ubiquity of information technology (IT) and the availability of information has placed all organizations in a dilemma. For a supply chain to work effectively and efficiently, information – some of it sensitive or confidential – must be shared between many organizations.

Building Cyber-Resilience into Supply Chains

Adrian Davis

Yet, at the same time, one or more of those organizations may not want to share that information or may have external obligations, such as those set out in law or regulation, to protect the same information. Certain types of information, for example, personally identifiable information and medical records, are subject to legal or regulatory obligations concerning their protection and use. These obligations may preclude sharing – yet such sharing is essential to supply chain success. This requirement to share is a key risk in today's digitally connected, information-dependent supply chain. Sharing information has become easier with the advent of IT and the Internet but, paradoxically, has also become harder with the proliferation of technologies and services made available by IT and the Internet. As a result, information can be shared in many forms and in many formats (including paper), multiplying the number of copies in existence and, in some cases, multiplying the possibility of error.

Across a supply chain, the capability and desire of suppliers to expend resources on cybersecurity and cyber-resilience will vary significantly. Some suppliers will possess the expertise, knowledge, and ability to address cyber-related issues in a consistent and comprehensive manner. Other suppliers will not. From the perspective of an acquiring organization (hereafter "the acquirer" in accordance with the ISO/IEC 27036-1:2014 [ISO, 2014; Part 1]), a key issue is that, despite a lot of hard work and significant expenditure, the acquirer cannot negotiate, agree, measure, and assess the cybersecurity and associated risks of its suppliers and across a supply chain. For an acquirer, various factors may combine to make up this issue, including the inability to:

1. State cybersecurity requirements to suppliers using a common framework and language.

2. Integrate cybersecurity into the acquirer procurement process.

3. Devote resource to investigate the makeup of the supply chain (i.e., which supplier organizations make up the supply chain).

4. Understand how a supplier meets the acquirer's requirements when not using a common, shared, framework, and language.

5. Identify acquirer information shared between the acquirer and its direct suppliers, and acquirer information shared between direct and indirect suppliers.

6. Specify cybersecurity requirements for indirect suppliers (i.e., the suppliers to the direct suppliers).

7. Measure the effectiveness of cybersecurity arrangements at suppliers and across the supply chain using a consistent set of indicators.

8. Identify and quantify cyber-related risks across the supply chain.

9. Identify the use of technology (such as the cloud) and technology providers by the acquirer and suppliers across the supply chain.

10. Control the confidentiality, integrity, and availability (CIA) of information once shared with suppliers and the supply chain.

These factors may vary in their significance across a supply chain. It worth noting that an acquirer may have multiple supply chains and that the issues and factors may vary in their significance across each supply chain. If we look at a simplified supply chain from an information or cybersecurity perspective, we can highlight where the ten factors listed above often occur.

Figure 1 shows that the factors can be grouped into two types:

1. Acquirer-focused

2. Supply-chain-focused

Acquirer-focused factors (numbered 1 to 4 in the list and in Figure 1) are internal to the acquirer and, to a degree, can be actively managed and addressed by the acquirer's management and staff. Typically, these factors fall under information security, third-party (i.e., supplier) security and data privacy programmes, and projects run by the organization's staff or by consultants.

Supply-chain-focused factors (numbered 5–10) are outside of the acquirer's control. Once acquirer information is passed to a supplier, then that information can be shared, copied, stored, changed, deleted, and so on without the acquirer's knowledge or permission. The acquirer thus has no idea how its information is being protected, who its information is shared with, where that information is – physically and electronically – and who may have seen or used that shared acquirer information. Once this situation occurs, it is very difficult to regain (or gain) any control over the protection of in-

Building Cyber-Resilience into Supply Chains

Adrian Davis

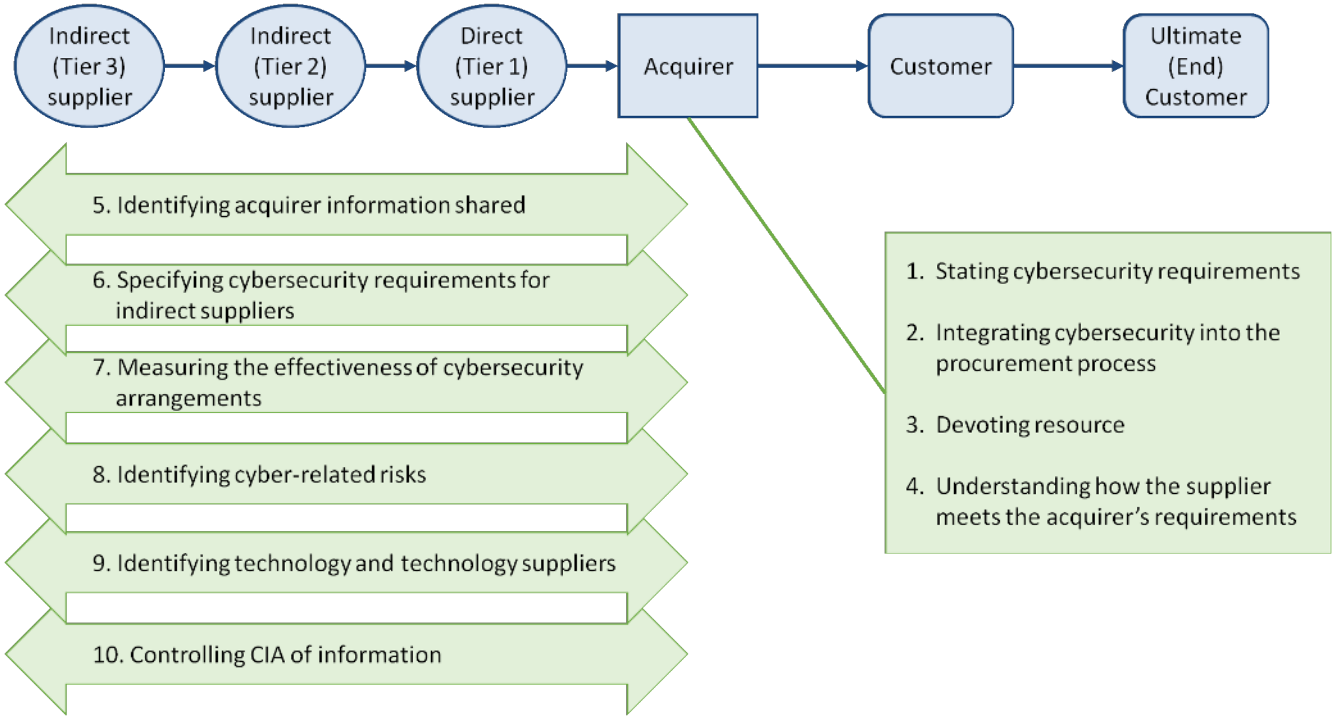

Figure 1. Factors that can impact the ability of an acquirer to protect its information using a simplified supply chain model

formation and to assess the risks to that information. Because the acquirer typically has little or no ability to work with, or influence, its indirect suppliers (e.g., if there is no contract in place), the acquirer cannot set out its requirements for the protection of its information at those indirect suppliers, which makes it difficult to measure the effectiveness of the cybersecurity arrangements across the supply chain and may significantly impact the overall cybersecurity risk associated with sharing. Sub-contracting by the supplier – especially to technology or service providers offering cloud, mobile device, and social media services – can also significantly impact the risks of sharing, protecting information, and controlling the CIA of acquirer information.

Securing Information in Supply Chains

Given the requirements to share and protect information, and the issue and factors discussed above, acquirers have made efforts to address how best to share and protect information they make available to suppliers. Typically though, these efforts are focused at Tier 1 suppliers, occur late in the procurement cycle, and apply "one size fits all" information security approaches. Thus, an acquirer will specify certification or compliance with an information security management system (e.g., ISO/IEC 27001:2013 [ISO, 2013a]), the "right to audit" and requiring a supplier to meet the requirements of the acquirer's internal policy documents, irrespective of the information being shared or the goods and services being supplied. Such an approach may not provide the best protection to shared information, because information risks may not have be adequately addressed, and so risk treatment may be overly strong in one area and weak in another. Acquirers have also struggled to identify what information they actually share, further dispersing their efforts in terms of protection.

To protect information shared with Tier 1 suppliers in the manner the acquirer is expecting requires an information-centric approach. In this approach, the acquirer determines at the start of the procurement cycle what information has to be shared to purchase a particular good or service. Knowing what information is to be shared will allow the acquirer to understand the harm it may suffer should the information be compromised at a supplier and the risk treatment the supplier should put in place at a minimum. This information-centric approach allows the acquirer to indicate:

- what information is being shared

Building Cyber-Resilience into Supply Chains

Adrian Davis

- its importance to the acquirer (the organization sharing the information)
- the sensitivity of that information when it is shared
- the harm to the acquirer should that information have its confidentiality, integrity, or availability compromised
- the protection required for that information – and the requirements a supplier must meet

Thus, an acquirer can state to a supplier what is being shared, what can happen if that information is lost, and how that information should be protected. This approach is the application of information risk assessment, but now it has been used in an external context. The protection required can include processes, technologies (such as encryption), and the ability to assess and audit that the supplier is actively implementing the protection required. Figure 2 illustrates how information – and its protection – can be built into a typical procurement cycle.

Once the information to be shared has been determined, the protection of information can be worked into all procurement documents used by the acquirer (such as the Expression of Interest and Invitation to Tender) and to make decisions. Importantly, what information is shared and the harm to the acquirer should that information lose its confidentiality, integrity, or availability can be used to drive the protection required using a risk-based approach. Standards such as the multi-part ISO/IEC 27036 (ISO, 2014) can be used to provide a common starting point, a common set of terminology, and a common understanding of how each organization approaches its business and its cybersecurity.

This approach is limited because it is only focused on Tier 1 suppliers. To protect acquirer information further upstream (Tier 2 and beyond) is much more difficult, but a degree of protection can be achieved by using pass-through clauses, technical approaches, and auditing. Pass-through clauses, which are placed in the acquirer-supplier contract, are an attempt to ensure the supplier's suppliers put in place the same protection as the contract requires the supplier to do. For example, if an acquirer wants a supplier to adopt an information security management system and the supplier's suppliers to do the same, a pass-through clause could be inserted into the acquirer-supplier contract stating "all suppliers of the contracted supplier that are likely to handle the information provided by the acquirer must have an information security management

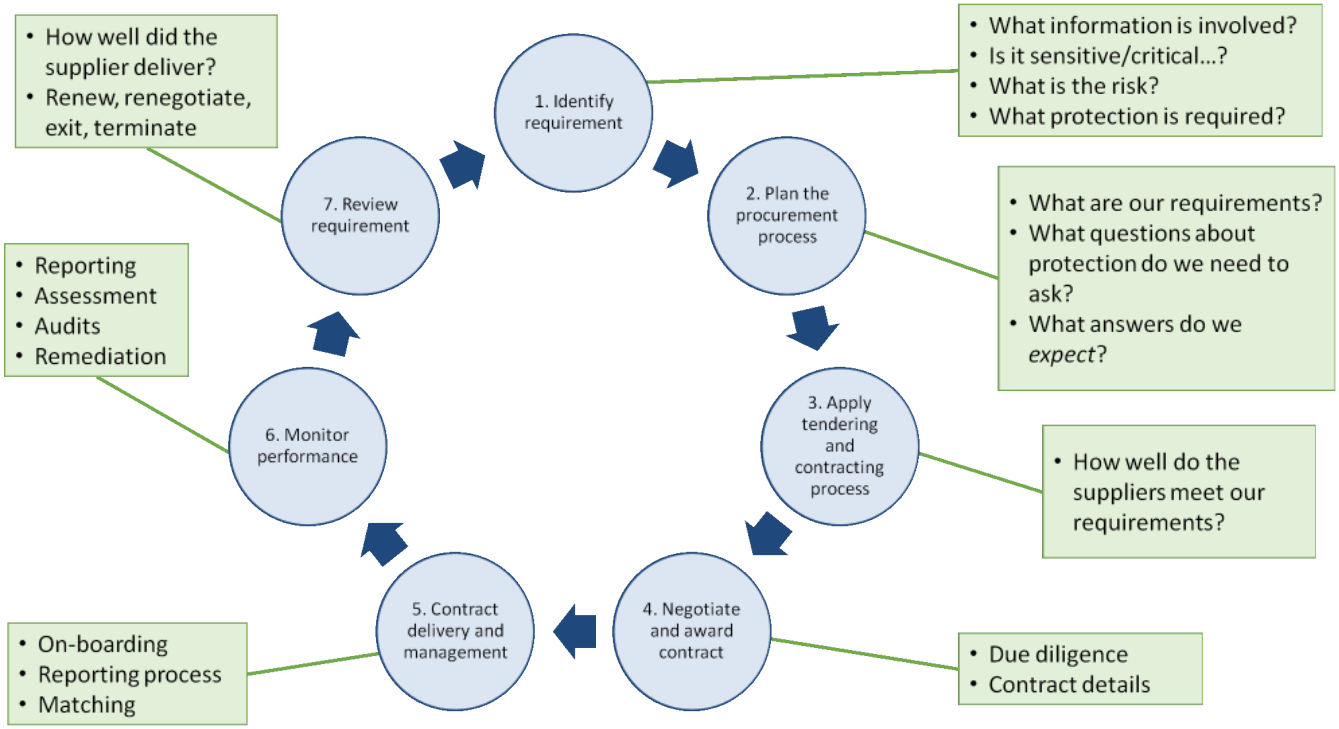

Figure 2. Integrating information into a typical procurement cycle

Building Cyber-Resilience into Supply Chains

Adrian Davis

system in place. The contracted supplier will be held responsible for ensuring compliance with this clause." Needless to say, pass-through clauses are not necessarily popular with suppliers, because such clauses place obligations on them. Pass-through clauses typically only reach Tier 1 and Tier 2 suppliers. Technical approaches, such as digital rights management, offer a partial solution, which may extend to upstream suppliers. Allowing suppliers to connect to the acquirer's infrastructure to access information is another control mechanism, because a control over who sees acquirer information and what is copied can be exercised, thus hopefully limiting wider exposure to the supply chain. However, there are both management and technical overheads to these approaches, which an acquirer may feel outweigh the protection offered. Finally, a thorough audit of the supplier and its communications will also allow the acquirer to understand how its information is being shared. Audits of this nature are time consuming and expensive and also rely on the supplier having kept records of such communications and of the goodwill of the supplier in sharing them. Resource, cost, time, and other constraints often mean that audits such as these are performed very infrequently. Figure 3 summarizes how the approaches discussed in this section can be applied and illustrates the reach of those approaches across a model supply chain.

Being able to protect information at a Tier 1 supplier, let alone upstream, is a major step forward, but to achieve true cyber resilience, other steps are necessary. First of these is to understand and then create resilience.

Resilience

The concept of resilience takes many forms and has been applied to supply chains, organizations, and IT. Unfortunately, there are many definitions of resilience itself, which are then appropriated to fit specialist disciplines. As a starting point, we will use this definition of resilience: "[…] the ability of a system to return to its original [or desired] state after being disturbed" (Peck et al., 2003). Resilience can be viewed from several broad perspectives, which are briefly discussed here. The first approach views resilience from an organizational viewpoint and is concerned with preparing for and reacting to an incident and reducing the harm or impact. The second approach, which is narrower, views resilience as the ability of an organization's IT to keep running in the event of error, failure, or incident. These two approaches share much in common and are intertwined, because organizations are typically dependent on IT to carry out and support their business operations: a failure in IT could significantly harm an organization. The third perspective is that of business continuity, which views business continuity plans and disaster recovery as

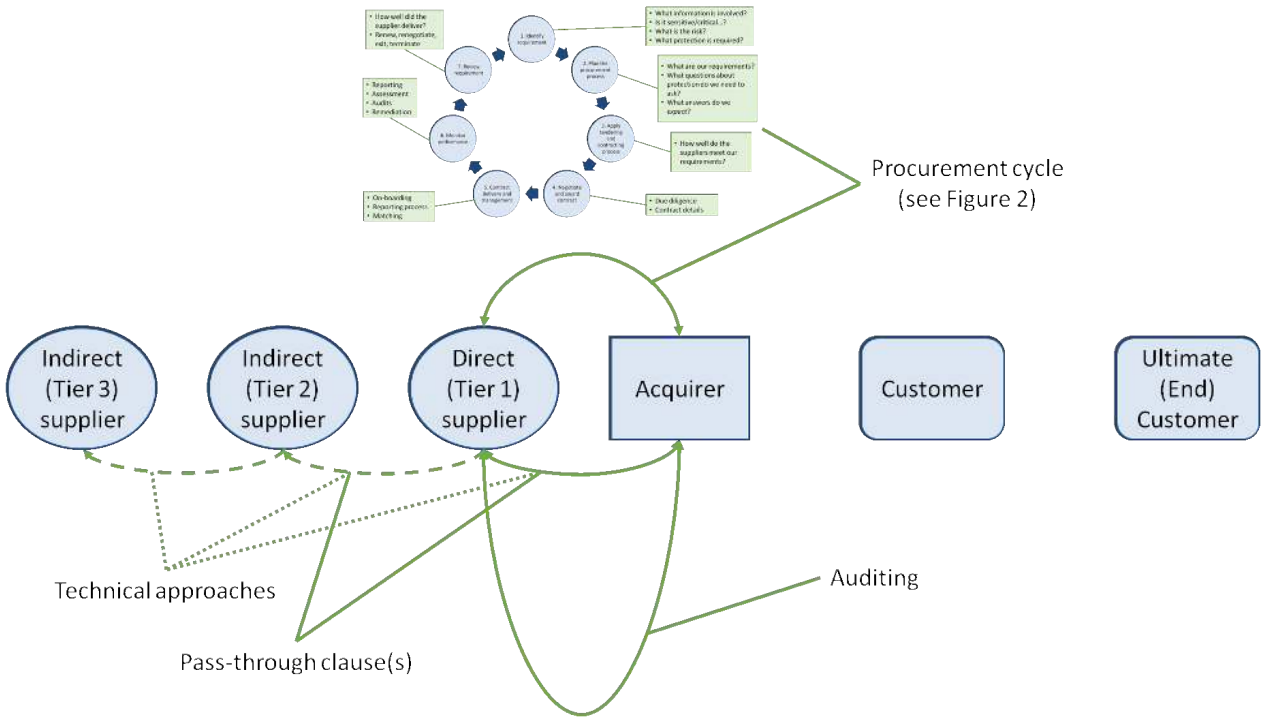

Figure 3. Approaches to protecting information in the supply chain

Building Cyber-Resilience into Supply Chains

Adrian Davis

an essential component of resilience (Davis & Skelton, 2014) and provides the basis upon which an organization can plan and execute its responses to an incident. Importantly, resilience has a time component; for example, the concepts of "recovery time objective" and "maximum tolerable downtime" are taken from business continuity (Tipton & Hernandez, 2013). These three perspectives are typically organizationally-focused and inward-looking to a great extent.

Supply chain resilience is “the ability of the supply chain to cope with unexpected disturbances” (Christopher, 2011) and one of its characteristics is a business-wide recognition of where the supply chain is most vulnerable. Supply chain management, design, and business continuity all have a role to play in creating resilience (Waters, 2011).

Finally, resilience is a developing concept in cyberspace. Again, various perspectives can be taken. The broadest looks at the resilience of the physical and virtual components of the Internet – the hardware, software, processes, and communication links – and how that entire system of systems could still operate if there were failures, attacks, or other incidents. Another perspective examines how an organization could continue to do business if its access to its information, the Internet, or the services delivered via the Internet were interrupted or impaired. This is what the author takes to be "cyber-resilience": the ability of a system that is dependent on cyberspace in some manner to return to its original [or desired] state after being disturbed.

So, cyber-resilience is more than just an IT or information security issue (Information Security Forum, 2012; World Economic Forum, 2012). It is a business issue and should be woven into business or enterprise risk management, it should be considered across all business operations, and it has special relevance to an acquirer’s supply chains. Attacks against information – and the systems that process, store, and transmit that information – strike at the resilience (cyber- or otherwise) of the supply chain. Thus, protecting information can be regarded as a fundamental component of building cyber-resilience.

Building Cyber-Resilience in the Supply Chain

Good cybersecurity and cyber-resilience in the supply chain starts "at home". An organization that understands, in the broadest sense, which information it holds is sensitive, critical, or damaging should it be compromised will be able to protect its information and start to create resilience. Techniques such as classifying or labelling information and educating users about the utility and value of information will create or enhance a security-positive approach to how information is handled. Senior executives will need to champion this cause and ensure that resources are committed to achieving this information-centric approach. Hand in hand with this approach is the need for information security governance (as laid out in ISO/IEC27014: 2013[ISO, 2013b]) and information security strategy, to direct, manage, and deliver the approach inside the organization. Key to the success of this approach will be the ability to categorize, group, or define groups of related information – for example, trade secrets, intellectual property, legal documents, and commercial documents – and then express the harm caused should information in each group be compromised. Once this harm can be expressed, risk treatment options can be selected, using published or in-house processes and methodologies.

Protecting information is one part of this task. To build cyber-resilience across the supply chain, each organization needs to build a set of capabilities, both internal- and external-facing. A summary list for an organization, based on material published by the World Economic Forum (2012), is presented here:

1. Implement a cybersecurity (or information security) governance framework and place a member of the executive management team at its head.

2. Create a cybersecurity programme.

3. Integrate the cybersecurity programme with enterprise risk management approaches.

4. Communicate, share, and apply the cybersecurity programme with suppliers, educating them where necessary.

To achieve these four steps requires significant effort. The achievement can be assisted by the adoption of standards, the sharing of cyber-related information, such as threats, attacks, weaknesses, and mitigations – a point made in several publications (Information Security Forum, 2012; World Economic Forum, 2012). For many organizations, they do not have the resources, expertise, or time to act on cyber-related information, or they may be reliant on a supplier to act for them. This is where education and, if necessary, actually investing in a supplier’s capabilities may be required and may yield a return.

Building Cyber-Resilience into Supply Chains

Adrian Davis

Conclusion

So, building cyber-resilience starts at the organization. This article has discussed components of organizational cyber-resilience such as an information-centric approach, adopting a governance framework, a strategy of integrating information into the procurement cycle. To extend cyber-resilience to the supply chain, an acquirer needs to take the following further actions:

1. **Map the supply chain.** Many organizations do not actually understand the make-up of their supply chains. Even Toyota, often held up as an example of supply chain excellence, could not map its chain (Supply Chain Digest, 2012). Mapping is complicated by the resources available, the number of suppliers an organization may have, the willingness of suppliers to reveal their suppliers, and the linear and lateral nature of the supply chains themselves. As an acquirer, understanding who is in a supply chain at Tier 1 and Tier 2 (even if partially) – and the information they may need from the acquirer – means that information risk and risk treatment can be better identified and addressed. Additionally, knowing the risks in the supply chain builds resilience, because the acquirer can prepare for incidents and interruptions. The acquirer can also spot potential weak links in the supply chain where information may be compromised. Mapping past Tier 2 may be very difficult for many acquiring organizations but some may have to do so for regulatory or other requirements.

2. **Build capability.** Both the acquiring organization and its suppliers may not have the resources, expertise, or knowledge to protect information. If a supplier cannot protect information or its systems, then it may provide a route for attackers to compromise both the supplier and the acquirer, thus causing harm and directly undermining the cyber-resilience of the supply chain. For an acquirer, helping suppliers to protect acquirer information is a win-win, because the costs of remediation after a breach and failure of resilience (perhaps including fines levied by regulators and any legal costs) will probably far exceed the costs of assisting a supplier to correct any deficiencies. Building capability does not necessarily mean employing experts to work in silos: integrating cybersecurity questions and checklists into procurement documents, or better yet, integrating cybersecurity professionals into the procurement process and function is an alternative and value-adding approach many organisations can take easily. Adopting standards such as the ISO/IEC 27036 series (ISO, 2014) discussed above and enhancing supply chain risk management to include information security- and privacy-related questions (such as PAS 7000:2014 [BSI, 2014]) can also raise an acquirer's capability and increase awareness in the supplier community. Acquirers and suppliers may wish to jointly invest in staff training as well.

3. **Share information and expertise.** Both acquirers and suppliers should share information about threats, attacks, and incidents – anything that may adversely affect their combined cyber-resilience. These organizations may also want to share information about the protective mechanisms they have in place – and their effectiveness – to further enhance their resilience. Sharing information about cyber-resilience can take many forms including joining government information-sharing networks, discussion and presentation within membership or other trusted groups, direct communication between individuals, and using social media. Sharing expertise may involve both acquirers and suppliers cross-posting staff, sharing best practice, recommending the use of standards or creating joint ventures to promote best practice across their supply chains and upstream suppliers. Acquirers may wish to provide education and training, to both on-boarded and prospective suppliers, about standards and frameworks that can be used.

4. **State requirements across the supply chain using standards, common frameworks, and languages.** Acquiring organizations should ensure that, whenever they work with suppliers, they follow standards and use a common language to promote understanding with their suppliers. Additionally, if the same standards, language, and frameworks are used with all suppliers, then the acquirer will have a basis for comparison between suppliers, which may assist risk management, supplier measurement, and associated efforts. Similarly, when an acquirer shares information, the requirements for protection should be couched in the same language for all suppliers. Using pass-through clauses and technology solutions, such as digital rights management may have a role to play here, as does education and training.

5. **Measure, assess, and audit.** All organizations in the supply chain will have to be able to measure their cybersecurity, their cyber-resilience, the cyber-risks in their supply chain and their governance. Additionally, organizations will need to be able to share and interpret these measurements, so they understand

Building Cyber-Resilience into Supply Chains

Adrian Davis

their own cyber-resilience, their partners, and the supply chain as a whole. Acquirers may need to define performance indicators for suppliers, based on their internal measurement systems, or they may have to create new measures in conjunction with their suppliers. Both acquirers and suppliers may need to create continuous monitoring and measurement systems to overcome the rather static nature of audits, and to allow the detection and prevention of and reaction to attacks in real time or near real time.

Cyber-resilience – the ability of a system that is dependent on cyberspace in some manner to return to its original [or desired] state after being disturbed – is an evolving and important concept. When applying cyber-resilience to the supply chain, the protection of information and its associated attributes (such as confidentiality, integrity, and availability), understanding information and cyber-risks across the supply chain and building a collaborative approach are important concepts. Yet, it is these areas where much work needs to be done, because information and cyber-risk assessment across supply chains are emerging fields of research; there is thus little to guide organizations and little best practice for them to study and adapt.

About the Author

Adrian Davis, PhD, MBA, FBCS CITP, CISSP, heads the Europe, Middle East, and Africa (EMEA) team for (ISC)^2, the global, not-for-profit leader in educating and certifying information security professionals throughout their careers. His role is to deliver the (ISC)^2 vision of inspiring a safe and secure cyber-world and its mission of supporting and providing members and constituents with credentials, resources, and leadership to secure information and deliver value to society. Before working for (ISC)^2, Adrian delivered practical business solutions to over 360 blue-chip multinational clients for the Information Security Forum. His expertise included: managing information security in supply chains; information security governance and effectiveness; the relationship between information security and business continuity; and possible near-term threats to organizations. Adrian regularly attends and chairs conferences and contributes articles for the press. He also contributed to the development of *ISO/IEC 27014: Governance of Information Security* and currently acts as a co-editor for *ISO/IEC 27036 Information Security in Supplier Relationships, Part 4: Guidelines for Security of Cloud Services.*

References

BSI. 2014. *PAS 7000 Supply Chain Risk Management – Supplier Prequalification.* The British Standards Institution. Accessed March 26, 2015: http://www.bsigroup.com/en-GB/PAS7000/

Christopher, M. 2011. Logistics and Supply Chain Management (4th ed.). London: FT Prentice Hall.

Davis, A., & Skelton, E. 2014. Engaging the Board: Resilience Measured. In L. Bird (Ed.), *Operational Resilience in Financial Institutions.* London: Risk Books.

Information Security Forum. 2012. *Cyber Security Strategies: Achieving Cyber Resilience.* London: Information Security Forum.

ISO. 2013a. *ISO/IEC 27001:2013 Information Technology – Security Techniques – Information Security Management – Requirements. International Organization for Standardization.* Accessed February 9, 2015: http://www.iso.org/iso/catalogue_detail.htm?csnumber=54534

ISO. 2013b. *ISO/IEC27014: 2013: Information Technology – Security Techniques – Governance of Information Security. International Organization for Standardization.* Accessed February 9, 2015: http://www.iso.org/iso/catalogue_detail.htm?csnumber=43754

ISO. 2014. *ISO/IEC 27036: Information Technology – Security Techniques – Information Security for Supplier Relationships. International Organization for Standardization.* Accessed February 9, 2015:
Part 1: Overview and Concepts: http://www.iso.org/iso/catalogue_detail.htm?csnumber=59648
Part 2: Requirements: http://www.iso.org/iso/catalogue_detail.htm?csnumber=59680
Part 3: Guidelines for Information and Communication Technology Supply Chain Security: http://www.iso.org/iso/catalogue_detail.htm?csnumber=59688
Part 4 (under development): Guidelines for Security of Cloud Services: http://www.iso.org/iso/catalogue_detail.htm?csnumber=59689

Krebs, B. 2014. Target Hackers Broke in via HVAC Company. *Krebs on Security,* February 5, 2014. Accessed April 1, 2015: http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

Peck, H., Abley, J., Christopher, M., Haywood, M., Saw, R., Rutherford, C., & Strathern, M. 2003. *Creating Resilient Supply Chains: A Practical Guide.* Bedford, UK: Cranfield School of Management, Cranfield University.

Building Cyber-Resilience into Supply Chains

Adrian Davis

Supply Chain Digest. 2012. Global Supply Chain News: Toyota Taking Massive Effort to Reduce Its Supply Chain Risk in Japan. *Supply Chain Digest,* March 7, 2012. Accessed February 9, 2015: http://www.scdigest.com/ontarget/12-03-07-2.php?cid=5576

Tipton, H. F., & Hernandez, S. (Eds.) 2013. *Official (ISC)^2 Guide to the CISSP CBK* (3rd ed.). Boca Raton, FL: CRC Press.

Waters, D. 2011. *Supply Chain Risk Management* (2nd ed.). London: Kogan Page.

World Economic Forum. 2012. *Partnering for Cyber Resilience.* World Economic Forum. Accessed February 9, 2015: http://www.weforum.org/projects/partnership-cyber-resilience

Citation: Davis, A. 2015. Building Cyber-Resilience into Supply Chains. *Technology Innovation Management Review,* 5(4): 19–27. http://timreview.ca/article/887

Keywords: cyber-resilience, cybersecurity, supply chain, resilience, direct suppliers, Tier 1 suppliers, indirect suppliers, procurement, information-centric approach, requirements

Cybersecurity and Cyber-Resilient Supply Chains

Hugh Boyes

> *"Our technological powers increase, but the side effects and potential hazards also escalate."*
>
> Alvin Toffler
> Writer and futurist
> in *Future Shock*

There has been a rapid growth in the use of communications and information technology, whether embedded in products, used to deliver services, or employed to enable integration and automation of increasingly global supply chains. Increased use of information technology introduces a number of cybersecurity risks affecting cyber-resilience of the supply chain, both in terms of the product or service delivered to a customer and supply chain operation. The situation is complicated by factors such as the global sourcing of technology components or software, ownership of the systems in a supply chain, different legal jurisdictions involved, and the extensive use of third parties to deliver critical functionality. This article examines the cyber-resilience issues related to the supply of products, services, and the supply chain infrastructure considering the nature of threats and vulnerabilities and the attributes of cybersecurity. In doing so, it applies a model for cybersecurity that is adapted from the Parkerian hexad to explore the security and trustworthiness facets of supply chain operations that may impact cyber-resilience.

Introduction

Over forty years ago in his book *Future Shock*, Alvin Toffler (1971) recognized that our rapid technological advances were accompanied by side effects and hazards. This is certainly true of supply chains in the 21st century, where information technology is often an integral part of both the supplied product or service, and the supply chain infrastructure.

To stay competitive in a global economy, deliver timely responses to changing customer demands, and meet increasing service expectations, organizations have adapted their supply chains by incorporating computer-based management systems (Christopher & Towill, 2002), automating many processes using cyber-physical systems, and reducing stocks through the deployment of just-in-time manufacturing and production-to-order systems. This widespread use of information technology and advances in connectivity have transformed many businesses and transferred supply chain information flows from paper or the telephone to digital transactions and databases (WEF, 2013). The improved communications flow has also delivered significant advances in the service offered by supply chains to their customers, enabling the tracking of goods through the logistics chain.

These innovations place significant demands on supply chains, with the role of information technology now critical to the delivery of responsive, cost-effective manufacturing and supply (Christopher & Peck, 2004; Khan & Stolte, 2014).

This article discusses how, in many information technology systems, insufficient attention has been paid to overall system resilience and security issues, creating significant cybersecurity and cyber-resilience vulnerabilities. It examines what is meant by cyber-resilience and cybersecurity, and outlines the attributes that affect the cyber-resilience of a system or system-of-systems. Although the underpinning work originates in the construction and built-environment sectors, this article demonstrates that it can be applied more widely.

What Do We Mean by Cyber-Resilience and Cybersecurity?

The World Economic Forum (WEF, 2012) defined cyber-resilience as "the ability of systems and organiza-

Cybersecurity and Cyber-Resilient Supply Chains

Hugh Boyes

tions to withstand cyber events, measured by the combination of mean time to failure and mean time to recovery". The use of the term "cyber" is intended to encompass the "interdependent network of information technology infrastructures, and includes technology "tools" such as the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries". Although not defined by the WEF, it is assumed that a cyber-event is therefore any disturbance to this interdependent network that leads to loss of functionality, connectivity, performance, or capacity (i.e., a breach of the network's cybersecurity). Such events are all too common, with frequent publicity about yet another serious security breach on an IT system. Notable recent examples include the cyber-attacks on Sony and Target. The latter incident is of particular significance given that the attack originates in the company's supply chain, with the initial compromise of an HVAC supplier's systems (Krebs, 2014).

There is a common misconception, reinforced by media coverage of incidents, that cybersecurity is solely about technology. This is not the case: good cybersecurity is based on a holistic approach that encompasses people, process, physical, and technological aspects (Boyes, 2014a). A weakness in the treatment or implementation of one or more of these aspects will undermine the overall cybersecurity of a system or business process. For example, if an individual does not practice good cyber-hygiene or fails to follow established security processes – such as failing to protect sensitive physical storage media from theft or loss – then there is an increased risk of compromise.

The lack of attention to system security and resilience, referred to in the introduction, is illustrated by the Apple "goto fail" bug and the "Heartbleed" vulnerability (Boyes et al., 2014). In the case of the former, a simple coding error exposed all iOS users to a serious vulnerability in the Transport Layer Security (TLS) protocol, which is used by applications to secure Internet communications. In the latter, poorly written code, which had not been subject to adequate inspection or test, exposed users of OpenSSL to a serious vulnerability. The affected OpenSSL software had been deployed by many of the major industrial control systems (ICS) suppliers. In both cases, the cause of the security breach is poor software engineering and a failure to detect coding errors during integration and testing.

Figure 1 illustrates the categories of risk that need to be considered when assessing the cyber-resilience of a supply chain. The presence of nature may seem at odds in a discussion of cyber-resilience, however, it is important to recognize that natural events can have significant impact on communications and IT infrastructure. For example, solar storms can disrupt wireless communications, both on a global scale for satellite communications and on a local scale for mobile communications (3G and 4G). Natural causes, such as earthquakes, floods, and damage by animals may also damage or disrupt cable connections carrying telephony and Internet traffic, thus interfering with a supply chain.

To improve the cyber-resilience of a supply chain, it is essential to understand the various aspects that should be addressed in designing for cybersecurity. Much of the good practice currently available is based on the information assurance community's use of the "CIA triad": confidentiality, integrity, and availability. However, this approach does not adequately address the cyber-security of complex global information technology systems or the cyber-physical systems used in our supply chains. An alternative approach, which is better suited to these complex systems, is to start by considering the Parkerian hexad (Parker, 2002), which comprises confid-

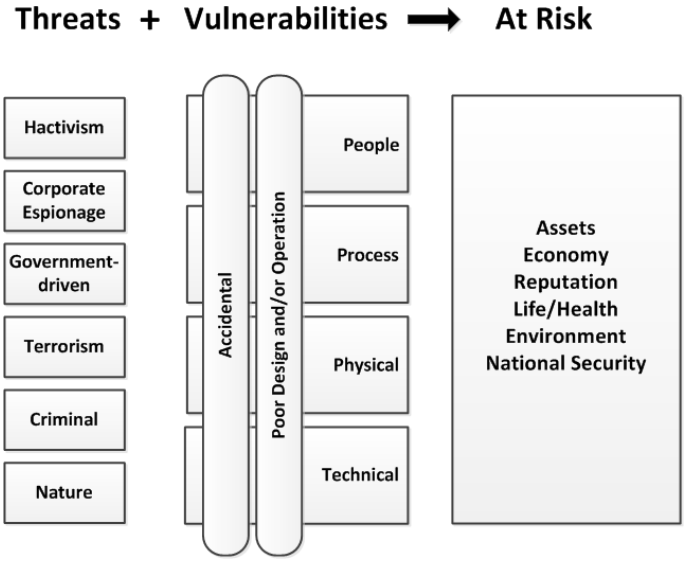

Figure 1. Threats and vulnerabilities that affect cyber-resilience

Cybersecurity and Cyber-Resilient Supply Chains

Hugh Boyes

entiality, integrity, and availability, plus utility, authenticity, and possession. The rationale for this approach is that the hexad better encompasses the security considerations that apply to control systems and cyber-physical systems (Boyes, 2014b); however, it does not fully address the need for systems to be trustworthy.

The United Kingdom Government has supported the development of a publicly available specification for trustworthy software, where trustworthiness is based upon five facets: safety, reliability, availability, resilience, and security (BSI, 2014). It is therefore proposed that, in considering the cyber-resilience of the complex systems in the supply chain, we should augment the Parkerian hexad with two additional attributes, safety and resilience, as illustrated in Figure 2. Although the reliability of the supply chain is a by-product of addressing the other attributes, the model associates it with availability.

This model for cyber-security enables us to consider the supply chain from three perspectives:

1. The continuity of operations, including safety of personnel and assets (i.e., availability, safety, and resilience)

2. The control of access and system operations (i.e., confidentiality and possession)

3. The quality and validity of information, including the system's configuration (i.e., integrity, utility, and authenticity)

This model has been developed based on investigation of the security and resilience issues affecting cyber-physical systems (Boyes, 2014b) and has been extended to fully integrate the facets of trustworthiness (BSI, 2015).

The importance of the individual perspectives and their underpinning attributes will vary between supply chains, but serious vulnerabilities in any attribute or perspective are likely to result in significant loss of overall cyber-resilience. In the following sections, this model will be applied to explore the cyber-resilience of the supply of products, the supply of services, and the supply chain infrastructure.

Cyber-Resilience and the Supply of Physical Products or Assets

The scale and complexity of the supply chains for physical products or assets vary widely, but the generic end-to-end process may be represented as shown in Figure 3. From a cyber-resilience perspective, there are a number of areas that could be disrupted:

- the specification and design process for new, bespoke, or customized products

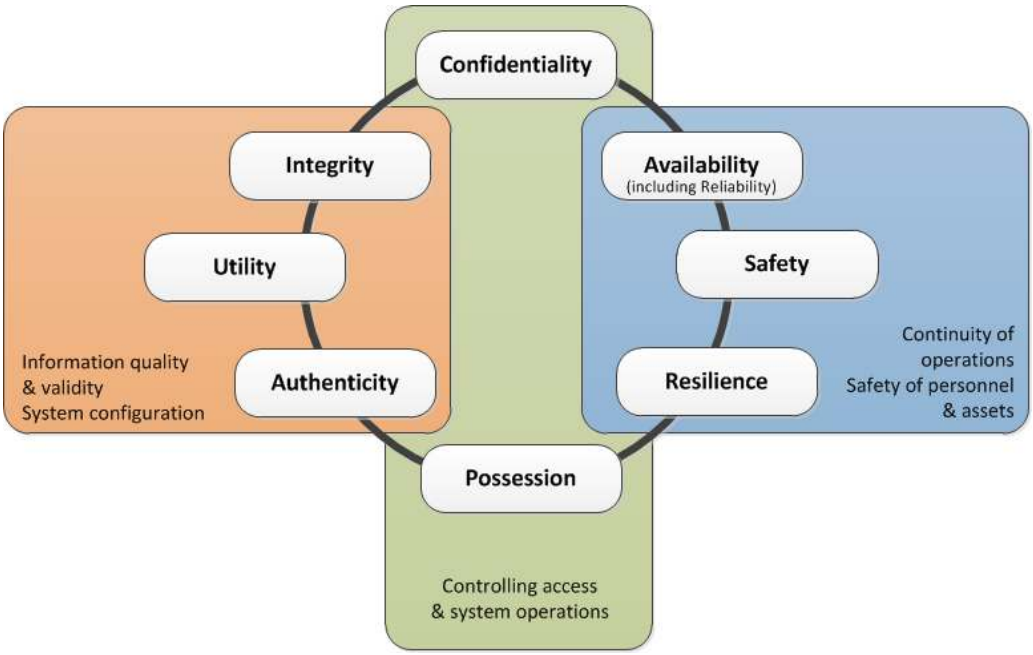

Figure 2. Cybersecurity attributes that affect cyber-resilience

Cybersecurity and Cyber-Resilient Supply Chains

Hugh Boyes

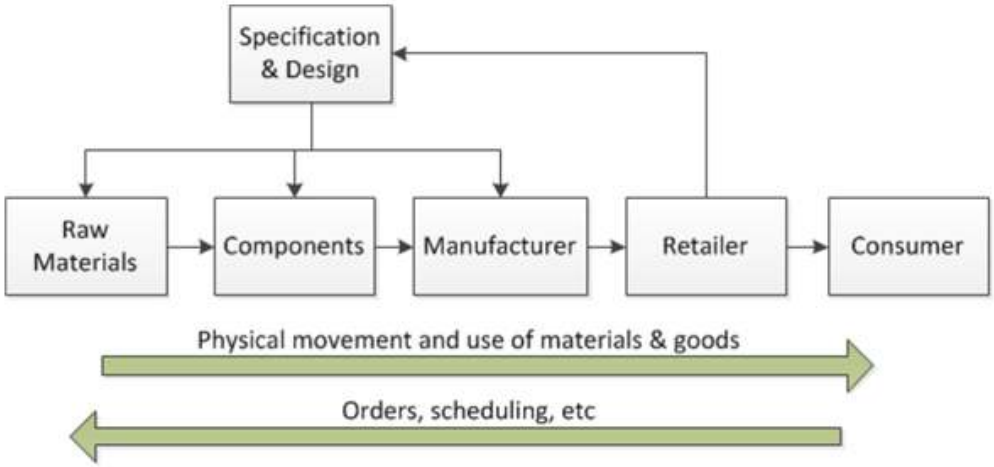

Figure 3. Generic supply chain for physical products or assets

- the flow of orders, scheduling ,and associated information
- the coordination and control of the movement of supplies and finished products through the supply chain

The nature of cyber-resilience issues will vary over a product's lifecycle. For example, during product specification and design, threats and vulnerabilities that affect the integrity or authenticity of information are particularly important. A manufacturer of high-availability pumps used in hazardous environments discovered this when an unauthorized change to tolerances of a critical mechanical component led to premature failures of the installed product and escalating warranty claims.

Once product design is complete, the long-term utility of design information becomes a resilience issue. The typical lifecycle of many software packages, for example, computer-aided design packages, is often much shorter than the operational life of capital items and major assets. The packages go through regular software revisions and their operating systems become obsolete. For manufacturers employing computer-aided design and computer-aided manufacturing (CADCAM) today, this may be a serious issue if they need to access original design information in say 10 or 20 years. This problem is already a reality for documents created using common word-processing packages in the 1980s and early 1990s.

In some cases, it is the metadata associated with a physical product that may be at risk. For example, the use of collaborative tracking and tracing by the Swedish fresh fish supply chain to track codfish catches from trawlers though the supply chain to the end consumer (Mirzabeiki, 2013). The raw fish is a perishable product that is handled by multiple organizations as it moves from sea to plate. There are ample opportunities for this tracking to fail due to human actions or the breakdown or failure of IT equipment.

There are also integrity and authenticity issues regarding digital information and software embedded in products. In particular, there are risks associated with the presence of counterfeit electronic products, assemblies, and software in supply chains. Examples of this problem include the discovery that Dell had shipped malware infected components during 2010 (Grainger, 2010), HP shipped malware-laden switches in 2011 (Rashid, 2012), and Microsoft discovered during 2012 new PCs in China preinstalled with malware (Kirk, 2012). These examples illustrate the need for good cybersecurity practices in the procurement, manufacture, and distribution of products containing software: failure to do so can cause significant disruption to the supply chain and its customers.

The recent cyber-attack on a German blast furnace (Zetter, 2015) illustrates how poor cybersecurity can have a major impact on the continuity of operations, including safety of personnel and assets (i.e., availability, safety, and resilience). In this case, there appears to have been a serious breach of the access controls on the plant's industrial control systems, allowing the attacker to cause the plant to malfunction and resulting in physical damage and operational disruption. Man-

Cybersecurity and Cyber-Resilient Supply Chains

Hugh Boyes

aging the control of access and system operations (i.e., confidentiality and possession) can be a complex task, particularly on large sites where there is wireless access to these systems. This challenge was illustrated by the Maroochy water treatment works incident, where a former contractor had unauthorized access to the plant controls (Abrams & Weiss, 2008). The cause of the sewage spillages was a mystery until a site engineer witnessed a valve being remotely changed.

From a cyber-resilience perspective, the above examples illustrate the importance of good cybersecurity in the supply of items containing electronic data or software and in the operation of cyber-physical systems. With fragmented supply chains spanning the globe, there is a need for constant vigilance and good situational awareness to counter emerging and existing threats that affect cyber-resilience.

Cyber-Resilience and the Supply of Services

The supply of services creates a number of additional challenges in terms of a supply chain's cyber-resilience. Depending on the nature of the service, a cyber-event may make it difficult for personnel and systems involved in service delivery to receive, process, and fulfill service requests. Typically, the cyber-resilience issues affecting the supply of services will predominantly relate to the operation of call centres, websites, payment systems, and where the service involves electronic delivery of content, for example playing a pay-per-view video, the fulfillment systems.

Often predominantly Internet-based, the service delivery infrastructure is vulnerable to a range of generic cybersecurity attacks, for example denial of service (DoS), distributed denial of service (DDoS), and the hacking of servers, routers, and switches. The techniques for dealing with DoS and DDoS attacks, and protecting infrastructure from hacking are understood, although often not applied. From a cyber-resilience perspective, organizations offering services need to invest in appropriate hardening and protection of all critical digital aspects of their supply chain.

It is important to recognize that, for service delivery supply chains, the threats and vulnerabilities in Figure 1 may affect only parts or all of the supply chain. This is particularly relevant where key components rely on outsourced or bought-in elements, over which the service operator may have minimal control. For example, where the service is ordered and paid for online prior to service delivery, to meet the payment card industry's security standards (PCI DSS), it is common practice for websites to employ payment gateways operated by third parties. These gateways have themselves been the target of cyber-attacks, denying the use of their service and therefore either preventing organizations receiving payment or seriously degrading the performance of the payment systems. To mitigate such events and maintain cyber-resilience, an organization would need to have business continuity plans in place that allow use of alternative payment engines or otherwise restore the performance of the payment process.

Organizations also need to put in place adequate capacity to handle peaks in demand. There have been a number of cyber-resilience incidents where a website has crashed or otherwise failed to handle peak traffic volumes. Examples include problems with national authorities websites on the deadline day for submission of personal tax returns, the collapse of ticketing systems for major events such as concerts and sporting events, and the launch of online sales events. These peaks of traffic are generally predictable and cyber-resilient systems should be able to satisfactorily handle surges in demand.

Cyber-Resilience and Supply Chain Infrastructure

Given the global nature of both trade and supply chains, there are three infrastructure elements that will have a significant impact on their cyber-resilience. These are the ports used to handle goods and raw materials, the navigation systems used by both cargo carry vessels and delivery vehicles, and the global data processing, storage, networking, and communication infrastructure. The latter elements are often referred to as ”the cloud”.

In October 2013, there were press reports about an operation in the port of Antwerp, where police discovered that a criminal gang had gained access to the port's logistics systems in order to smuggle drugs through the port (Bateman, 2013). This sophisticated cyber-attack, which it is believed had started two years earlier, allowed the gang to access the computer system used to manage the handling and release of shipping containers, enabling the gang to remove the drugs from the port without being detected. The sophistication of this attack mirrors other unreported incidents, where it is understood that valuable goods have been targeted and stolen. Breaches of security have serious implications for the integrity of supply chains, both with regard to the protection of goods or materials in transit, and to prevent substitution of counterfeit supplies.

Cybersecurity and Cyber-Resilient Supply Chains

Hugh Boyes

The widespread use of global navigation satellite systems (GNSS) is taken for granted by most transport and fleet operators. The benefits are considerable from a logistics perspective, in particular, the ability to precisely locate and route aircraft, vessels, and road vehicles. Unfortunately, these navigation signals from satellites are vulnerable to jamming and interference, which can severely degrade navigation in affected areas. While the occasional presence of localized interference or jamming is generally an inconvenience, if a large solar storm were to occur, of a similar magnitude to the 1859 Carrington event (tinyurl.com/mhsmve), disruptions to satellite transmissions could have a serious impact on the cyber-resilience of many supply chains.

The use of cloud computing is increasing rapidly, but this is not without risk. At the end of January 2013, 2e2, an IT systems and cloud service provider in the United Kingdom went into liquidation (Robinson, 2013). The immediate effect was that 2e2 customers lost access to their hosted systems and data, and were faced with demands for payment from the liquidator if they wished to keep the data centres running or retain access to their data. To reduce IT costs, organizations are being encouraged to replace their own locally-based servers with cloud-based services. The cyber-resilience consequences of such actions need to be carefully assessed, particularly where the hosted services are mission critical.

A consequence of the increased adoption of cloud services, as well as the global nature of many supply chains, is the dependence on smooth functioning of the global communications and networking services. The nature of these services is complex, relying largely on undersea telecommunications cables that span the globe. These cables are vulnerable to both natural and human damage, the former due to geological incidents such as earthquakes. In May 2013, it was reported that the SEA-ME-WE4 cable had been cut near Alexandria in Egypt (Malik, 2013). This was a deliberate act, although it is more common for such cuts to be the result of cables snagging on fishing nets or anchors. The cut resulted in a dramatic slow down in communications traffic speeds in Africa, the Middle East, and part of India, by as much as 60% in some locations. This type of damage could have serious consequences if the link is carrying time-sensitive supply chain scheduling data or provided connectivity to business critical cloud-based services. From a cyber-resilience perspective, supply chain managers should consider the impact that any loss or degradation of global communications infrastructure may have on their operations.

Conclusion

This article has considered the cyber-resilience of supply chains that deliver both physical products and services. In both cases, there are key cybersecurity issues that need to be addressed if an acceptable level of cyber-resilience is to be achieved. It is important that cyber-resilience, like cybersecurity, is not considered to be a purely technical issue, as it is also affected by personnel, process, and physical aspects.

A model of cybersecurity based on the Parkerian hexad has been outlined, which addresses important aspects that determine whether a system or process is cybersecure. This model is particularly relevant to complex, time-critical and cyber-physical systems as it fully addresses continuity of operation, control of access and systems operations, and data quality and systems configuration. It is currently being documented for use in the construction industry supply chain to support deployment of security-minded building information modelling (BIM) in the United Kingdom. As illustrated in this article, it is applicable to other supply chains. When considering the elements in this model, it is essential that personnel, process, and physical aspects are addressed in addition to underlying technical issues.

When designing or modifying a supply chain, it is essential that the organizations involved consider the cyber-resilience implications of the global technology components they plan to use. Moving applications into the cloud and the remote storage of data can introduce significant cyber-resilience issues, particularly where time-critical processing or data access is required.

Supply chain managers should examine the vulnerabilities of the technologies involved, including the physical location of business-critical elements, the interdependence of components and business processes, and the skills required by personnel involved in supply chain operations. Achieving cyber-resilience will involve a holistic approach to security, given that purely technical solutions are unlikely to address the breadth of potential threats and vulnerabilities.

Recommended Reading

Code of Practice for Cyber Security in the Built Environment (Institution of Engineering and Technology, 2014; tinyurl.com/oyjkkk6).
This book provides a strategic approach to managing the cybersecurity of cyber-physical systems that is also of relevance to supply chains.

Cybersecurity and Cyber-Resilient Supply Chains

Hugh Boyes

About the Author

Hugh Boyes is a Principal Fellow at WMG at the University of Warwick, United Kingdom, where he focuses on cyber-resilience and the cybersecurity of cyber-physical systems. He is a Chartered Engineer, a Fellow of the IET and holds the CISSP credential issued by (ISC)2. Hugh is also the Cyber Security Lead at the Institution of Engineering and Technology (IET), where he focuses on developing cybersecurity skills initiatives for engineering and technology communities. This work is particularly focused on the design and operation of physical-cyber systems (e.g., industrial control systems, building automation systems). He has written two guidance documents for the Institution of Engineering and Technology (IET) on cybersecurity in the built environment, and with Alex Luck, is the joint technical author of a BSI publicly available specification (PAS) on security-minded building information modeling, digital built environments, and smart asset management.

References

Abrams, M., & Weiss, J. 2008. *Malicious Control System Cyber Security Attack Case Study - Maroochy Water Services, Australia.* National Institute of Standards and Technology, Computer Security Division.

Bateman, T. 2013. Police Warning after Drug Traffickers' Cyber-Attack. *BBC News,* October 16, 2013. Accessed March 14, 2015: http://www.bbc.co.uk/news/world-europe-24539417

Boyes, H. A. 2014a. *Code of Practice for Cyber Security in the Built Environment.* London: Institution of Engineering and Technology.

Boyes, H. A. 2014b. Cyber Security Attributes for Critical Infrastructure Systems. *Cyber Security Review,* Summer 2014: 47–51.

Boyes, H. A., Norris, P., Bryant, I., & Watson, T. 2014. Trustworthy Software: Lessons from `goto fail' & Heartbleed bugs. In *Proceedings of the 9th IET International Conference on System Safety and Cyber Security:* 2.2.1. http://dx.doi.org/10.1049/cp.2014.0970

BSI. 2014. *PAS 754:2014 Software Trustworthiness – Governance and Management – Specification.* London: British Standards Institution.

BSI. 2015. *PAS 1192-5:2015 Specification for Security-Minded Building Information Modelling, Digital Built Environments and Smart Asset Management.* London: British Standards Institution.

Christopher, M., & Peck, H. 2004. Building the Resilient Supply Chain. *International Journal of Logistics Management,* 15(2): 1–13. http://dx.doi.org/10.1108/09574090410700275

Christopher, M., & Towill, D. 2002. Developing Market Specific Supply Chain Strategies. *International Journal of Logistics Management,* 13(1): 1–13. http://dx.doi.org/10.1108/09574090210806324

Grainger, M. 2010. Dell Shipped Malware Infected Components. *PCR,* July 22, 2010. Accessed March 14, 2015: http://www.pcr-online.biz/news/read/dell-shipped-malware-infected-components/021984

Khan, O., & Stolte, T. 2014. The Rising Threat of Cyber Risks in Supply Chains. *Effektivitet,* 4 (2014): 32–35.

Kirk, J. 2012. Microsoft Finds New PCs in China Preinstalled with Malware. *PCWorld,* September 14, 2012. Accessed March 14, 2015: http://www.pcworld.com/article/262308/

Krebs, B. 2014. Target Hackers Broke in Via HVAC Company. *Krebs on Security*, February 5, 2014. Accessed March 14, 2015: http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

Malik, O. 2013. Underseas Cable Cut Near Egypt, Slows down Internet in Africa, Middle East, South Asia. *Gigaom,* March 27, 2014. Accessed March 14, 2015: http://gigaom.com/2013/03/27/undersea-cable-cut-near-egypt-slows-down-internet-in-africa-middle-east-south-asia/

Mirzabeiki, V. 2013. *Collaborative Tracking and Tracing – A Supply Chain Perspective.* Gothenburg, Sweden: Chalmers University of Technology.

Parker, D. B. 2002. Towards a New Framework for Information Security. In S. Bosworth & M. E. Kabay (Eds.). *Computer Security Handbook* (4th ed). Hoboken, NJ: John Wiley & Sons.

Rashid, F. Y. 2012. HP's Malware-Laden Switches Illustrate Supply Chain Risks. *PC Magazine*, April 12, 2012. Accessed March 14, 2015: http://securitywatch.pcmag.com/pc-hardware/296547-hp-s-malware-laden-switches-illustrate-supply-chain-risks

Robinson, D. 2013. 2e2 Collapses Amid Failure to Find Buyer. *Financial Times*, February 6, 2013. Accessed March 14, 2015: http://www.ft.com/cms/s/0/2332e418-7077-11e2-a2cf-00144feab49a.html

Toffler, A. 1971. *Future Shock.* New York, NY: Bantam Doubleday.

WEF. 2012. *Partnering for Cyber Resilience: Risk and Responsibility in a Hyperconnected World – Principles and Guidelines.* Geneva, Switzerland: World Economic Forum.

WEF. 2013. *Building Resilience in Supply Chains.* Geneva, Switzerland: World Economic Forum.

Zetter, K. 2015. A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever. *Wired,* January 8, 2015. Accessed March 14, 2015: http://www.wired.com/2015/01/german-steel-mill-hack-destruction/

Citation: Boyes, H. 2015. Cybersecurity and Cyber-Resilient Supply Chains. *Technology Innovation Management Review*, 5(4): 28–34. http://timreview.ca/article/888

Keywords: cyber-resilience, cybersecurity, supply chain, risk management, threat management

Challenges in Maritime Cyber-Resilience

Lars Jensen

> *"Maritime cyber-attacks are no longer the stuff of science fiction. They are happening now, and the threats are growing."*
>
> Fred Roberts
> Professor of Mathematics and Director of CCICADA

The maritime industry has been shown to be under increasing levels of cyber-attack, with future attacks having the potential to severely disrupt critical infrastructure. The industry lacks a standardized approach to cybersecurity, a national approach will be counterproductive, and a global mandatory standard, while needed, will take a long time to implement. In the shorter term, this article recommends that the industry coalesce around a set of voluntary guidelines in order to reduce the risk profile and increase resilience. To provide context for these recommendations, this article examines the specific characteristics of the maritime industry in relation to cybersecurity. Examples of existing vulnerabilities and reported cyber-attacks demonstrate that the threat is current and real.

Introduction

The maritime industry is the foundation for the efficient functioning of all aspects of modern society, from the supply of raw materials such as oil, iron, and grain to virtually every product on the shelves of the local stores and supermarkets – and it is wide open to disruptive cyber-attacks.

In the wake of the 9/11 attacks on the Twin Towers in New York, the maritime industry saw an escalation in physical security procedures aimed at reducing the risk of paralyzing vital infrastructure; in particular, there was a focus on port security (IMO, 2015). However, a similarly security-conscious approach is found to be lacking in relation to cyber-risks. As this article will demonstrate, a closer investigation of the landscape of both cyber-threats and actual incidents in the maritime sector, shows that risks are indeed real and that the impact of an attack can range far beyond the company being attacked.

A hypothetical scenario to illustrate the point would be a cyber-attack that involved the deletion of operational data in a few large container shipping terminals. Such an attack would choke the entire supply chain for tens of thousands of companies. The 100 largest container ports globally each handle in excess of one million 20-foot containers annually (Lloyds List, 2014). Shutting down just a handful within the same geographical region means that the overflow cannot be handled elsewhere. The economic impact on society would be large. In 2002, the key ports on the western coast of the United States were shut down for ten days due to a labour dispute. At that point in time, it was estimated that this had a cost to the United States economy of $1-2 billion USD per day due to disrupted supply chains (Cohen 2002). Since then, the volume of containerized trade has grown significantly, and hence a cyber-attack shutting down key ports can thus be expected to have an even larger impact on the national economy of the affected country – or countries.

Four key sources provide an overall perspective on this issue:

1. A study by the European Union Agency for Network and Information Security (ENISA, 2011) provides a baseline analysis of maritime cybersecurity and the related policy context.

2. A policy paper by The Brookings Institution focused on critical infrastructure cyber-vulnerabilities in port facilities in the United States (Kramek, 2013).

Challenges in Maritime Cyber-Resilience

Lars Jensen

3. A United States Senate (2014) inquiry into cyber-intrusions emphasized the threat of cyber-attacks on the networks of the United States Transportation Command, which is responsible for Department of Defense transportation, including maritime transportation.

4. A whitepaper issued by the author's maritime cybersecurity company, CyberKeel (2014a), examined the vulnerability of the maritime industry to various cyber-risks and highlighted its lack of adequate defenses.

Generally, these studies all arrived at the same conclusion, albeit while covering different sub-domains. The various authors found the levels of cybersecurity to be very low and that significant and dedicated efforts were needed to improve the situation. They furthermore showed that the amount of publically reported incidents do not represent the actual amount of malicious activity ongoing in the industry – a fact particularly underscored by the US Senate inquiry, which revealed a large gap in reporting despite such reporting being mandatory in stated contractual terms with suppliers.

This article aims to propose immediate and longer-term steps the industry can take to improve its cyber-resilience. It will initially examine the specific characteristics of the maritime industry that are of importance in relation to cybersecurity. It will assess whether certain types of threats are to be considered theoretical or whether they have in fact already been seen, and then it will identify the likely entities behind the threats. Finally, the emerging view of the industry will be used to recommend how cybersecurity and cyber-resilience can be improved in the maritime industry in both the short and long term.

Industry Characteristics

In terms of cyber security, the maritime industry has a range of characteristics that makes it difficult to implement solid cyber-defenses. To illustrate the point, it is worthwhile examining how a generic container shipping line operates. A large container shipping line will have offices spread across 150 different countries. They own, and hence control, half of these offices, but for the other half, they rely on the services of local agents. The shipping line thus has to share access to key backend systems with a large number of local agents who have their own IT infrastructure, and where the shipping line usually has extremely limited insight, and influence, on the cybersecurity standards.

Additionally, the shipping line may be operating a fleet of 300 vessels of which they own 150. The other 150 vessels are chartered from a wide range of vessel-owning companies for short- or medium-term duration. The shipping line will not have the ability to control the IT structure onboard vessels chartered for a shorter period. Even for the vessels the shipping line owns, cybersecurity on vessels tend to be an issue. In many shipping companies, the IT department located at headquarters tends to be in charge of land-based IT systems, whereas the vessel-based IT systems fall under the purview of the marine technical department – who often have very limited IT background knowledge. Adding to the challenges, the shipping line may not be the one fully in control over the crewing of the vessel, hence opening an avenue for social engineering intrusion on board the vessels themselves. A tangible example of such a scenario was shared with CyberKeel by a physical maritime security company. They had experienced a vessel approaching the Gulf of Aden, which at the time had a significant piracy risk. However, prior to entering the Gulf of Aden, it was discovered that a person onboard the vessel had been uploading significant amounts of images to a Facebook account – images that provided a detailed look into the safety measures in place on the vessel. The ability to do this is a consequence of the recent, rapid roll-out of "crew welfare", which is the term most often used to indicate making Internet access available to crew using satellite connections.

Finally, when a container is moved from point A to point B, the information related to this movement may pass through between 10 and 50 different systems, each being controlled by different entities such as ports, customs offices, trucking companies, banks, shared-service centres, and industry information portals. These entities do not share a common IT infrastructure, nor do they have any agreed cybersecurity standards. At CyberKeel, we have asked several of the major players in the industry who provide IT systems or IT services how often their customers ask about the cybersecurity aspects of a link-up. The answers are that this is not the norm, the discussion is basically focused on functionality. Given that the successful movement of illicit cargo, or the theft of cargo, only requires successful penetration of one or two of these many hand-over points, it is easy to see how this system can be utilized by criminal elements.

The industry is hence characterized by companies who may have solid control of central parts of their own IT landscape, but have limited – or no – control over more "remote" parts of the landscape. These remote parts

Challenges in Maritime Cyber-Resilience

Lars Jensen

thus present an easy access approach to attacks directed at the central elements of the IT landscape.

Is the Threat Genuine?

As CyberKeel approached management layers in many maritime companies in the first half of 2014 on the topic of cybersecurity, many voiced the opinion that the threats appeared to be more theoretical than real. After all, the fact that something can be done is not the same as somebody actually going through the trouble of doing it.

As a consequence, CyberKeel issued a whitepaper (Cyberkeel, 2014a) and subsequently started a monthly newsletter called Marine Cyberwatch (tinyurl.com/ozxukd5) including an identifications of actual attacks across the maritime sector. Some attacks had already been known, particularly within the cybersecurity sector, but still appeared to be relatively unknown by maritime managers. Additionally, a number of attacks were described that, until then, had been relatively unknown.

One such incident was a cyber-attack against the Iranian shipping line IRISL, which took place in August 2011 (cited in CyberKeel, 2014a). The attacks damaged all the data related to rates, loading, cargo number, date and place, meaning that "no-one knew where containers were, whether they had been loaded or not, which boxes were onboard the ships or onshore" (CyberKeel, 2014a). Although the correct data was eventually restored, the company's operations were significantly impacted: the company's internal communication network was disrupted, cargo was sent to the wrong destinations, and the company suffered severe financial losses in addition to losses of actual cargo. A similar attack on a major international container line would have a crippling effect on the supply chains of thousands of international companies.

Another incident was first reported by CyberKeel based on a forensic analysis performed by Clearsky, a cyber-intelligence company (CyberKeel, 2014b). A number of maritime companies – principally shipping lines and bunker fuel suppliers – were infiltrated with a remote access tool. This remote access was used to monitor email communication and subsequently spoof the communication resulting in a change of bank account information pertaining to large payments. This type of incident is also known in other industries, but was first reported in the maritime sector in late 2014.

In addition to identifying actual attacks, CyberKeel made a simple investigation of the 50 largest container shipping lines who collectively control 94% of the global container vessel fleet (CyberKeel, 2014a). The investigation was simple in the sense that only two aspects were tested. One test was for potential SQL injection vulnerabilities; the other was a simple Shodan search for accessible hardware running a systems version with known exploits available. The results were that 37 out of the 50 carriers exhibited vulnerabilities.

Who Performs the Attacks

The motivations of the attackers in the maritime sector appear no different than in a number of other industry sectors. Some attacks are motivated by financial gain, though from various angles. Some, as illustrated earlier, aim at stealing money directly from the targeted companies. Others are aimed at, for example, contraband cargo. A widely publicized cyber-intrusion enabled a drug smuggling operation through the port of Antwerp (Bateman, 2013), where the terminal operation system had been penetrated, allowing smugglers to extract containers from the terminal using manipulated data.

Another type of attack is aimed at potentially infiltrating, controlling, or damaging critical infrastructure. The global shipping industry is undeniably an element of critical infrastructure to all nations, given that a disruption could have a significant impact on national economies – not to mention the ramifications of disrupting shipping services related to military operations. The report from the US Senate inquiry described earlier documented 50 intrusions into suppliers for the United States Transportation Command in a span of one year (United States Senate, 2014). In terms of shipping, the report also noted that commercial vessels handled 95% of all military dry cargoes in 2012.

Conclusion

In the context of cyber-crime related to the theft of money, the maritime industry is fundamentally no different from other industries. Criminals will use weaknesses to obtain a financial payoff, and the main victim of such attacks is the company losing the money. However, the nature of shipping also results in a situation where cyber-attacks, even those “only” aimed at a single company, can have significant ripple effects into entire national economies. As an example, a ransomware attack against a few key container terminals can

Challenges in Maritime Cyber-Resilience

Lars Jensen

cripple an entire national or regional supply chain, resulting in losses significantly out of proportion with the loss suffered by the company under attack. Or, even worse, remote tampering with on-board vessel systems – something that has been demonstrated as feasible – can result in catastrophic effects with not only economic but also significant environmental impacts.

In order to improve the situation, it is important that the maritime industry rapidly develops a set of best practice guidelines to improve the situation, while at the same time working on a longer-term plan to introduce global cybersecurity standards. National governments in many places need to increase their awareness of the critical vulnerabilities of their port infrastructure systems and provide the necessary support to allow for an improvement in cybersecurity.

The current challenge is that no practical guidelines are in place for the maritime sector, and given the global nature of the maritime industry, nationally mandated guidelines are highly likely to become conflicting and hence counterproductive as vessels move across different national jurisdictions.

Reaching a consensus on standards would require the involvement of the International Maritime Organization (IMO; www.imo.org); however, this process will likely take many years to come to fruition. In the interim, a practical approach would be the rapid establishment of voluntary global guidelines that heighten security industry-wide, and such an approach could be beneficially anchored with industry-wide best practice forums such as the Baltic and International Maritime Council (BIMCO; bimco.org). Such anchoring would allow maritime companies to pool their resources related to the necessary analysis and research, as well as attract the attention of IT companies towards dedicated maritime cybersecurity solutions. This approach would further support the adoption of voluntary guidelines.

Maritime organizations should then be encouraged to adopt these voluntary guidelines using three principal tools: i) informational campaigns directed at the maritime companies in terms of the cyber-risks they face; ii) pressure from customers who are made increasingly aware of the risk to their cargo in cases where maritime companies lack cyber-defenses; and finally iii) "cyber-premiums" on insurance policies that reflect the degree to which maritime companies adhere to the voluntary guidelines. Also, national governments could play a key role in helping identify and map out the cyber-risks faced by maritime companies within their own domain, and make such analyses readily available to maritime companies. Additionally, governments could emphasize collaboration with the IMO to fast-track the development and adoption of more binding cyber-standards in the future. Together, these steps would bring us greater cyber-resilience for the efficient functioning of the maritime industry, upon which we all depend.

About the Author

Lars Jensen is CEO and Co-Founder of CyberKeel, an international maritime cybersecurity company based in Copenhagen, Denmark. He is a recognized global expert in container shipping markets, having worked initially working for Maersk Line, where he was responsible for global intelligence and analysis as well as e-Commerce. In 2011, he founded SeaIntel Maritime Analysis, and he is currently the CEO of SeaIntel Consulting in addition to being CEO of CyberKeel. He holds a PhD in Theoretical Physics from the University of Copenhagen, and he has received strategy and leadership training from the London Business School and the Copenhagen Business School.

References

Bateman, T. 2013. Police Warning after Drug Traffickers' Cyber-Attack. *BBC News,* October 16, 2013. Accessed April 1, 2015: http://www.bbc.com/news/world-europe-24539417

Cohen, S. S. 2002. *Economic Impact of a West Coast Dock Shutdown.* Berkeley, CA: Berkeley Roundtable on the International Economy. http://www.brie.berkeley.edu/publications/ships%202002%20final.pdf

CyberKeel. 2014a. *Maritime Cyber-Risks: Virtual Pirates at Large on the Cyber Seas.* Copenhagen: CyberKeel. http://www.cyberkeel.com/images/pdf-files/Whitepaper.pdf

CyberKeel. 2014b. Shipping Companies Successfully Penetrated for Money Transfers. *Marine Cyberwatch,* October: 1. http://www.cyberkeel.com/images/pdf-files/Oct2014.pdf

ENISA. 2011. *Cyber Security Aspects in the Maritime Sector.* Heraklion, Greece: European Union Agency for Network and Information Security. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/dependencies-of-maritime-transport-to-icts/cyber-security-aspects-in-the-maritime-sector-1

Challenges in Maritime Cyber-Resilience

Lars Jensen

IMO. 2015. Frequently Asked Questions on Maritime Security. *International Maritime Organization*. Accessed April 1, 2015: http://www.imo.org/OurWork/Security/Guide_to_Maritime_Security/Pages/FAQ.aspx

Kramek, J. 2013. *The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities*. Washington, DC: Brookings Institution. http://www.brookings.edu/research/papers/2013/07/03-cyber-ports-security-kramek

Lloyds List. 2014. *One Hundred Ports*. London: Informa Publishing. http://europe.nxtbook.com/nxteu/informa/ci_top100ports2014/#/6

United States Senate. 2014. *Inquiry into Cyber Intrusions Affecting U.S. Transportation Command Contractors*. Washington, DC: United States Senate Committee on Armed Services. http://www.armed-services.senate.gov/imo/media/doc/SASC_Cyberreport_091714.pdf

Citation: Jensen, L. 2015. Challenges in Maritime Cyber-Resilience. *Technology Innovation Management Review*, 5(4): 35–39. http://timreview.ca/article/889

Keywords: maritime, cyber-resilience, cyber-risk, cybersecurity, CyberKeel, container, terminal, vessel

Q&A

Richard Wilding and Malcolm Wheatley

Q. How can I secure my digital supply chain?

A. CEOs and management teams know that digital security is important. But, simply making it an organizational priority is much easier than knowing how to assess the organization's security posture, and then taking appropriate actions to identify and mitigate against relevant risks in their supply chain. Yet, the issue cannot be ducked, with the high-profile computer hacks at businesses such as Sony Pictures and the American retailer Target highlighting just how vulnerable companies can be (Richwine, 2014; Yang & Jayakumar, 2014). In each case, hackers were able to remotely access key IT systems, and steal what they wanted. In the case of Target, that was customer credit card data and other personal details; in the case of Sony Pictures, it was – well, pretty much everything.

The trouble is, many businesses still view IT security through the lens of simple fraud-based attacks such as those at Target, where the goal has been financial gain. Too few businesses have been worried about Sony-style hacks, where the goal has been to deliberately cause damage to the business being hacked – damage caused by such things as the theft of intellectual property, reputational impact, business disruption, and – potentially – using the illicit access to cause physical harm to critical infrastructure and equipment.

Yet, undeniable though the damage at Sony Pictures seems to have been – given that hackers stole emails, financial data, and not-yet-released movies – the Sony attack might be atypical, in that the hackers were targeting its central administrative IT systems: financial systems, human resources, email, and so on (Richwine, 2014). Had Sony Pictures been a run-of-the mill manufacturing business, there would also have been an extensive set of manufacturing and supply chain management systems to attract individuals with malign intent: warehouse management systems to bring to a halt, along with the SCADA controller systems that control factory floor machinery; building management systems to disrupt; market-sensitive secrets to steal from enterprise resource planning (ERP) systems; and a rich cornucopia of product-related intellectual property held in product lifecycle management (PLM) systems.

So, how real are the dangers to a business's supply chain and supply chain management systems? And what can be done to minimise them? In the subsections that follow, we identify five areas for chief executives and directors of manufacturing and supply chains to focus on securing.

Securing enterprise resource planning and other central administrative systems

Although ordinary manufacturers typically do not have digital products to protect, they do have a lot of confidential information, such as price lists, customer lists, supplier lists, supplier pricing arrangements, internal emails, and so on (Wheatley, 2011).

So, what can a business do to minimize the danger of cyber-attacks on their supply chain? Studying what went wrong at Sony and other high-profile hacks would be a useful start. Use strong passwords, for instance – and, in particular, do not follow Sony's lead by storing them on the server, alongside the data they are meant to be protecting, in an unencrypted folder marked "password" (Curtis, 2014). Consider, too, storing ultra-sensitive data separately, away from the central enterprise resource planning system and its extensive user base, to avoid compromised access rights to transactional data leading to a more serious breach (Warren, 2014).

And, perhaps most importantly, insist on the use of a virtual private network in conjunction with two-factor authentication – especially for employees (and business partners) accessing key systems remotely (Wheatley, 2008). By requiring people who are accessing digital data to first insert a physical token (such as an encrypted USB dongle) or enter a two-factor code in order to prove that they are who their login claims they are, hackers have to acquire both a compromised login and a compromised form of two-factor identification, which is a more difficult challenge (Warren, 2014).

Securing critical operational systems on the factory floor

Subsequently attributed to American and Israeli intelligence agencies, the well-known disruption to Iran's

Q&A. How Can I Secure My Digital Supply Chain?

Richard Wilding and Malcolm Wheatley

uranium enrichment programme in 2009 was subsequently attributed to a sophisticated virus called Stuxnet, which targeted the Siemens S7-315 programmable logic controllers in use at Iran's Natanz enrichment facility, randomly changing the centrifuges' speed and damaging their rotors beyond repair (Goodwin, 2011). Buried deep underground, the facility was reckoned to be immune to potential bombing attacks– but quickly fell prey to targeted malware. Stuxnet, it is generally accepted, had taken considerable resources to develop. It has been described as "the world's first cyber super-weapon" (Goodwin, 2011).

But, the bar is getting lower: according to an incident disclosed in the 2014 annual report of the German Federal Office for Information Security (BSI) (BBC, 2014), a blast furnace at a German steel mill suffered "massive damage" after hackers used malware-loaded emails to gain access to the un-named steel mill's automated control systems. Apparently, a social engineering and phishing campaign was undertaken to gain passwords and login details for the mill's internal administration system, from which it was possible to bridge over to the blast furnace's control systems.

Clearly, the dangers are significant. A manufacturer, for instance, could effectively be brought to a standstill by disrupted warehouse management systems, supervisory control and data acquisition (SCADA) systems (as in Iran), and disrupted manufacturing execution systems – all of which are routinely seen as "part of the plumbing", and are rarely considered vulnerable to external threat. In light of the examples of recent cyber-attacks described here, this assumption now looks rather optimistic.

What can be done to prevent such attacks? Again, a large part of the battle must be to prevent access to that initially compromised system. But, recognizing that no system can be totally secure against attack, companies should "harden" their plant-floor systems by, for example, eliminating the dial-up modems and Internet access often found with such systems (used for remote diagnostics and out-of-hours management), physically disabling USB ports, and even physically disconnecting such systems from broader networks (Wheatley, 2003, 2007, 2011, 2014). In the latter case, the result will be a loss of the sort of supply-chain and in-plant work-in-progress visibility that managers often strive to deliver, but at least the in-plant systems will be more secure.

Securing building management systems

Building management is increasingly automated, with computers routinely controlling heating, lighting, and air conditioning. More worryingly, computers also control elevators, security access, intruder alarms, and CCTV cameras. Any disruption to this functionality would substantially inconvenience or even endanger a company. Heating, lighting, and air conditioning not working, elevators not working, or behaving erratically: these events are not necessarily life-threatening or business-critical, but they are definitely worth close consideration.

Yet, some of these attacks are more easily undertaken than is imagined. In 2013, for instance, two security researchers found that they could easily gain access to the building management system at Google Australia's offices in the Pyrmont section of Sydney, Australia. The system had been connected to the Internet so that specialist third-party suppliers could remotely manage the building's internal environment – but apparently without due attention being given to configuring the system securely, or applying routine patches (Zetter, 2013). In this case, the intention was not malign: the researchers were simply evaluating and highlighting the risks to businesses through insecure building management systems. And, although there is no evidence in the public domain that such attacks are taking place, the fact that they are possible means that a tangible – if not extensive – risk exists. Suppose, for example, that hackers had been able to override the security access systems that govern internal – and external – door locks. Or remotely switch off CCTV systems and cameras watching a building's physical perimeter. Under such circumstances, intruders could gain access to almost any part of a building, with impunity.

And what are businesses doing about this? Not enough, in our view. Such systems are seen as "low risk" – as were SCADA systems, prior to Stuxnet, of course.

In the meantime, it is important to stress the need to change the default logins and passwords for such systems, and carry out regular IT security audits of building management systems in the same way that the security of other business systems is regularly audited. It would also appear to be good practice to take steps to ensure that the digital "name" used on the Internet for a given building management system does not provide clues as to the building's physical location and ownership – the Google hack, for instance, was inspired by the hackers discovering that a vulnerable building management system, openly visible on the Internet, had the word "Google" within its name, prompting them to probe further (Zetter, 2013).

Q&A. How Can I Secure My Digital Supply Chain?

Richard Wilding and Malcolm Wheatley

Securing supplier portals

In late 2013, American retailer Target found out that hackers had been able to steal the personal data and credit card details of up to 110 million customers, having first used a compromised login from a supplier's system in order to then bridge across to Target's own IT systems and data centres (Feinberg, 2014; Yang & Jayakumar, 2014). The reputational damage was immense, with nervous customers worrying that future shopping trips at Target could result in them being defrauded. Both the chief executive and chief information officer lost their jobs. And, the company's embarrassment was compounded by the news that the hackers had been spotted by a sophisticated detection system that the company had installed – which had issued warnings that were ignored (Riley et al., 2014). Yet, supplier access to enterprise resource planning and other systems is very common. For over a decade, it has been reasonably routine for companies in certain industries – among them the automotive, aerospace, and consumer goods industries – to grant suppliers access rights to their enterprise applications for the purpose of downloading orders, uploading invoices, and reporting delivery status.

But, if the Target episode is prompting second thoughts about this practice, the emerging Internet of Things paradigm looks set to only reinforce those concerns. Simply put, the Internet of Things enables computer-to-device and device-to-device connectivity between trading partners. Equipment on customers' premises can "call home" when it requires consumables to be replenished or when it needs servicing. Innovative "pay per use" business models are also emerging.

So, what can be done to make such connections secure? As at Target, electronic vigilance is one answer – provided that any alarms are listened to, not switched off. But some IT experts are going further, calling for connections between trading partners to be "dumbed down", using text-based email rather than fully-digital "ERP system to ERP system" connections (Wheatley, 2014). A rules-based parser at the recipient business then takes the arriving text and encodes it. This approach lacks efficiency, but it is preferable to being hacked and would seem prudent should a risk assessment suggest a material risk.

Securing the systems containing product-related intellectual property

A 2011 report undertaken by IT consultants Detica – a subsidiary of defence contractor BAE Systems – in conjunction with the United Kingdom government's Office of Cyber Security and Information Assurance in the Cabinet Office, put the cost of "cybercrime" to the UK economy at £27 billion a year. Of that £27 billion ($50 billion CAD), just over a third – £9.2 billion ($17.2 billion CAD)– was made up of intellectual property losses by UK businesses, with hi-tech manufacturers ranging from aerospace to electronics and pharmaceutical manufacturers deemed to be most at risk (Detica, 2011).

Consequently, the UK Ministry of Defence launched a cybersecurity initiative in February 2013, specifically seeking to guard against the loss of military technology – not from its prime contractors, but from its prime contractors' *suppliers* (Wheatley, 2013). Begun in the wake of IT security breaches at the American aerospace manufacturer Lockheed Martin, the message was uncompromising: the threat of industrial espionage – and state-sponsored industrial espionage – is very real. And, in today's interconnected world, the security of suppliers' systems is just as important as that of the manufacturers' own systems. Not that the security of manufacturers' own systems can be taken for granted: in 2014, the United States Department of Justice charged five Chinese army officers with stealing trade secrets and internal documents from five companies, including Westinghouse Electric, US Steel, Alcoa, and Allegheny Technologies (Segal, 2014).

But, what exactly can businesses do to protect themselves, particularly in a world where ever-shorter product lifecycles and R&D programmes are pushing businesses to both digitize their product data within product lifecycle management (PLM) systems, and then link those PLM system to their ERP systems?

Again, two-factor authentication can help, by requiring people accessing digital data to first insert a physical token or two-factor code in order to prove who they are. Secure digital data distribution is another option: through its "Policy Rights Server" and "LiveCycle Rights Management" technologies, Adobe, for instance, offers encrypted Adobe Acrobat PDF documents deliberately intended for secure document distribution in supply chains, which cannot be opened by unauthorized third parties, and which 'time expire' after a given interval. (Adobe, 2015)

Businesses should also consider rigorous audits of their suppliers' IT security policies and practices, and giving greater weight to IT security within the overall supplier assessment framework. Are purchasers buying from the cheapest supplier, or the most secure? While ideally a business will want both, there will be times when a choice has to be made.

Q&A. How Can I Secure My Digital Supply Chain?

Richard Wilding and Malcolm Wheatley

About the Authors

Richard Wilding OBE is a Full Professor and Chair of Supply Chain Strategy at Cranfield School of Management, England. A European and Chartered Engineer, he is a chartered fellow of the Institute of Engineering and Technology (Manufacturing Division) (FIET), the Chartered Institute of Logistics & Transport (FCILT) and the Chartered Institute of Purchasing & Supply (FCIPS). He has published widely in the area of Supply Chain Management and is an editorial advisor to a number of major journals in this area. In recognition of his outstanding achievements in the area of logistics and supply chain management, he was appointed an Officer of the Most Excellent Order of the British Empire (OBE) by Queen Elizabeth II in the 2013 New Year Honours, for services to business.

Malcolm Wheatley PhD is a visiting fellow at Cranfield School of Management, England. A former management consultant with Price Waterhouse and Deloitte, Haskins & Sells, he has written extensively on manufacturing and supply chain management IT, security and strategy matters. His supply chain security-specific work has appeared in publications such as *CIO Magazine*, *CSO Magazine*, *The Manufacturer,* and *Procurement Leaders.*

References

Adobe. 2015. Securing Documents with Adobe LiveCycle Rights Management ES. *Adobe.com.* Accessed March 1, 2015: http://help.adobe.com/en_US/acrobat/X/pro/using/WS58a04a822e3e50102bd615109794195ff-7d65.w.html

BBC. 2014. Hack Attack Causes 'Massive Damage" at Steel Works. 2014. *BBC,* December 22, 2014. Accessed March 1, 2015: http://www.bbc.com/news/technology-30575104

Curtis, S. 2014. Sony Saved Thousands of Passwords in a Folder Named 'Password'. *The Telegraph,* December 5, 2014. Accessed March 1, 2015: http://www.telegraph.co.uk/technology/sony/11274727/Sony-saved-thousands-of-passwords-in-a-folder-named-Password.html

Detica. 2011. *The Cost of Cyber Crime: A Detica Report in Partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office.* Surrey, UK: Detica Ltd. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf

Feinberg, A. 2014. Last Month's Massive Target Hack Was the Heating Guy's Fault. *Gizmodo,* February 5, 2014. Accessed March 1, 2015: http://gizmodo.com/last-months-massive-target-hack-was-the-heating-guys-1516926877

Goodwin, C. 2011. The Worm That Threatens the World. *The Sunday Times,* December 4, 2011. Accessed March 1, 2015: http://www.thesundaytimes.co.uk/sto/Magazine/Features/article829818.ece

Richwine, L. 2014. Cyber Attack Could Cost Sony Studio as Much as $100 million. *Reuters,* December 9, 2014. Accessed March 1, 2015: http://www.reuters.com/article/2014/12/09/us-sony-cybersecurity-costs-idUSKBN0JN2L020141209

Riley, M., Elgin, B., Lawrence, D., & Matlack, C. 2014. Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It. *Bloomberg Business Week,* March 13, 2014. Accessed March 1, 2015: http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data

Segal, A. 2014. Department Of Justice Indicts Chinese Hackers: What Next? *Forbes,* May 19, 2014. Accessed March 1, 2015: http://www.forbes.com/sites/adamsegal/2014/05/19/department-of-justice-indicts-chinese-hackers-what-next/

Warren, C. 2014. Four Security Takeaways from the Epic Sony Hack. *Mashable,* December 3, 2014. Accessed March 1, 2015: http://mashable.com/2014/12/03/sony-hack-4-security-lessons/

Wheatley, M. 2003. Rogue Modems: Your Network's Back Door. *CSO,* September 1, 2003. Accessed March 1, 2015: http://www.csoonline.com/article/2116678/

Wheatley, M. 2007. Harrying the Hackers. *The Manufacturer,* May 2007.

Wheatley, M. 2008. Wireless VPNs: Protecting the Wireless Wanderer. *CSO,* December 15, 2008. Accessed March 1, 2015: http://www.csoonline.com/article/2123488/

Wheatley, M. 2011. Hacked Off. *The Manufacturer,* November 25, 2011. Accessed March 1, 2015: http://www.themanufacturer.com/articles/hacked-off/

Wheatley, M. 2013. Hidden Depths. *Procurement Leaders,* July/August 2013: 26–29.

Wheatley, M. 2014. Only Connect. *The Manufacturer,* November 2014.

Yang, J. L., & Jayakumar, A. 2014. Target Says up to 70 Million More Customers Were Hit by December Data. *Washington Post,* January 10, 2014. Accessed March 1, 2015: http://www.washingtonpost.com/business/economy/2014/01/10/0ada1026-79fe-11e3-8963-b4b654bcc9b2_story.html

Zetter, K. 2013. Researchers Hack Building Control System at Google Australia Office. *Wired,* May 6, 2013. Accessed March 1, 2015: http://www.wired.com/2013/05/googles-control-system-hacked/

Citation: Wilding, R., & Wheatley, M. 2015. Q&A. How Can I Secure My Digital Supply Chain? *Technology Innovation Management Review,* 5(4): 40–43. http://timreview.ca/article/890

Keywords: supply chain risk, IT security management, cyber-crime, intellectual property protection, cybersecurity, supply chain security

Author Guidelines

These guidelines should assist in the process of translating your expertise into a focused article that adds to the knowledge resources available through the *Technology Innovation Management Review*. Prior to writing an article, we recommend that you contact the Editor to discuss your article topic, the author guidelines, upcoming editorial themes, and the submission process: timreview.ca/contact

Topic

Start by asking yourself:

- Does my research or experience provide any new insights or perspectives?
- Do I often find myself having to explain this topic when I meet people as they are unaware of its relevance?
- Do I believe that I could have saved myself time, money, and frustration if someone had explained to me the issues surrounding this topic?
- Am I constantly correcting misconceptions regarding this topic?
- Am I considered to be an expert in this field? For example, do I present my research or experience at conferences?

If your answer is "yes" to any of these questions, your topic is likely of interest to readers of the TIM Review.

When writing your article, keep the following points in mind:

- Emphasize the practical application of your insights or research.
- Thoroughly examine the topic; don't leave the reader wishing for more.
- Know your central theme and stick to it.
- Demonstrate your depth of understanding for the topic, and that you have considered its benefits, possible outcomes, and applicability.
- Write in a formal, analytical style. Third-person voice is recommended; first-person voice may also be acceptable depending on the perspective of your article.

Format

1. Use an article template: .doc .odt
2. Indicate if your submission has been previously published elsewhere. This is to ensure that we don't infringe upon another publisher's copyright policy.
3. Do not send articles shorter than 1500 words or longer than 3000 words.
4. Begin with a thought-provoking quotation that matches the spirit of the article. Research the source of your quotation in order to provide proper attribution.
5. Include a 2-3 paragraph abstract that provides the key messages you will be presenting in the article.
6. Provide a 2-3 paragraph conclusion that summarizes the article's main points and leaves the reader with the most important messages.
7. Include a 75-150 word biography.
8. List the references at the end of the article.
9. If there are any texts that would be of particular interest to readers, include their full title and URL in a "Recommended Reading" section.
10. Include 5 keywords for the article's metadata to assist search engines in finding your article.
11. Include any figures at the appropriate locations in the article, but also send separate graphic files at maximum resolution available for each figure.

Issue Sponsor