SYM-AM-16-041

PROCEEDINGS
OF THE
THIRTEENTH ANNUAL ACQUISITION RESEARCH SYMPOSIUM

WEDNESDAY SESSIONS
VOLUME I

The Cybersecurity Challenge in Acquisition

Sonia Kaestner, Adjunct Professor, McDonough School of Business, Georgetown University
Craig Arndt, Professor, Defense Acquisition University
Robin Dillon-Merrill, Professor, Georgetown University

Published April 30, 2016

Prepared for the Naval Postgraduate School, Monterey, CA 93943.

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF BUSINESS & PUBLIC POLICY
NAVAL POSTGRADUATE SCHOOL

The research presented in this report was supported by the Acquisition Research Program of the Graduate School of Business & Public Policy at the Naval Postgraduate School.

To request defense acquisition research, to become a research sponsor, or to print additional copies of reports, please contact any of the staff listed on the Acquisition Research Program website (www.acquisitionresearch.net).

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF BUSINESS & PUBLIC POLICY
NAVAL POSTGRADUATE SCHOOL

Panel 9. The Operational and Developmental Dimensions of Cybersecurity

Wednesday, May 4, 2016	
3:30 p.m. – 5:00 p.m.	**Chair: Rear Admiral David H. Lewis, USN,** Commander, Space and Naval Warfare Systems Command ***The Cybersecurity Challenge in Acquisition*** Sonia Kaestner, Adjunct Professor, McDonough School of Business, Georgetown University Craig Arndt, Professor, Defense Acquisition University Robin Dillon-Merrill, Professor, Georgetown University ***Improving Security in Software Acquisition and Runtime Integration With Data Retention Specifications*** Daniel Smullen, Research Assistant, Carnegie Mellon University Travis Breaux, Assistant Professor, Carnegie Mellon University ***Cybersecurity Figure of Merit*** CAPT Brian Erickson, USN, SPAWAR

Sonia Kaestner—is an Adjunct Professor at the McDonough School of Business at Georgetown University. She has recently conducted a Strategy and Portfolio Management research study for the Defense Acquisition University and developed the course material, exercises, and instructor support material for a new course offering at DAU on this topic. In addition, she has extensive consulting experience in the benchmarking and risk analysis of capital projects, quantitative and qualitative analysis, and training and development management.

Craig Arndt—is the Department Chair for Engineering and Technology and a Professor of Systems Engineering at the Defense Acquisition University. Dr. Arndt studies the development of new methods for the development of taxonomies of learning environments. This research effort is developing methods that will allow future educational designers to select and develop new learning environments based on the nature of the curriculum and the requirements and demographics of the student population. He holds a PhD in electrical engineering**.**

Robin L. Dillon-Merrill—is a Professor in the McDonough School of Business at Georgetown University. She seeks to understand and explain how and why people make the decisions that they do under conditions of uncertainty and risk. She is currently in year two of a multi-year funded research project with the Department of Homeland Security titled *Beyond Technical Solutions to Cybersecurity Risk Management and Risk Communication: Utilizing Tools and Research from Behavioral, Economic, and Policy Research.*

Abstract

To improve cybersecurity, the acquisition community must understand and manage multiple dimensions of cyber-attacks both as an opportunity and as a risk that can compromise the bottom line of the organizations they work for and with. In particular, the acquisition community must understand and recognize the cyber threats inherent in procuring complex modern systems with significant cyber components. If cybersecurity is not designated as a requirement of a modern system, it is often challenging to add effective security on later, and the severity of the cyber vulnerabilities may only be identified after a breach has already occurred. If appropriate cybersecurity is designed and built-in, these systems will have higher up-front costs but potentially lower life-cycle costs because of the reduced need to fix vulnerabilities in the systems later. Additionally, individuals working in acquisition need to recognize that given the sensitive nature of their work, including intellectual property and financial data, their IT processes, information, and systems will be an attractive target for cyber threats from both criminal sources (e.g., organized crime) and nation state adversaries, and the complexity and integration of the modern supply chain will add vulnerabilities to these linked supplier systems.

Introduction

Cyber Threat Challenges

The accelerated growth in cyber/digital technology development has changed the way we direct our lives, business, and countries. This same technology development has driven the rise in cybersecurity breaches through the increased complexity of IT systems, the increased use of personal and mobile devices, and the explosion of social media. In addition, as users, we have not had the same speed to grow the skills and capabilities required to safely absorb the technologies we now depend on. So far, there are no cybersecurity risk management readiness standards, and organizations' employees (at all levels) lack the cybersecurity training required to prevent and/or promote a cyber-attack. The lack of leadership's understanding of potential vulnerabilities and liabilities leads organizations to address these risks mainly from a technical perspective, and hence, rely

mainly on IT professionals to solve the problem. This common approach ignores the vulnerabilities that an untrained workforce represents.

According to the UK Information Commissioner's Office, 93% of cybersecurity incidents are caused by human error (errors even when designing cybersecurity processes and systems); thus this workforce (untrained and sometimes even trained) is the weakest link in the cybersecurity chain. The remaining 7% was due to technical failures.

The consequences of cyber-attacks are diverse and include the suspension of system operations, the loss of current and future revenue, the loss of intellectual property, reputation harm, decreased customer confidence, leaks of sensitive information, and legal liability, among others. These consequences are often exacerbated because attacks are not always detected immediately. Verizon (2013) estimates that 62% of data breaches were not detected for at least several months if not longer.

The Identity Theft Resource Center (ITRC; 2016) found that in 2015, the Health/Medical, Banking/Credit/Financial, Government/Military and the Education sectors were the most affected by cybercrime, but these data may be underestimating the scale of the cybercrime, as often firms (predominantly small- and medium-size business) do not disclose cyber-attacks to attempt to avoid the financial costs, liability, and loss of goodwill that come with disclosure and notification (Supply Chain Quarterly, 2015).

Some progress is being made in increasing the recognition of cybersecurity problems. As of 2015, a survey conducted by PricewaterhouseCoopers (PwC) described that over two-thirds of organizations were more concerned about cyber threats (PwC, 2015) than in previous years' studies. Also, the U.S. Department of Homeland Security (DHS) has included cybersecurity as a top priority for 2016, and $587.5 million have been allocated to fund programs to enhance cybersecurity situational awareness and information sharing (National Cybersecurity Protection System and Continuous Diagnostics and Mitigation; DHS, 2016). Despite all the media coverage, government guidance, and the increasing awareness, cybersecurity risk management continues to not been widely implemented or standardized among all target levels: Individuals, Organizations and Critical Infrastructure. This paper will begin to address some of the training and education needed to improve cybersecurity risk management, particularly in acquisition.

Target Levels: Individuals

As shown in Figure 1, individuals face the risk of losing data and privacy, having their devices hacked for a ransom (denial of service—DoS), or simply damaged. In the first week of March 2016, Mac users were targeted by hackers with "ransomware" in what is believed to be the first complete attack campaign of its kind against users of Apple's operating system. Also, several incidents have been reported where internet-enabled baby monitors have been hacked to disturb infants. This last example depicts the increasing risks associated with the Internet of Things (IoT), the expanding network of billions of everyday objects/devices with network connectivity and data-sharing capabilities that are part of our daily lives. This inappropriate use of these everyday devices was certainly not considered when they were designed. How individuals use pieces of an acquired system and where individual personal devices plug into an acquired system will be a challenge for the acquisition professional to understand and consider.

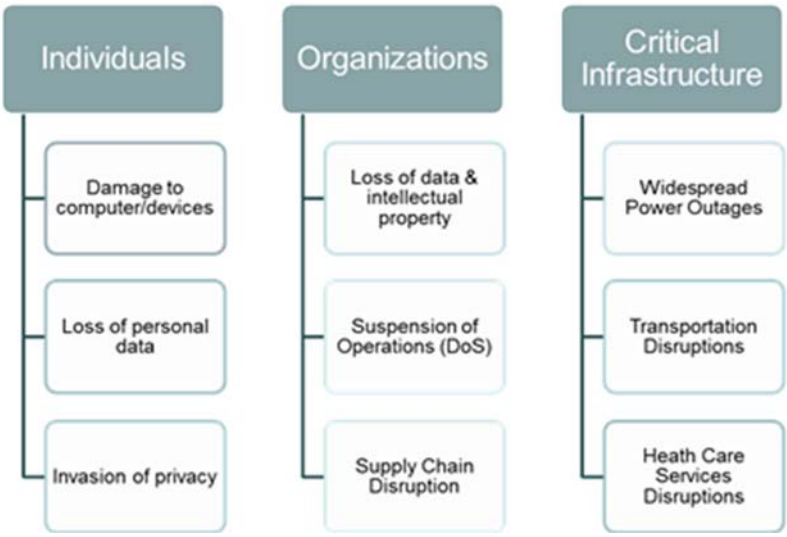

Figure 1. Target Levels for Cyber-Attacks

Target Levels: Organizations

Organizations face the same risks as individuals, but to a larger and more complex extent, as they own customer and proprietary data that represent the core of their business. In addition, they also face legal liability from their customers, reputation damage, and higher exposure to the IoT through their employers, suppliers, and customers. In a recent example (February 2016), the Hollywood Presbyterian Medical Center was victim of a DoS attack that locked employees out of their systems by encrypting files for which only the hackers had the decryption key. The communications between physicians and medical staff were paralyzed, and they suddenly had to rely on paper records to keep operations running. The hospital chose to pay hackers a ransom of $17,000 in bitcoins to regain control of their computer systems after the cyber-attack. The origin of the computer network intrusion remains unknown at this time. The ever increasing sophistication of the cyber-attacks makes the job of the acquisition workforce ever more challenging. Following the Hollywood Presbyterian Medical Center "ransomware" attack, this is now a new concern for those responsible for the acquisition of medical record systems. Since the cyber threats keep changing and evolving, how is a manager trained in acquisition supposed to keep track?

Target Levels: Critical Infrastructure

Critical Infrastructure organizations face all previously mentioned risks, but with bigger consequences, such as the suspension/restriction of normal operations of whole communities. The Ukrainian power grid cyber-attack in 2015, for example, caused a blackout for hundreds of thousands of people in Ukraine. The attack used destructive malware that wrecked computers and wiped out sensitive control systems for parts of the Ukrainian power grid. A team of hackers coordinated attacks at the same time against six power providers. The attack was so severe that it knocked out internal systems intended to help the power companies restore power. Computers were destroyed, and even the call centers used to report outages were knocked out. The source of the attack is still under investigation (but many suspect it originated in Russia). Since the risks associated with critical infrastructure are so great, it is imperative for acquisition specialists in these environments to understand the relevant and evolving threats to their computer systems.

External Attackers Versus Insiders in the Supply Chain

Most frequently, cybersecurity is perceived as a risk from the outside (i.e., hackers/criminals) getting illicit access to the organization's data/assets with ill purposes. However, organizations are not adequately addressing the internal type of cyber risk that includes employees and third-parties which have access to critical assets. Among organizations with cybersecurity risk mitigation plans, 48% have not considered third-party vendors, 43% have not examined the role of contractors, 58% have not examined the role of suppliers, and 92% have not assessed the supply chain risk management as a whole (PwC, 2014, 2015).

External types of cyber-attacks against prominent organizations such as JPMorgan Chase and the U.S. Central Command get plenty of attention. Cyber-attacks involving internal resources (i.e., business partners and direct employees) do not get the same coverage despite the fact that they pose more malicious threats. Internal resources have much easier access to systems and a much greater window of opportunity.

The Target and Home Depot attacks provide good examples where third-party contractors unintentionally facilitated the breach. The Target breach was traced back to stolen network credentials from a third party vendor (a refrigeration, heating and air conditioning subcontractor). Home Depot reported that criminals used a third-party vendor's user name and password to enter the perimeter of their network and then acquired elevated rights that allowed them to navigate portions of Home Depot's network and to deploy unique, custom-built malware on its self-checkout systems in the United States and Canada.

Additionally, at a general level, ill-trained direct employees also pose significant insider cybersecurity risks. Their inability to identify cyber threats leads them to unintentionally click on phishing email links, download malware, access sensitive data from mobile or personal devices, etc. At a more specific level, professionals who are in charge of designing and acquiring products and systems do not have the cybersecurity knowledge to identify potential risks in the programs they are designing, managing, or acquiring. Cyber risks are then left in systems during the requirements, design, and contracting of the systems development, too often only to be discovered later during operations after an attack.

It is widely known that there is a significant shortage of cybersecurity professionals. On average it takes three months to hire a cybersecurity professional, as only 25% of the applicants meet the requirements for the position, but over 70% of these finally hired professionals lack the ability to understand the organization's business (CSX, 2015). There are plenty of efforts made and resources allocated to close the cybersecurity talent gap. However, the focus of these concerns is related to cyber professionals with a technical background to create the protection walls around the organization's assets, and to create the systems to detect and respond to threats. This type of professional is in low supply because organizations (of all sizes) decided in the early 2000s to send "low-level" IT work, such as network and systems administrators, offshore to reduce costs. These same organizations missed the opportunity to grow and groom those professionals that they need now. The solution for this type of shortage is going to require the collaboration of universities (to create cyber-specific careers or add cybersecurity training to complement other fields), marketing campaigns (increase the awareness of a cyber career as an attractive option), private and government incentives (e.g., scholarships), and so forth.

The other, and mostly ignored, cybersecurity talent gap is related to the employees at the different levels of the organization. This is a more specific talent gap that requires a customized type of training that accounts for the roles each employee plays and the type of

data he/she has. Certain functions need to have an extensive cybersecurity knowledge comparable to the IT professional to complement their non-IT role. For example, engineers who are designing the next product need to have extensive cybersecurity knowledge to close potential cybersecurity gaps in their designs to prevent a future cyber breach.

The Car Manufacturing Case

As can be seen in most areas of technology, computers have become common components, and this is especially true in the cars we drive. The use of computers embedded into systems does not in itself create cybersecurity vulnerabilities. However, adding computer-based capabilities to existing systems creates the opportunities for a wide range of cyber risks and threats.

The hackers are publicizing their work to reveal vulnerabilities present in a growing number of car computers. All cars and trucks contain anywhere from 20 to 70 computers. They control everything from the brakes to acceleration to the windows and are connected to an internal network. A few hackers have recently managed to find their way into these intricate networks.

In one case, a pair of hackers manipulated two cars by plugging a laptop into a port beneath the dashboard where mechanics connect their computers to search for problems. Scarier yet, another group took control of a car's computers through a cellular telephone and Bluetooth connections and could access systems including, for example, the tire pressure monitoring system.

"The more technology they add to the vehicle, the more opportunities there are for that to be abused for nefarious purposes," says Rich Mogull, CEO of Phoenix-based Securosis, a security research firm. "Anything with a computer chip in it is vulnerable, history keeps showing us."

Two years ago, researchers at the University of Washington and University of California, San Diego did more extensive work, hacking their way into a 2009 midsize car through its cellular, Bluetooth, and other wireless connections. Stefan Savage, a UCSD computer science professor, said he and other researchers could control nearly everything but the car's steering. "We could have turned the brakes off. We could have killed the engine. We could have engaged the brakes," he said. Savage wouldn't identify which manufacturer made the car they hacked into. But two people with knowledge of the work said the car was from General Motors and the researchers compromised the OnStar safety system, best known for using cellular technology to check on customers and call for help in a crash. The people didn't want to be identified because they were not authorized to speak publicly on the matter ("Hackers Find Weaknesses," 2013).

When we look at the underlying causes of the current generation of hacking attacks on the auto industry, we look at the basics of the mechanisms of cybersecurity. First is the threat; given the current state of interest in the hacker community and the ubiquitous nature of cars in the United States there will be a continuing and rapidly evolving level of threat against cars now that there is an understanding that accessing their networks is possible.

Next are the vulnerabilities. There are a number of different vulnerabilities that could be exploited in any of the new car designs as has been noted above. As we look for lessons learned to build better systems we look at where and when the vulnerabilities are introduced. The different vulnerabilities fall into three principle categories: design vulnerabilities, interface vulnerabilities, and supply chain vulnerabilities. In our case, all of their vulnerabilities were introduced by the people in the car companies who designed the

car and did not anticipate how cyber threats could work because that was not their job to understand the technical details of cyber intrusion.

Acquisition professionals need to have the technical and cybersecurity skills to identify potential gaps in the products and systems they are acquiring. This type of cybersecurity talent gap needs to be addressed through the implantations of training programs customized to close the specific talent gaps in critical functions of the organization.

Cybersecurity does not always have the strategic priority it should. According to a Ponemon Institute (2015) study, as of 2015, only 34% of companies consider cybersecurity to be a strategic priority, and thus, it is unlikely that enough resources are allocated to support something that is not seen as a priority. Acquisition organizations have to assess their acquisition strategies to include cyber security and need to focus mitigation efforts to include all parties involved in the organization's supply chain.

Acquiring Cyber Secure Systems

Understanding and recognizing the cyber threats inherent in procuring complex modern systems with significant cyber components is a challenge. For example, as was mentioned in the car manufacturing example, in 2011, the vulnerability of telematic systems like GM's OnStar was demonstrated to not require hacking but just identification of each equipped car's OnStar telephone number. That flaw was later fixed, but highlights the challenges of understanding the vulnerabilities of new, complex modern networked systems. As described by Greenberg (2015), from the time the problem was first identified until it was fixed was more than five years. Greenberg (2015) goes on to explain, "Automakers five years ago simply weren't equipped to fix hackable bugs in their vehicles' software … and many of those companies may not be much better prepared today."

Training the acquisition workforce to understand the complex cyber challenges of their systems at the right level of detail is the only viable solution to this problem in the long run.

Securing Supply Chains

Technology development has significantly changed the way organization conduct their business:

> The flexibility, scalability, and efficiency of the technology that enables information sharing among partners, has created additional points of access to an organization's proprietary information, increasing the risks that the corporate knowledge that drives profitability may fall into the wrong hands. (Supply Chain Quarterly, 2015)

Any vendor with company credential access can expose the internal network to an attack.

As shown in Figure 2, the acquisition challenge is based on the complexity of the supply chain that most organizations have, which in many cases includes both upstream (i.e., suppliers) and downstream (i.e., market) components and the global environment. More and more, organizations are required to share information with suppliers, contractors, third-party vendors (and their vendors—fourth-party partners), that do not have the same approach to cybersecurity. Cybersecurity vulnerabilities in their supply chains will in turn introduce new vulnerabilities in the organization and must be managed by those acquisition specialists focused most on the supply chain relationships.

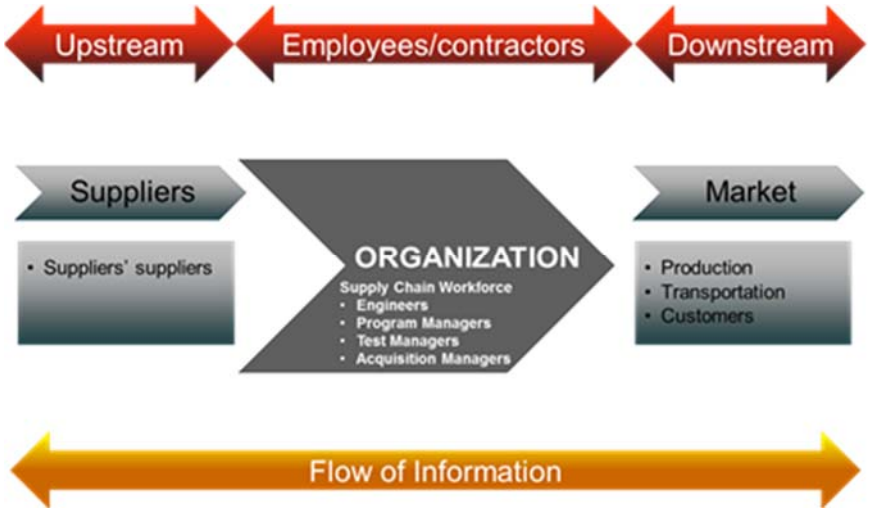

Figure 2. Supply Chain Complexity

In addition, the supply chain not only is the mechanism that develops and delivers products and services from source to customer, but also represents critical parts of the value chain system (inbound logistics, operations, and outbound logistics) in which interdependence is the fundamental tenet behind gaining a competitive advantage (Porter, 1985). Organizations share proprietary data across their value chain (e.g., marketing, dales, pricing, metrics, point-of-sale information, inventory flows, enterprise system activities, etc.), increasing the number of potential cyber breach entry points.

From an organization's strategic point of view, consolidating the supply chain is critical to reduce costs and develop integrated profit centers. The efficiency of the global supply chain is highly dependent on the speed data is transferred among supply change partners. How to do this without introducing more cybersecurity risks is the challenge organizations have now to address.

Vertically integrated organization (upstream and downstream operations) will carry a higher risk profile than a horizontally integrated organization. For example, in the Volkswagen (VW) emissions case, the organization (OEM[1]) was able to install deceiving software to cheat on the emissions testing for its diesel cars. The cars' computers were able to alter how their engines worked to reduce emissions (to meet required levels of pollutants) while they were being tested. Customers became aware of this practice (when the cars have left the supply chain) after six years of "successful" implementations of the software. Although in this case, VW was fully responsible for the implementation of this software. Using the same approach, cyber criminals could use the same strategy to benefit from the potential damage to an organization.

Many breaches seen so far have been because of a lack of standardized credentialing processes and a lack of technology updates and patches. As organizations share their information with their business partners (through the internet, mobile devices,

[1] Original Equipment Manufacturer

cloud computing, etc.), their cybersecurity vulnerability increases, opening new doors for hackers (*Wall Street Journal* [WSJ], 2014).

Third- and fourth-party supplier's technology use also represents a challenge as organizations do not have control over the type of technology and technology upgrades those parties rely on. In 2015, over 40% of large and medium size organizations in the United States and UK were still using Windows XP, which is no longer supported by Microsoft, and, hence, no up-to-date security upgrades are available (Prince, 2015). According to Microsoft, Windows XP users are five times more vulnerable to security risks and viruses than organizations using up-to-date operating systems. Based on these statistics, most likely many suppliers are still using Windows XP.

The most frequent supply chain attacks are related to malware,[2] compromised credentials,[3] distributed denial of services (DDoS),[4] and SQL injections.[5] Supply chain partner relations bring an additional cybersecurity potential entry point (Supply Chain Quarterly, 2015):

- Vendor relationships and global information transmission
- Open access to data rather than "need to know" access
- Frequent changes in suppliers and products
- Lack of standardization of security protocols across vendors and other partners
- Infected devices on a corporate network
- Obsolete security infrastructure or outdated hardware/software

The vulnerabilities of these multiple entry points need to be recognized, monitored, and addressed by the acquisition specialists.

Responsibility and Accountability

Historically, IT managers were responsible and accountable for any issues related to the cyber world which was viewed as a technology-centered issue. Almost half of most organization leadership still views cybersecurity risk as an IT matter, rather than an organization-wide risk. Many organizations (46%; PWC, 2014) do not have a leadership role such as a Chief Information Security Officer (CISO) or a Chief Information Officer (CIO) to centralize all cyber related issues.

Supply chain cyber risk cannot be outsourced and can only be address with a holistic and collaborative risk mitigation plan that includes effective collaboration of a multidisciplinary team that includes not only IT professionals but also supply chain, finance, and HR professionals and, foremost, the support of the senior leadership (PWC, 2015).

---

[2] Malicious software that is imbedded on computers, devices, or networks, damaging files (e.g., spyware, worms, viruses, and Trojan horses)
[3] Unauthorized use of usernames and passwords to access a company's network
[4] Disruption systems or networks to prevent the normal operations of the organization
[5] Insertion of malicious code into Structured Query Language (SQL) to illegally access proprietary data, bypassing firewalls and other security measures

Creating effective cybersecurity operations requires significant in-house resources, but at the end of the day, it is the only way to protect the organization's data (CFO, 2015).

The cybersecurity approach is now also expanding the technology-centered view to include people and processes.

IT leadership is required to manage all technical aspects required to address cybersecurity risks (both hardware and software). They also play a key role creating systems and processes to mitigate the risks and communicating cyber threats to the organization's highest leadership groups.

Supply chain managers need to understand how the cybersecurity risk management process of their suppliers could expose/affect their own organization. They also need to understand the type of threats the organization faces, the assets that are under risk, and how the IT department is handling these risks.

Finance leadership support is required not only to support the cybersecurity program among the organization, but also to identify threats and quantify the financial impact of cyber risk (CFO, 2015).

The Human Resources (HR) managers also play a key role to prevent the hiring and contracting of employees who pose high risk (intentional or not) to the organization. Research has shown that people who are willing to conduct or assist in cyber-attacks suffer from one or more identifiable conditions (Machiavelism, narcissism, and psychopathy) and have a combination of these personality traits: immaturity, low self-esteem, amorality and lack of ethics, superficiality, lack of conscientiousness, manipulativeness, and instability. HR managers can look out for threats when hiring and contracting.

The other role that HR plays in cybersecurity is in the recruiting and retention of highly skilled cybersecurity experts. This is a prevalent challenge for organizations of all sizes. Either because cybersecurity employees choose to create their own security firm or they move to a more attractive job position, the current shortage is affecting the way organizations deal with the cyber risk.

Given that cybersecurity breaches carry a series of financial, operational, reputational, and legal damages, senior leadership involvement becomes more critical to support the development and implementation of a sound cybersecurity risk mitigation program. At the end of the day, the magnitude of the consequences will make them accountable for the approach the organization has taken to address cyber risks.

Cost & Benefits of Cybersecurity

As serious as the cybersecurity risk is, it does not receive the attention and priority it requires among organizations across industries. Most cybersecurity budgets are inadequate to address the organization's risk until a breach becomes a reality. A sound cybersecurity cost benefit analysis is usually done post mortem (after an attack) and then generally by a third-party, such as the media. The Heartland Payment Systems Inc. attack in 2015 (more than 100 million credit and debit card numbers were stolen) is a good example of this analysis. The company had to pay $150 million in fines and legal costs and suffered damage to its reputation as a payment processor. To address future liabilities, the company quadrupled its security budget, reduced the number of computer systems that process credit and debit card data, and added more encryption and system-monitoring tools.

The WSJ (2014) describes an interesting metric tracked by Gartner Inc. which states that for every $5.62 a business spent after a breach, an organization could spend $1 before an attack on encryption and network protection to prevent intrusions and minimize damages.

As obvious as this might look, not all organizations appear to justify the investment, as they assume the investment cost will be higher than the cost related to the breach. There might be different reasons behind this negligence, and we discuss four: the accounting perspective, the human nature perspective, the financial perspective, and the political perspective.

Accounting Perspective

Since cybersecurity investments do not generate revenue, it is usually treated as an expense of doing business and not part of the net profit of the organization. Hence, the potential impact is not proactively and consistently quantified (much less the assessment of the intangible consequences of a cyber-attack, such as the credibility, reputation, legal expenses, etc.). But even so, a more reasoned approach, as Dew Smith (Supply Chain Quarterly, 2015) suggested, would be to revise the accounting method used to include IT and cybersecurity spending into the cost methodology of supply chain management (absorption costing[6]). This method would consider cybersecurity spending as part of the total direct cost (including overhead cost associated with logistics, sales/marketing, and manufacturing).

Human Nature Perspective

Behavioral and brain science research shows that the human moral judgement system drives the urgent need for actions when it deems the issue at task a moral imperative (the principle originating inside a person's mind that compels that person to act). Reasons that cyber risk is not currently registering as a moral imperative could be (1) that cyber risk is communicated as an abstract and complex potential event (no immediate threat with a specific shape), and hence it does not generate a rapid emotional intuitive reaction; (2) that it is not perceived as an intentional moral transgression on the part of employees, and therefore is judged less severely than if it were an intentional act; and (3) it is deemed to be an uncertain event (may or may not happen) too far away in the future which promotes unrealistic optimisms (it will not happen to us), and this optimism prevents people from identifying themselves as a target. Changing the way in which organizations communicate cybersecurity risk can change the way we perceive its urgency to act.

Financial Perspective

Driven by a financial statement/budget compliance focus, some may argue that for some organizations (especially large ones), the losses involved are so small compared to their revenue that it is easier to take a chance and write off any losses should they occur. For example, Target's data breach had a $252 million cost during 2013 and 2014. After insurance coverage and tax deductions, Target ended up paying $105 million, which is about 0.1% of its 2014 revenue. Similarly, Home Depot paid $28 million, after the $15 million insurance payment, which represents 0.01% of the company's revenue the same year (CBS News, 2015). This approach not only does not assess the full consequences of a data breach (e.g., competitive advantage, brand equity, customer loyalty, reputation, etc.), but also ignores the ethical component. The responsibility to protect customers' data, inform them of the breach, and gain back their trust still lies with the organization, and it is not reflected in the financial statements.

---

[6] All of the manufacturing costs are absorbed by the units produced.

Since 2011, the SEC[7] has urged organizations to provide details about the operational and financial risk posed by cyber-attacks in the risk section of their filings and discuss with the investors (in the Management's Discussion and Analysis section) any effects of cyber-attacks on operating results, liquidity, or financial position. So far, investors have not been satisfied with the information provided and feel the disclosures were presented "merely for legal prophylaxis, instead of for informing investors" (Fortune, 2015).

Political Perspective

In 2014, the Obama administration issued new cybersecurity guidelines urging companies in critical infrastructure industries to increase their efforts to protect and monitor their networks and train employees. Some organizations took the guidelines as non-commercial because cybersecurity measures must be cost-effective for an individual company or be supported by some economic incentives. Some suggested that if the government wants to improve cyber-defense, the government should subsidize the cost (e.g., tax breaks). To complicate this matter, many regulators consider this problem more of a corporate responsibility that national security (CFO, 2105).

Organizations perform cost-benefit analysis for expenses. The cybersecurity cost (i.e., budget allocation) then represents a careful balancing act where it is critical to identify the right amount of security given the risks the organization is exposed to.

Trends

Cybersecurity Approach

Cybersecurity risk management has been focused on preventing cybercrime through the use of internal controls, employee training, and firewalls, among others. Acknowledging that it is impossible to protect a network against 100% of the attacks, it is key to include a plan to address the possible breaches to minimize the damage. According to Heather Crofford, CFO of Shared Services at Northrop Grumman, "detections, response and recovery are where the increasing investment needs to be" (CFO, 2015).

Supply Chain Analytics (Souza, 2014), Cyber Risk Modeling (CFO, 2015), & Big Data (PwC, 2016)

Supply chain analytics currently focuses on the use of information and analytical tools to make better decisions regarding the material flows in the supply chain. Some of these same concepts and tools can also be used for cybersecurity purposes (including the supply chain cyber risk). The availability of Big Data and the use of descriptive and predictive analytics could prove useful as tools to fight cybersecurity threats.

Descriptive analytics[8] tools can be quite useful to provide a clear view of the current situation of the suppliers. Supply chain mapping is an example where an organization can map all their suppliers (and their suppliers) and plot them using different criteria such as the importance in the organization's supply chain, level of cybersecurity maturity, etc. Figure 3 illustrates how the French Nuclear Power Supply Chain is mapped using one of the currently available tools (Sourcemap, n.d.).

---

[7] Security and Exchange Commission
[8] Uses existing information to evaluate what is happening

Figure 3. Example of Supply Chain Mapping Using Sourcemap.com

Predictive analytics can use past data to forecast future cyber risks, including those coming from the supply chain. Data source and quality are important components to use these tools (e.g., linear and non-linear regression and data mining).

Despite the limited detail data availability (both the causes of the breach and balance sheet impact), some insurance-related organizations are already focusing their efforts on using data analytics in cyber risk modeling to help assess their clients' cyber risk. In theory, the frequency of cyber-attacks is rapidly increasing the amount of data to be analyzed. However, the number of organizations who are cyber-attack victims who are willing to share these types of data is pretty small, and hence current models are based only on publicly available data from various insurance sources.

Furthermore, in 2015, almost 60% of private and government organizations used Big Data analytics to model and monitor cybersecurity threats, respond to incidents and audit and review data to understand how it is used, by whom, and when. As more data become available, this trend is expected to significantly increase in the next few years.

Cloud Enabled Cybersecurity, Advanced Authentication (PwC, 2016)

Cloud service providers have invested significant amounts in advanced technologies for data protection, privacy, network security, and identity and access management. The most frequently used cloud-based cybersecurity services include real-time monitoring and analytics, advanced authentication, identity and access management, threat intelligence, and end-point protection.

Simple password use is no longer an adequate way to access data. All industries are quickly migrating to the use of advanced authentication to help manage access and improve trust among customers and business partners. Combinations of one-time passwords and hardware tokens, biometrics, security keys, and special applications are the most common advanced authentication methods used.

Cybersecurity Risk Management Practices

Risk-Based Cybersecurity Frameworks

Most private and government organizations use a standard framework, or a combination of multiple frameworks, currently available to develop an effective cybersecurity program. The most frequently used are the National Institute of Standards and Technology (NIST) framework and ISO 27001 (Information security management). In addition, there are

other, more acquisition specific frameworks, such as the Centre for the Protection of National Infrastructure (CPNI) Framework (methodology) which helps develop supply chain specific security risk mitigation implementation plans, ISO 2800-2700 (Specification for security management systems for the supply chain), and the Supplier Assurance Framework (UK Cabinet Office, 2015).

The **NIST** Framework was developed after President Obama's executive order on "Improving Critical Infrastructure Cybersecurity" and is quickly becoming a standard among industries in the United States. The Framework consolidates existing global standards and practices to help organizations understand, communicate, and manage their cyber risks (White House, 2014). The Framework offers a road map to develop a cybersecurity program for organizations with no security experience. For organizations with a more mature cybersecurity, the Framework helps them improve the communication with the organization's leadership and suppliers about cyber risk management. The Framework has three components: Core, Tiers, and Profile.

The Framework core is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. The Framework has four implementation Tiers (Partial, Risked Informed, Repeatable, and Adaptive) to reflect how the organization views cybersecurity risk and assess the processes in place to manage that risk. The Framework profile represents the outcomes based on business needs that an organization has selected from the Framework categories and subcategories.

ISO 27001 was developed to "provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system." It uses a top-down, risk-based approach and is technology-neutral. Also, it provides requirements to develop an information security management system to managing sensitive company information so that it remains secure. It includes people, processes, and IT systems by applying a risk management process. It can help small, medium, and large businesses in any sector keep information assets secure.

The whole ISO 27000 family aims to help organizations keep information assets (e.g., financial information, intellectual property, employee details or information entrusted to you by third parties) secured.

The **CPNI** proposes that supply chain security risk be an extension of existing risk management processes. The extensions should include:

- Comprehensive maps of all tiers of the upstream and downstream supply chains to the level of individual contracts
- Risk scoring each contractor to link in to the organization's existing security risk assessment
- Due diligence/accreditation/assurance of suppliers (and potential suppliers) and the adoption, through contracts, of proportionate and appropriate measures to mitigate risk
- Audit arrangements and compliance monitoring
- Contract exit arrangement

ISO 2800-2007 (Specification for security management systems for the supply chain) offers a framework for providing effective physical security management through a system that identifies security threats, assesses risk, establishes objectives for implementing controls, and continuously improves the physical security of the organization. It identifies requirements for implementing and operating a security management system, including

organizational (security) structure, authorized personnel responsible for security management, assessing and maintaining competence of personnel, and training for personnel responsible for security.

The **Supplier Assurance Framework** (UK Cabinet Office, 2015) applies to official contracts and enables the early identification of high risk projects; it provides a framework for the risk management of contracts that is consistent, effective, and understood by government, stakeholders, and suppliers and enables information sharing and accountability. It is flexible enough to allow its customization to meet specific business needs. It is particularly relevant where information is shared through contracts or agreements.

To different extents, all these frameworks address training needs. Note, however, that none of them do so specifically for the acquisition community and much less to the detail it is required.

High-Reliability Organizations (HROs)—An Alternative Approach to Cybersecurity

As previously discussed, cyber-attacks are mostly driven by network administrators and users' errors rather than by inadequate security technology. Organizations can implement key concepts of HROs (Weick & Sutcliffe, 2015) to address the human error component of cybersecurity risks as the U.S. military has successfully done. The basic principle is to treat the unknown as knowable by following some key principles:

- Mindful organizing (organizing is about coordination)
- Preoccupation with failure
- Reluctance to simplify
- Sensitive to operations
- Commitment to resilience
- Deference to expertise

The U.S. Navy's nuclear-propulsion program is arguably the HRO with the longest track record. There are six principles that helped the Navy contain the impact of human error: (1) integrity, (2) depth of knowledge, (3) procedural compliance, (4) forceful backups, (5) a question of attitude, and (6) formality in communication.

Building an HRO requires the personal attention of senior leadership as well as a substantial financial investment in training and oversight. This is approach has proven to be effective at the whole organization level and can certainly be extended to include the acquisition group of the organization.

Recommendations

Considering that each organization has a different cybersecurity maturity level, the following recommendations are directed to the risks on the acquisition process, and hence, assume there is already a risk analysis based cybersecurity risk management program in place.

Purely technical solutions will not address the magnitude of the risk. Even the best technology will not work well with poorly trained operators. Processes and people need to be part of the solution in order to deliver a comprehensive cybersecurity approach customized to address the cyber risks associated to the supply chain.

To improve cybersecurity, the acquisition community must understand

- and manage the multiple dimensions of cyber-attacks (opportunities and risks) that can compromise the bottom-line of the organizations they work for and with.
- and recognize the cyber threats inherent in procuring complex, modern systems with significant cyber components and the challenges of understanding the vulnerabilities of new, complex modern networked systems.
- that purchasing products and services that have the appropriate cybersecurity designed and built-in may have higher up-front costs but lower life-cycle costs because of the reduced need to fix vulnerabilities in the systems later.
- that given the sensitive nature of their work, including intellectual property and financial data, their IT processes, information, and systems will be an attractive target for cyber threats from both criminal sources and nation state adversaries.

Risk Assessment

Risk management experts agree that the first step to take is to assess the financial risk of a security breach. This requires a detailed inventory of the organization's assets at risk that will be used to assess the financial risk. However, the training of the professionals who will be assessing the cyber risks should be a step even before this, as the validity of the cyber risk assessment will be as good as the cyber risk skill and knowledge the employees who perform the analysis have.

Subsequently, organizations need a detailed accounting of all firms (partners, affiliates, network participants, etc.) that are part of the supply chain (both upstream and downstream) to identify the weakest link then, assess the degree of reliance of each of those organizations (size and scope).

Finally, survey and audit all third-party partners' (i.e., fourth-party contractors) cybersecurity process/programs and capabilities to identify the level of risk each of them carry. All this information will allow the organization to create a vendor compliance protocol and strategic outsourcing guidelines to ensure a standard level of cybersecurity across the supply chain.

New vendor compliance can be achieved through the consistent implementation of cybersecurity incentives/requirements. This can include but is not limited to the requirement of cybersecurity protocols, conditions, and capabilities to be aligned with the organization's cybersecurity risk mitigation process as part of the contract approval criteria.

The case is slightly different with existing vendors, as contracts have already been awarded. In this case, a contract amendment (allowed within the law) to include the new cybersecurity requirements is the easiest way. In the event this is not feasible, the procurement and IT groups should create a process to mitigate the risks those existing vendors bring to the organization.

The greater the complexity of the supply chain, the more extensive the risk management efforts should be. Therefore, organizations with a complex supply chain should include multiple layers of security (e.g., redundant backup systems, multiple-stage access thresholds for credentials, ongoing threat monitoring, etc.).

Insurance Use for Commercially Developed Systems

To reduce the financial impact of a breach, organizations are including cyber liability insurances in their organizations' plans. Cyber insurance organizations provide *partial protection* against internet-based risks relating to information technology infrastructure and information assets. Typical first-party coverage includes forensic investigation, legal advice, notification costs of communicating the breach, credit monitoring, PR expenses, loss of profits and extra expenses during the time your network is down. Common third-party coverage includes legal defense, settlements, damages and judgements related to the breach, liability to banks for re-issuing credit cards, cost of responding to regulatory inquires, and regulatory fines and penalties (WS&Co, 2014).

The use of cyber insurance is meaningful for large organizations with auditable cybersecurity programs. However, some small- or medium-size organizations might get a false sense of security from cyber insurance and fail to implement a sound cybersecurity program (Market Watch, 2015).

From an acquisition perspective, suppliers who have cyber insurance might indicate a higher level of cyber maturity as insurance companies perform extensive cyber audits before securing a policy.

Implementation of KPIs to Monitor Progress

Having a cybersecurity program that includes supplier risk is not enough to conclude the threats are under control. The performance of this program needs to be continuously monitored to address the dynamic nature of the risks. The use of Key Performance Indicators (KPIs) has been proven as an effective way to communicate challenges and opportunities. The cyber world includes technological, process/procedural, and people KPIs that can be implemented to assess the effectiveness of the current cybersecurity program (Dowdy, Hubback, & Solyom, 2014). KPIs can also be used to assess the level of risk each supplier brings to the organization.

Technological KPIs focus on the number and type of electronic touchpoints and highlight the quality of management of these connections. An example of such a KPI is the number of days that elapse between Microsoft issuing a critical software update and the entire organization installing it. Process/procedural KPIs can include data-policy and operational policy indicators to assess, for example, if the percent of sensitive data encryption meets the current policies, or if the number of attempted security-policy breaches within a certain period meets industry standards. People KPIs (including business partners' employees) measure the success rate of training, employee conformity to security guidelines, or employee knowledge and use of best-practice e-mail behavior. They may be assessed through spot tests.

It is certainly a good practice to include cybersecurity metrics into the organizations KPIs, balance scorecard and/or executive dashboard. Given the current technology focus of cybersecurity, it will require the effective training of both cybersecurity professionals and employees to identify (and implement) a set of meaningful KPIs that will bridge technology issues with business context to better respond to the needs of the organization.

The Future

As of 2015, only 34% of U.S. organizations (30% UK/Europe and 28% Middle East/North Africa) were prepared to deal with cybersecurity risks resulting from the IoT (Ponemon Institute, 2015). Current predictions assess the number of devices connected to the internet will reach 30 billion by 2020 (IDC, 2015). From 2014 to 2015, the number of incidents related to the IoT has increased by over 150%. Most of the IoT attacks were

related to mobile devices, embedded systems, consumer technologies and operational systems (PwC, 2016). The obvious consequence of the IoT is that the cyber risk penetration area will increase in size and complexity. Organizations need to consider a strategy to deal with risks created by the internet of things.

Early in 2015, President Obama signed the "Promoting Private Sector Cybersecurity Information Sharing" executive order to enable private and government organizations to share industry specific information and intelligence related to geographies, issues, events, or specific threats through the creation of new Information Sharing and Analysis Organizations (ISAOs). The goal of these ISAOs is to address cyber threats to public health and safety, national security, and economic security of the United States by sharing information related to cybersecurity risks and incidents from private companies, nonprofit organizations, executive departments and agencies (agencies), and other entities. Organizations need to join ISAOs or similar organizations to share and receive cyber intelligence.

References

CBS News. (2015, March 12). The reason companies don't fix cybersecurity. Retrieved from http://www.cbsnews.com/news/the-reason-companies-dont-fix-cybersecurity/

Centre for the Protection of National Infrastructure (CPNI). (2015, April). Mitigating the risk in the national infrastructure supply chain. Retrieved from https://www.cpni.gov.uk/documents/publications/2015/13-april-2015-mitigating-security-risk-in-supply-chain.pdf?epslanguage=en-gb

CFO. (2015, March 30). What's the cost of a cyberattack?. Retrieved from http://ww2.cfo.com/risk-management/2015/03/whats-cost-cyberattack/

CISCO. (2015). *Mitigating the cybersecurity skills shortage*. Retrieved from http://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-talent.pdf

CSX. (2015). *State of cybersecurity: Implications for 2015*. Retrieved from http://www.isaca.org/cyber/Documents/State-of-Cybersecurity_Res_Eng_0415.pdf

Department of Homeland Security (DHS). (2016). *Budget-in-brief fiscal year 2016*. Washington, DC: Author.

Dowdy, J., Hubback, J., & Solyom, J. (2014). *Can you hack it? Managing the cybersecurity challenge*. McKinsey.

Fortune. (2015, March 10). *Cyber security: An afterthought for corporate America?.* Retrieved from http://fortune.com/2015/03/10/cyber-security-an-afterthought-for-corporate-america/

Greenberg, A. (2015, September 9). GM took 5 Years to fix a full-takeover hack in millions of Onstar cars. *Wired*.

Hackers find weaknesses in car computer systems. (2013, September 4). Fox News. Retrieved from http://www.foxnews.com/leisure/2013/09/04/hackers-find-weaknesses-in-car-computer-systems

IDC. (2015, June). *Connecting the IoT: The road to success*.

Identity Theft Resource Center (ITRC). (2016, January 25). *2015 data breaches*.

MarketWatch. (2015, March 25). *Cybersecurity insurance—Weighing the cost and the risks.* Retrieved from http://www.marketwatch.com/story /cybersecurity-insurance-weighing-the-costs-and-the-risks-2015-03-25

Ponemon Institute LLC. (2015, February). *2015 global megatrends in cybersecurity* sponsored by Raytheon. Retrieved from

http://www.raytheon.com/news/rtnwcm/groups/gallery/documents/content/rtn_233811.pdf

Porter, M. E. (1985). *Competitive advantage: Creating and sustaining superior performance*. New York, NY: Free Press.

PricewaterhouseCoopers (PwC). (2014, June). *US cybersecurity stalled, key findings from the 2014 US state of cybercrime survey*.

PricewaterhouseCoopers (PwC). (2015, July). *US cybersecurity stalled, key findings from the 2015 US state of cybercrime survey.*

PricewaterhouseCoopers (PwC). (2016). *Turnaround and transformation in cybersecurity—Key findings from The Global State of Information Security® survey 2016.*

Prince, B. (2015, May). *Widespread Windows XP use remains among business despite end-of-life: Survey*. Retrieved from http://www.securityweek.com/widespread-windows-xp-use-remains-among-businesses-despite-end-life-survey

Sourcemap. (n.d.). *End-to-end supply chain visualization.* Retrieved March 23, 2016, from http://www.sourcemap.com/end-to-end-supply-chain-visualization/

Souza, G. C. (2014). *Supply chain analytics*.

Supply Chain Quarterly. (2015). *Is your supply chain safe from cyberattacks?.* Retrieved from http://www.supplychainquarterly.com/topics/Technology/20150622-is-your-supply-chain-safe-from-cyberattacks/

Tuttle, H. (2015, January 8). *Human error caused 93% of data breaches*. Retrieved from http://www.riskmanagementmonitor.com/human-error-caused-93-of-data-breaches/

UK Cabinet Office. (2015, February). *Supplier assurance framework.*

Verizon. (2013). *2013 data breach investigations report*. Retrieved from http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf

Wall Street Journal (WSJ). (2014, February 25). *Companies wrestle with the cost of cybersecurity*. Retrieved from http://www.wsj.com/articles/SB10001424052702304834704579403421539734550

Weick, K. E., & Sutcliffe, K. M. (2015). M*anaging the unexpected: Sustained performance in a complex world*. New York, NY: John Wiley and Sons.

White House. (2014, February 14). *Launch of the cybersecurity framework* [Press release].

Winnefeld, J. A., Jr. et al. (2015, September). *Cybersecurity's human factor: Lessons from the Pentagon.* Retrieved from https://hbr.org/2015/09/cybersecuritys-human-factor-lessons-from-the-pentagon

WS&Co. (2014, June). *Cyber insurance 101: The basics of cyber coverage*. Retrieved from https://wsandco.com/cyber-liability/cyber-basics/

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF BUSINESS & PUBLIC POLICY
NAVAL POSTGRADUATE SCHOOL
555 DYER ROAD, INGERSOLL HALL
MONTEREY, CA 93943

www.acquisitionresearch.net