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