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 organizations 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-

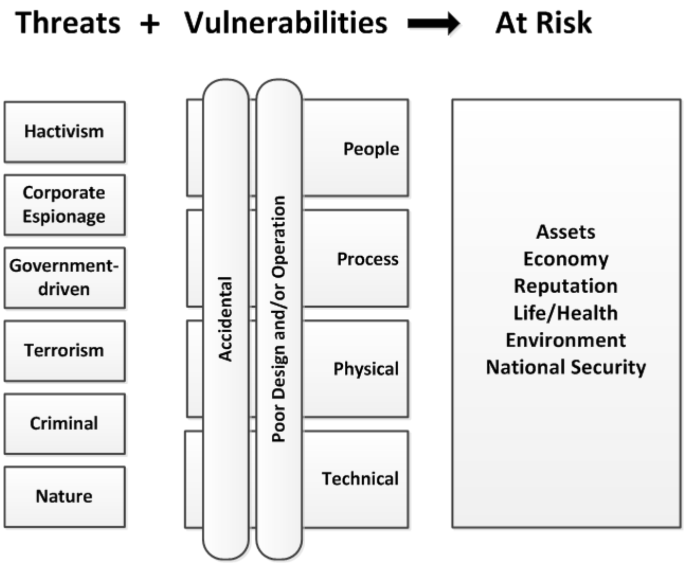

Figure 1. Threats and vulnerabilities that affect cyber-resilience

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

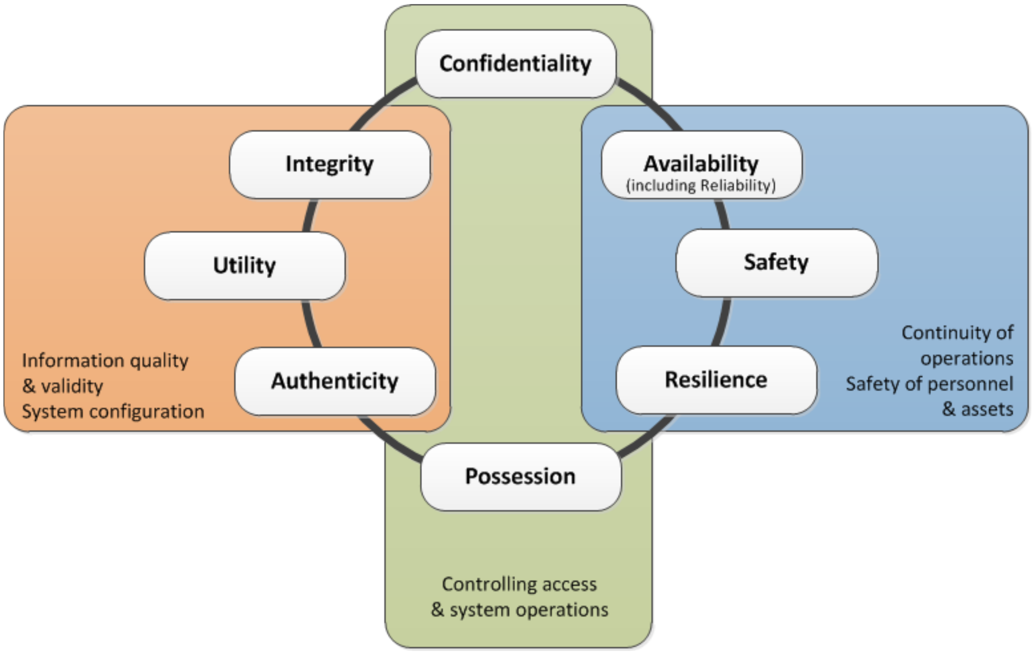

Figure 2. Cybersecurity attributes that affect cyber-resilience

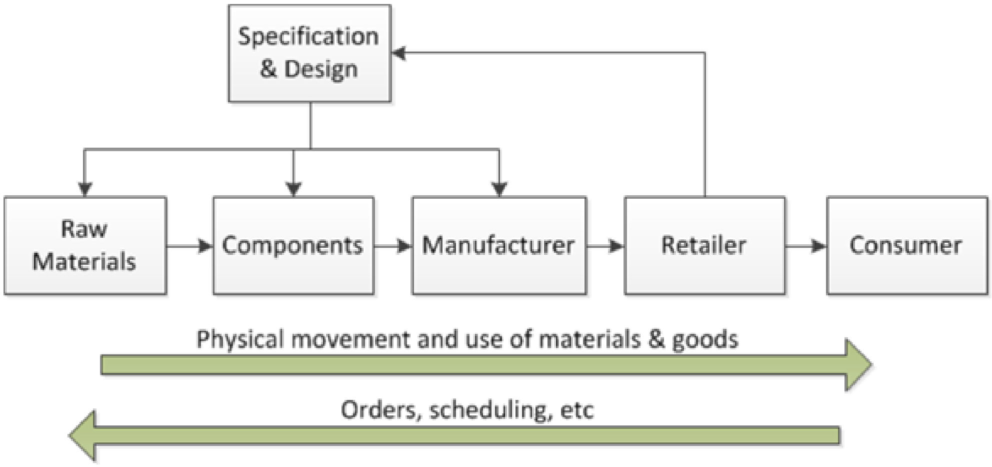

Figure 3. Generic supply chain for physical products or assets

- 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. Managing 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.

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