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.

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

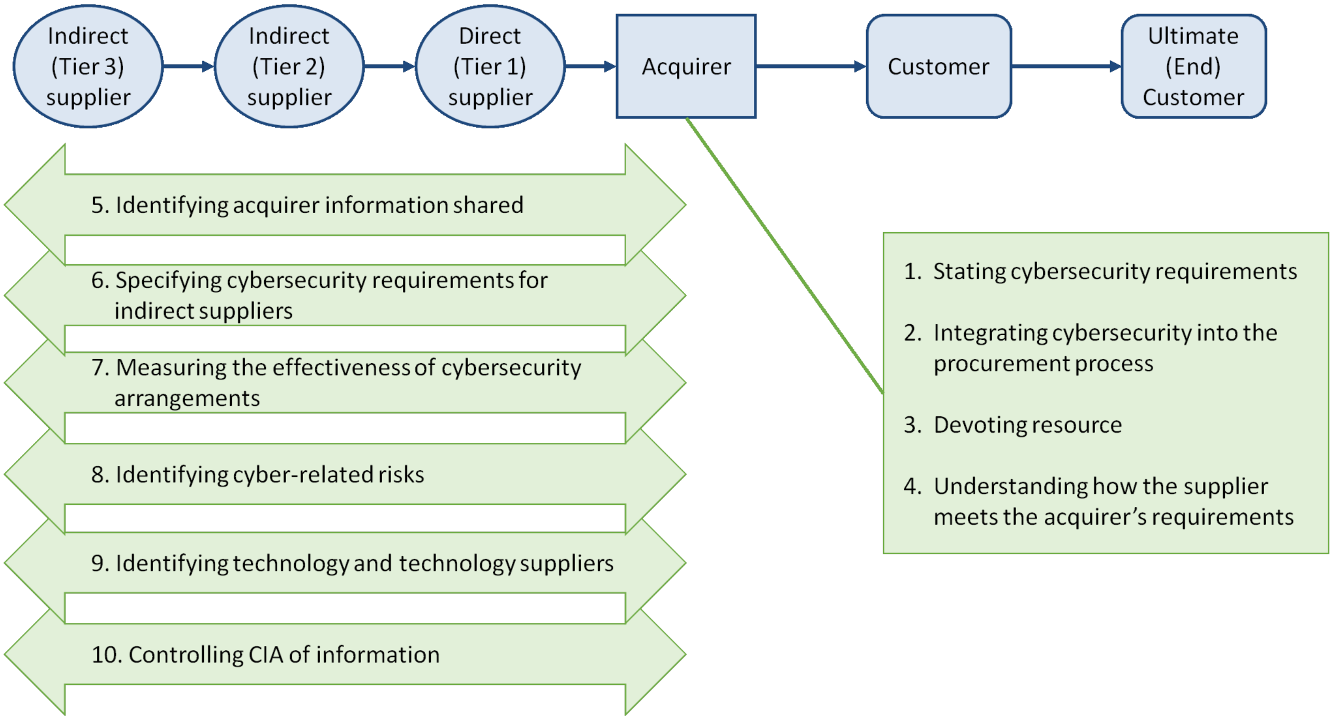
Indirect (Tier 3) supplier
Indirect (Tier 2) supplier
Direct (Tier 1) supplier
Acquirer
Customer
Ultimate (End) Customer
5. Identifying acquirer information shared
6. Specifying cybersecurity requirements for indirect suppliers
7. Measuring the effectiveness of cybersecurity arrangements
8. Identifying cyber-related risks
9. Identifying technology and technology suppliers
10. Controlling CIA of information
1. Stating cybersecurity requirements
2. Integrating cybersecurity into the procurement process
3. Devoting resource
4. Understanding how the supplier meets the acquirer's requirements

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

- 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

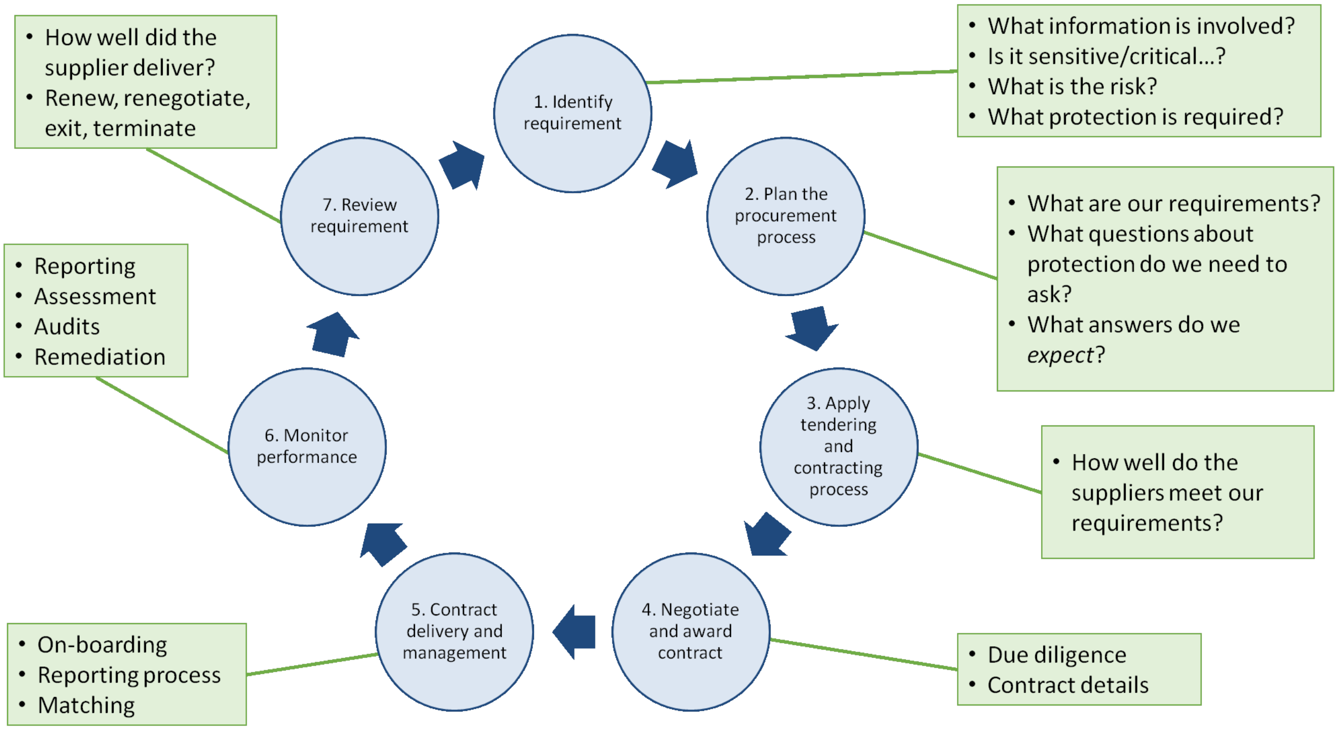
1. Identify requirement
• What information is involved?
• Is it sensitive/critical...?
• What is the risk?
• What protection is required?
2. Plan the procurement process
• What are our requirements?
• What questions about protection do we need to ask?
• What answers do we *expect*?
3. Apply tendering and contracting process
• How well do the suppliers meet our requirements?
4. Negotiate and award contract
• Due diligence
• Contract details
5. Contract delivery and management
• On-boarding
• Reporting process
• Matching
6. Monitor performance
• Reporting
• Assessment
• Audits
• Remediation
7. Review requirement
• How well did the supplier deliver?
• Renew, renegotiate, exit, terminate

Figure 2. Integrating information into a typical procurement cycle

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

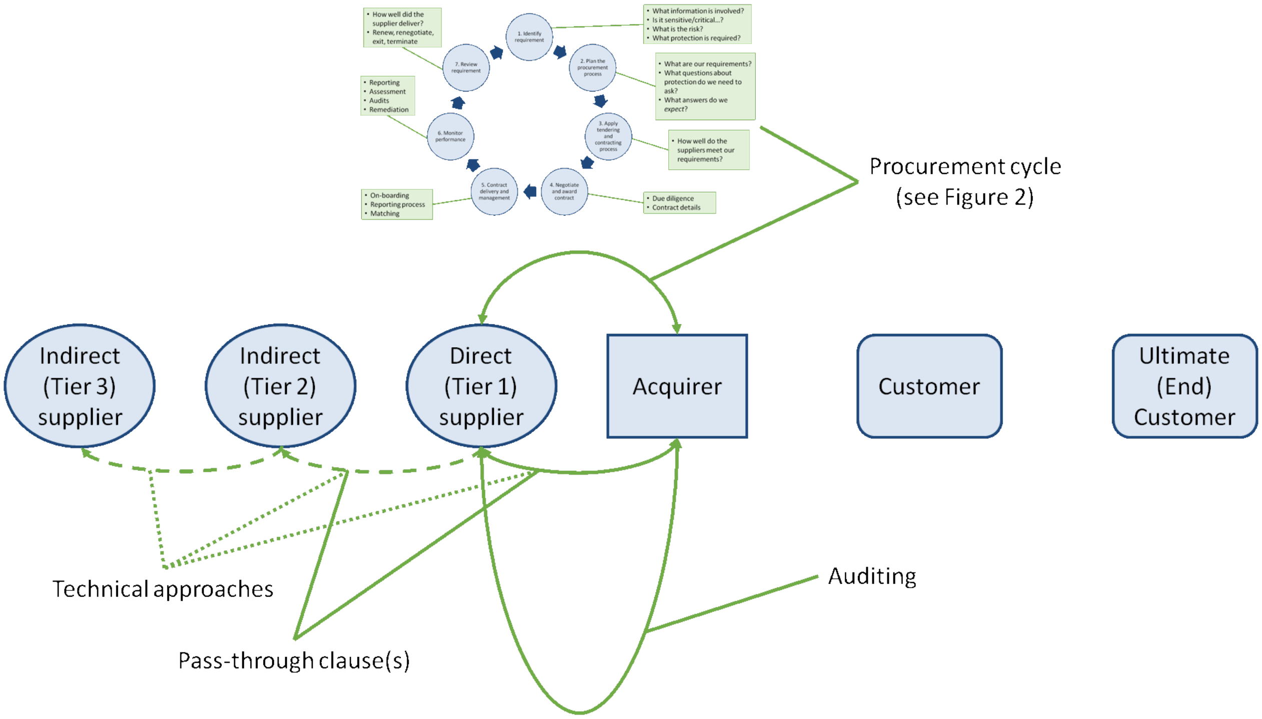
1. Identify requirement
2. Plan the procurement process
3. Apply tendering and contracting process
4. Negotiate and award contract
5. Contract delivery and management
6. Monitor performance
7. Review requirement
• What information is involved?
• Is it sensitive/critical…?
• What is the risk?
• What protection is required?
• What are our requirements?
• What questions about protection do we need to ask?
• What answers do we *expect*?
• How well do the suppliers meet our requirements?
• Due diligence
• Contract details
• On-boarding
• Reporting process
• Matching
• Reporting
• Assessment
• Audits
• Remediation
• How well did the supplier deliver?
• Renew, renegotiate, exit, terminate
Procurement cycle (see Figure 2)
Indirect (Tier 3) supplier
Indirect (Tier 2) supplier
Direct (Tier 1) supplier
Acquirer
Customer
Ultimate (End) Customer
Technical approaches
Pass-through clause(s)
Auditing

Figure 3. Approaches to protecting information in the supply chain

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.

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

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 cyberworld 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.

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