PELL CENTER
for INTERNATIONAL RELATIONS
and PUBLIC POLICY

SEPTEMBER 2016

UNDERSTANDING CYBER THREATS

LESSONS FOR THE BOARDROOM

FRANCESCA SPIDALIERI

SENIOR FELLOW, CYBER LEADERSHIP

About the Author

Francesca Spidalieri is the Senior Fellow for Cyber Leadership at the Pell Center for International Relations and Public Policy at Salve Regina University, where she leads the Cyber Leadership Research Project and the Rhode Island Corporate Cybersecurity Initiative (RICCI). Francesca has been appointed by Governor Gina Raimondo to the Rhode Island Cybersecurity Commission, and serves also as subject-matter expert for the Potomac Institute for Policy Studies' Cyber Readiness Index Project, and as a Distinguished Fellow at the Ponemon Institute. Her academic research and publications have focused on cyber-strategic leadership, cyber risk management, cyber education and awareness, cybersecurity workforce development, and the professionalization of the cybersecurity industry. She regularly speaks at cyber-related events nationwide and contributes to journal articles and other publications on cybersecurity matters affecting countries and organizations.

Ms. Spidalieri holds a B.A. in Political Science and International Relations from the University of Milan, Italy; an M.A. in International Affairs and Security Studies from the Fletcher School at Tufts University; and has completed additional coursework in cybersecurity at the U.S. Naval War College's Center for Cyber Conflict Studies.

Background

This paper is based on content presented at the Executive Seminar: "Understanding Cyber Threats in the Boardroom," hosted by Salve Regina University's Pell Center and Bank of America Merrill Lynch in May 2016. The event was attended by senior leaders and business executives from large, medium, and small-size enterprises in Rhode Island and Massachusetts.

REPORT SPONSORSHIP

Sponsoring companies have contributed input and feedback, however they are not responsible for the content of this report. The information provided in this report is presented as guidelines to be used for informational purposes, and are not intended to constitute legal advice or counsel. Please direct any comments or questions regarding our research sponsorship policy to Pell Center's Senior Fellow, Francesca Spidalieri, at francesca.spidalieri@salve.edu.

Sponsors:

The Cost of Cyber Insecurity

"Cyber insecurity is a tax on growth."[1]

The rapid proliferation of information communication technologies (ICTs) and the Internet has brought immense benefits to organizations of all sizes and in all sectors in terms of increased efficiency and productivity, enhanced global reach, and greater ability to deliver a wide range of goods, data, and services across borders. This proliferation and increased reliance on the Internet and ICTs have also exposed governments and organizations alike to a growing number of vulnerabilities and opened the door to a wide range of malicious cyber activities from cybercrime to economic espionage to cyber disruption (e.g. denial of service attacks). Moreover, the rise of the Internet of Things (IoT) and the growing number of connected devices coming online between now and 2020 (estimated to range from 20 to 50 billion) are expanding the attack surface at an exponential rate. Compounding these issues are the increased migration to the cloud environment and the hyper-connectivity brought on by new technologies like 5G, which are further amplifying the opportunities for malicious actors to compromise and breach information, disrupt service, and even destroy property (as in the 2012 cyber attack on Saudi Aramco).[2]

Today, cyber risks affect all industries and all markets and can represent an existential threat—especially to smaller companies that have limited resources and have often built their business around one line of products or services.

In recent years, corporate executives and board members worldwide have ranked cyber risk as the third-highest risk to their business, behind only taxation and customer loss.[3] Lloyd's estimates that cyber attacks cost businesses as much as $400 billion a year, including restitution, fines, business disruption, legal and remediation services. A 2015 Ponemon Institute study showed that the cost of cybercrime to businesses worldwide is on the rise and that average annual losses now exceeds $7.7 million per company, and as much as $15.4 million—more than twice the world average—for American firms.[4] A more recent survey conducted by PwC found that more than half of US companies have experienced some type of cyber incident and that, like many experts in the field estimate, the other half of the companies have most likely already been compromised without knowing it.[5]

In addition to the growing scope, volume, and sophistication of cyber attacks, there is a widening gap between the supply and demand of knowledgeable and experienced cybersecurity professionals capable of addressing the threats at hand.[6] The shortage of a highly trained cybersecurity workforce can be felt across all sectors, from the federal government to the private sector, with potential negative consequences for national security and the global economy. The demand for information security professionals has never been greater and is expected to rise to 6 million globally by 2019, with a projected shortfall of 1.5 million trained personnel.[7]

Despite this well-documented skills gap, a survey conducted by CyberVista and Zogby Analytics found that only 25 percent of C-level executives and board members—who should be responsible for building a team of trusted experts and fostering a culture of security—believe that recruiting and retaining skilled professionals is a critical cybersecurity issue, ranking it sixth out of seven main cybersecurity priorities.[8] Most of them still display tendencies to treat cybersecurity as an isolated "IT problem" best left to their already overwhelmed IT department. This approach is both untenable and dangerous. As research has shown, their natural optimism bias combined with a lack of understanding of cybersecurity risks often leads business executives to believe that their company's security posture is stronger than it actually is, or that since they have purchased the latest security tool or software, or they are complying with specific state or federal government policies, then they are secure.[9]

Only 25 percent of C-level executives and board members . . . believe that recruiting and retaining skilled professionals is a critical cybersecurity issue, ranking it sixth out of seven main cybersecurity priorities. Most of them still display tendencies to treat cybersecurity as an isolated "IT problem."

These common trends reinforce the conventional wisdom that views cybersecurity as a "technical problem" rather than a "people problem." And while technology solutions and compliance with business standards and regulations are certainly important to protecting an organization against cyber threats, those actions alone are insufficient.[10] No matter how good any particular technology is, its efficacy is limited if it is not effectively adopted and implemented by management teams and correctly used by skilled employees who follow well-defined processes. Otherwise, vulnerabilities will surface that can be leveraged by both internal and external threat actors.[11] In short, any technology for combating cyber threats is only as good as the people who develop, implement, use, and maintain it. Moreover, while technology failures and vulnerabilities can be blamed for many cyber incidents, the "people problem" is often at the core of some of the most damaging cyber attacks. Indeed, most cybersecurity issues start with ordinary technology users who have not received proper training, do not take security seriously, or prize convenience over security by—consciously or not—sidestepping basic standards of best practices.

Exacerbating this already complex problem is the attitude that many organizations continue to show towards cybersecurity: that no matter how bad cyber threats are, they will not be a victim because they are either too small, not as profitable, not part of a critical sector, already well-protected, and so forth. There are endless reasons they give themselves to justify not adopting proper cybersecurity measures and effective mechanisms to counter cyber risks. As a result, they operate under a false sense of security, which furthers the mismatch between senior executives' perception of cyber risks and the reality. This is compounded by the factors highlighted above and the additional "communication/language gap" that often puts policy-savvy executives and the technical people at odds with each other, and can ultimately lead to an even more fragile security environment.

Thus, it goes without saying that cybersecurity has to be considered one of the most important aspects of managing organizations of all sizes in all sectors, with duties and responsibilities extending through every level of the workforce. Achieving cybersecurity, however, is a complex and never-ending task. While there is no silver bullet solution to protect every organization from all cyber risks, staying informed, educating all employees about cybersecurity, and practicing good cyber

hygiene as a function of managing and growing a business are probably the most effective solutions any organizations can adopt to prevent, mitigate, and respond to cyber incidents.

This paper provides an overview of existing frameworks, toolkits, and other resources that organizations can consult to stay informed about cyber threats, develop and update comprehensive cyber risks management strategies, and learn about some of the best practices and effective mechanisms deployed in the field to combat those threats. Particular attention is given to the role that modern boards of directors and C-suite executives must play in the overall cybersecurity posture of any organization operating in the digital age.

Cyber Threats and Emerging Trends – Stay Informed and Plan Your Defenses!

"Ignorance is not bliss when it comes to cybersecurity"[12]

Understanding the threat landscape and staying abreast of the latest techniques and vulnerabilities can help organizations better plan their defenses and better allocate human and financial resources to minimize cyber risks. Multiple reports published every year by organizations such as Experian, Hewlett Packard, Ponemon Institute, PwC, Verizon, and others, provide analyses of year-long studies and survey results, including details about new cyber threats and emerging trends in cyberspace, and offer valuable recommendations and lessons learned from the field.

While many of these reports show a threat landscape still characterized by old problems and well-known threat vectors, they also shed some light on specific industry patterns, new techniques used by attackers to breach systems and wreak havoc, and the evolving nature of new technologies that are expanding the attack surface.

Common trends highlighted by these studies in the past year include:

(1) a widening gap between the time (minutes or even seconds) it takes an attacker to compromise a system and exfiltrate data, and the time (weeks or more) it takes an organization to discover a breach—it is typically customers, law enforcement, or a security blogger who sound the alarm, not the organization's own security measures;[13]

(2) a persistent and growing number of healthcare breaches—healthcare companies have become one of the most targeted sectors by cyber criminals, driven by the high value compromised data can command on the black market, along with the continuous digitization and sharing of medical records;[14]

(3) the rise of collateral damages resulting from cyber attacks to critical infrastructure (Ukraine's power grid) and large data breaches (such as the US Office of Personnel Management (OPM) and the Ashley Madison breaches), which affected people who never had direct contact with the entities attacked and who never expected they might be involved in a security breach;[15] and

(4) a growth of corporate extortion as prices for records fall.

It is worth noting the increase of third party (supply chain) risks, which will be further exacerbated by the proliferation of IoT, cloud computing, mobility and mobile devices, and big data analytics. According to a recent study conducted by the Ponemon Institute and the Santa Fe Group, only half of the organizations surveyed have formal programs in place to manage third party risks, and even those that have them do not think that they are necessarily being effective at mitigating or curtailing those risks.[16]

Setting the Tone from the Top

As with all other corporate risks, Boards of Directors, C-suite executives, and senior management ultimately bear the responsibility for cybersecurity issues, and must view cyber risk as a component of their overall enterprise risk management process rather than as a compliance issue. Companies must integrate cybersecurity front and center into their daily activities and must anchor it into their decision-making processes in a holistic and comprehensive manner. Today, no board or C-suite executive can ignore cybersecurity—it is the source of systemic risk and potential damaging "material effects" that can hurt an organization's profits, value, brand, and financial future.[17]

Companies must integrate cybersecurity front and center into their daily activities and must anchor it into their decision-making processes in a holistic and comprehensive manner.

As a result, it is important to set a positive tone and communicate an organization's values from the top and throughout the enterprise to employees and stakeholders, and also to business partners, vendors, and other third parties in order to minimize both business risks and cyber risks.[18] While cybersecurity is a shared responsibility, creating a culture of security that prioritizes addressing cyber risks across the entire organization must start at the top. If management is committed to a culture and environment that embraces honesty, integrity, security, and ethics, employees are more likely to uphold those same values.

In recent years, senior executives and board members have become more involved in cyber risk management activities, and some organizations have even put in place formal structures to report risk assessment results and cyber preparedness levels back to the board. Some of the best practices and lessons learned from the field include:

- Aligning the business objectives of an organization with its security needs and making cybersecurity part of the overall corporate planning process (e.g. strategic plan, 5 year plan).
- Knowing what the organization's high value assets (the "crown jewels") are, where they are, who has access to them, and how they are being protected—governance should ensure that access is limited to those who really need it and actual access is checked against this list.
- Shifting the focus to proactively identify risks—audits are not sufficient—and being more proactive in developing cyber risk mitigation strategies, including working with management to establish the vision, risk appetite, and strategic direction.[19]
- Conducting a cost-benefit analysis of the potential direct and indirect costs of cyber incidents to the organization—this may help justify increased financial and human resources dedicated to manage specific cyber risk areas.

- When partnering with third parties that have access to sensitive and confidential information, ensuring they have appropriate technologies and controls in place to mitigate cyber threats and are compliant with company's standards and policies.
- Carrying out risk assessments across the entire enterprise (including the compliance department; security/information security department; procurement department; legal department; human resource department; and so forth)
- Setting metrics to measure the effectiveness of security controls and risk management programs, and assigning accountability to ensure that objectives are accomplished.
- Reviewing management's analysis of the effectiveness of risk assessments; reviewing and approving plans to address and manage risks or control weaknesses; reviewing opinions on the results issued by independent risk management or internal audit functions; overseeing the deployment of risk management plans and ensuring that they incorporate people, processes, and technologies.
- Effectively communicating the organization's values to employees and other stakeholders through training, policies, on-the-job mentoring, memos/codes of conduct, and other awareness programs to ensure enterprise-wide adoption.[20]
- Ensuring that if employees witness unethical behaviors from other employees or third party vendors that they are able to report such behavior with guaranteed anonymity and without fear of retaliation.
- Leveraging available studies and statistics to show where an organization is compared to peers in the same field or industry; and establish what added value can be brought to the table, and what can be done more proactively and efficiently.
- Deciding whether to purchase cyber insurance to moderate the economic impact of cyber risks, including insider negligence and third party risks.
- Becoming involved in a consortium, trade association, or other forums dedicated to sharing best practices and effective mechanisms to counter cyber threats.
- Establishing relationships with law enforcement officials and other government officials to interdict or investigate cyber crimes (such as fraud, IP theft, privacy breach, etc.)

Risk Management Objectives, Incident Response and Business Continuity Planning

As discussed above, business processes, such as lengthy supply chains, bring-your-own-device (BYOD) policies, cloud computing, and IoT are undermining organizations' cybersecurity and increasing their overall risk exposure. While cyber risks, as with all risks, cannot be completely eliminated, they can be managed through informed decision-making processes, careful planning, and appropriate allocation of resources.

A comprehensive enterprise risk management (ERM) plan ought to integrate cyber risk as a major business risk. ERM plans are built on the premise that managing cyber risk is critical to an organization achieving its business' goals and objectives. Implementation of the ERM plan will, in turn, facilitate more informed decision making throughout an organization leading to more effective resource allocation, operational efficiencies, and the ability to mitigate and rapidly respond to cyber threats.

The core objectives of these plans should be to: prevent cyber attacks; protect sensitive information and intellectual properties; secure critical services and infrastructures; minimize downtime and business disruption caused by a cyber incident; preserve brand and reputation; comply with regulations and legal mandates; and maintain good relationships with customers and business partners.

Every organization must be able to respond to this basic set of questions:

- Where is the most sensitive information stored, who has access to it, and how is it being protected (for example, encryption, systems segregation, dual-factor authentication)?
- What are the most pressing cyber threats to this organization's industry or sector? What are the best practices to combat those threats?
- Are cybersecurity risks, controls, and costs briefed to the Executive team and Board of Directors?
- Who is responsible for cybersecurity in the organization and are those roles and responsibilities clearly identified and communicated?
- Are systems and servers patched promptly and sensitive data backed up regularly and stored offsite?
- Is system usage monitored and access to sensitive data immediately revoked when an employee leaves or changes roles?
- What are the security requirements for third party vendors that have access to sensitive and confidential information? How often are those requirements reviewed and by whom?
- What are the rules that govern the use of company resources (computers, smartphones, tablets) and policies regarding BYOD? How often are those rules and policies updated and communicated to the entire organization? Are they enforced?
- Is there a published incident response plan for emergencies and crises? Is it exercised?
- Is there a published business continuity plan in place? Is it exercised?
- Are organization-wide cybersecurity trainings and exercises conducted regularly?
- What are the reporting and notification requirements if a breach happens?

There are also various independently-validated best practices, security controls, assessment tools, and benchmarks that can help organizations assess their cybersecurity readiness, develop cybersecurity and risk management plans, and identify and address weaknesses and shortcomings. While no framework fits every organization or every sector, companies should consider the following foundational references and select the one(s) that best apply to their needs:

- The National Institute for Standards and Technology (NIST) Cybersecurity Framework;[21]
- NIST Special Publication 800 series;[22]
- The Center for Internet Security (CIS) Controls for Effective Cyber Defense;[23]
- The International Organization for Standardization (ISO) standards;[24]
- The Control Objectives for Information technology (CoBIT) standards;[25]
- The Department of Homeland Security (DHS) cybersecurity evaluation toolkits;[26]
- The Health Information Trust Alliance (HITRUST) Common Security Framework (CSF);[27] and

- The Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool.[28]

Closing the Cybersecurity Workforce Gap

"Competition for [cybersecurity] talent is fierce and establishing a strong team is essential."[29]

Over 209,000 cybersecurity jobs are currently estimated to be vacant in the United States alone, with the number predicted to rise to 1.5 million by 2019.[30] From the federal government to the Fortune 500, the demand for knowledgeable and experienced cybersecurity workers is only expected to increase in upcoming years, especially as organizations continue to experience data breaches and other cyber threats. The shortage of cybersecurity professionals is exacerbated by a lack of clarity and consistency in competency models, job descriptions, professional certifications, and training and education standards.[31] This in turn makes it harder to properly identify, recruit, place, and manage the cybersecurity workforce that organizations need.

The demand for knowledgeable and experienced cybersecurity workers is only expected to increase in upcoming years.

While no single panacea exists to close the gap between the burgeoning demand for cybersecurity talent and the supply of a professional workforce, organizations can start by focusing on their existing workforce and making them their first line of defense. This should include: ensuring that staff is regularly trained and tested so that they understand and fully appreciate their role in maintaining a strong cybersecurity posture; instituting clear cybersecurity policies for employees and vendors with access to sensitive information, systems, facilities, and equipments; and holding employees accountable for their role in limiting access to only those systems and data that employees actually need to do their job.

Organizations also have a variety of references, frameworks, and toolkits at their disposal to help them better assess their specific cybersecurity workforce needs, identify the most critical roles and responsibilities that need to be filled, and prioritize budget and talent acquisition efforts. For instance, the National Initiative for Cybersecurity Education (NICE) "National Cybersecurity Workforce Framework" identifies specific knowledge, skills, and abilities (KSAs) required to complete cybersecurity-related tasks;[32] the DHS "Cybersecurity Workforce Development Toolkit" can help organizations create their own cybersecurity career paths and devise solution to recruit and retain top talent;[33] and the CIS "Cybersecurity Workforce Handbook" provides a practical guide for managers of the cybersecurity workforce within an enterprise.[34]

Other best practices and effective mechanisms that can help organizations identify, recruit, place, manage, and retain a professional cybersecurity workforce include:

- Matching the culture of an organization to the type of workforce needed and understanding the specific human capital needs related to cybersecurity.
- Aligning the organization's cybersecurity strategy with the workforce management plan (involve the human resource department in the cybersecurity planning process from the outset).

- Performing a gap analysis to identify the roles and responsibilities that are not appropriately filled, and identifying positions that are most critical to the organization's security.
- Recognizing that cybersecurity is a complex subject that requires knowledge and expertise from multiple disciplines, including computer science, information technology, engineering, but also policy, law, economics, and ethics.
- Promoting a diverse workforce—it takes diverse experiences, different talents, and different ways of thinking to solve complex problems, and we cannot expect to close the talent gap to equilibrium without including more segments of the population.
- Making sure that personnel—from the IT department to the business units—are given proper (but limited) authority to access and protect data and systems, and that the people responsible for the organization's cybersecurity are properly deployed across the various functions of the business, enabled with clear scope of responsibilities, empowered with the appropriate authorities and reporting chains, and supported with ongoing training and development.[35]
- Encouraging cybersecurity workers, especially chief information security officers (CISOs), to understand the business they are in, the problems and business risks that a certain security tool or software may be able to address, and how to integrate security into business, and business into security. Their soft skills should include being able to communicate, negotiate, and develop relationships within the C-suite, so that they can be present when privacy or a corporate strategy is being discussed.[36]
- Exploring creative ways to source talent internally—current employees may have skills, abilities, and knowledge fit for cybersecurity, given the right training and development.
- Joining current and potential recruiting alliances that align with the organization's goals and recourses (for example, Centers for Academic Excellence (CAEs), career fairs, cyber competitions, hackathons, and Veteran's transition programs).
- Establishing an employee referral program to recruit talented and trusted cybersecurity professionals from employees' personal networks (such as universities, professional associations).
- Reaching out to local schools to help them develop a comprehensive cybersecurity curriculum and offer internships and traineeships for qualified students.
- Providing additional incentives to recruit and retain best talented employees, including but not limited to: training and education subsidies; flexible work arrangements; and leadership development opportunities.
- Determining the best mix of talent sourcing and deciding which cybersecurity functions can be performed by a third party (outsourcing).
- Engaging the entire workforce to secure the enterprise—cybersecurity is a shared responsibility.

Cyber Liability Insurance

Advanced cyber threats call for innovative approaches to combat data exposures, manipulation, hacks, insider threats, disruption of service, and other malicious cyber activities. As tactics to breach a system or steal sensitive information morphs, so must an organization's strategies in order to defend itself and be prepared to respond to significant data breaches and other cyber attacks. Organizations are increasingly considering cyber liability insurance to mitigate some of the financial

burden of cyber incidents. The reinsurance company Swiss Re predicted, "that by 2025, cyber coverage will be in every retail, commercial and industrial insurance policy."[37]

Today, the cyber insurance business is a $3 billion industry with more than 95 percent of all the cyber insurance policies underwritten in the world originating in the United States. Market experts estimate that the industry will triple in size by 2020 to about $8-9 billion and that it will continue to grow exponentially. "Cyber insurance will become this ubiquitous product that everybody will need to have in their business in the future."[38] Navigating the cyber insurance market, however, can be quite complex for organizations of all sizes given the different types of policies and products offered by various insurance companies, and the lack of standards for those types of coverage.

While regular insurance policies have started to add exclusions related to any type of digital risk, from disgruntled employees mouthing off about a company on social media to a big data breach, cyber insurance policies attempt to fill that void. They primarily help companies cover data breach impacts, response, and remediation costs (first-party costs), but are also starting to offer business interruption coverage (profit lost), networking interruption coverage, media liability, privacy liability, business-to-business lawsuit coverage, cyber extortion coverage (ransomware cases). Yet, tven within cyber liability insurance, there may be exclusions for social engineering coverage (phishing scams), employees' negligence, prior existing situations (check "retroactive date"), and so forth.

Evidence of well-established security best practices will increase the likelihood of acquiring coverage.

Before acquiring any type of coverage, organizations should determine what kind of data they collect, where they store it, for how long they keep it, how they are protecting it, how they are disposing of it, which cybersecurity standards they have adopted, and whether they are compliant with industry practices. Fault—which can negate coverage—often stems from negligence, which insurers define according to what they consider a reasonable effort to protect an organization's assets.[39] As a result, it is fundamental that companies understand their organization's security environment, and have a clear set of security standards (such as the ones discussed in above sections) and compliance policies that can be referenced if negligence or other exclusions ever comes into question. Moreover, evidence of well-established security best practices will increase the likelihood of acquiring coverage, since high-risk organizations pose a financial burden to insurers.

Aside from the NIST Cybersecurity Framework, other independent standards organizations, such as ISO, the International Electrotechnical Commission (IEC), ISACA, and SANS, have published sets of guidelines for organizational cybersecurity and created accreditation processes to further vet risk management strategies. These certifications, which often require compliance with specific industry standards and best practices, signal to insurers that a company is responsible and, thus, eligible for coverage.

In addition, the insurance industry recently adopted "Principles for Effective Cybersecurity," standards created by the cybersecurity task force of the National Association of Insurance Commissioners (NAIC). Other cybersecurity standards are evolving and being developed by different industries. When acquiring cybersecurity insurance, it is important to remember that an insurer's duty to provide coverage will depend on the organization's ability to meet the appropriate

standard of care. Organizations should therefore be familiar with the common standards in their specific industry as well as the guidelines required by their insurers.

Given the near-certainty that a breach will occur, even with the best cybersecurity policies and practices in place, post-breach loss management is and will be essential. In addition to the increase in cybersecurity standards, governments and industries are promoting, and in some cases mandating, cybersecurity insurance requirements in order to mitigate risks to companies and consumers. As a result, it is important for organizations to familiarize themselves with the cyber insurance market and decide how to integrate such policies into their overall ERM plans.

Conclusions

Cybersecurity issues and needs are complex and widespread, and call for knowledge and expertise from multiple disciplines, diverse experiences, different talents, and different ways of thinking to solve those complex problems.

Executive teams and board members of small, medium, and large-enterprise companies once viewed cybersecurity threats the same way they saw natural disasters—possible, but unlikely—and often continue to treat it as an isolated “IT problem” best left to chief information officers and technicians. A decade ago this may have been the right course of action, but today this approach is untenable and dangerous.

Companies must integrate cybersecurity front and center into their daily activities and must anchor it into their decision-making processes in a holistic and comprehensive manner. Modern boards and C-suite executives must view cybersecurity as a risk management problem, and develop sound strategies to protect their organizations’ sensitive information and digital investments. This requires them to have a deep understanding of the cyber context in which they operate and their organization’s security environment in order to make informed decisions based on cyber risk metrics and their appetite for risk, and to harness the right tools, policies, people, and training to respond to a dynamic and rapidly-developing array of threats.

Changing the mindset of senior executives—and holding them accountable for the overall cybersecurity posture of their organizations—may prove difficult, but it will be key to the survival of any enterprise in the digital age.

Endnotes

1. Melissa Hathaway et al., "Cyber Readiness Index 2.0 – A Plan for Cyber Readiness: A Baseline and an Index," *Potomac Institute for Policy Studies* (November 2015): 3.

2. Christopher Bronk, "The Cyber Attack on Saudi Aramco," *Survival* 55 (April-May 2013): 81-96, and Nicole Perlroth, "In Cyberattack on Saudi Firm, US Sees Iran Firing Back," *The New York Times,* October 23, 2012, http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html.

3. "Risk Index 2013," *Lloyd's* (July 2013): 5, http://www.ipsos.de/assets/files/presse/2013/publikationen/Lloyds%20Risk%20Index%202013report100713[1]%20Copy.pdf.

4. "2015 Cost of Cyber Crime Study: Global," *Ponemon Institute* (October 2015): 4, https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5207enw.pdf.

5. "Global Economic Crime Survey 2016," Pwc, (February 2016), https://www.pwc.com/gx/en/services/advisory/consulting/forensics/economic-crime-survey.html.

6. Francesca Spidalieri and Sean Kern, "Professionalizing Cybersecurity: A Path to Universal Standards and Status," *Pell Center Report* (August 2014): 1, http://www.salve.edu/sites/default/files/filesfield/documents/Professionalizing-Cybersecurity.pdf.

7. "The 2015 (ISC)² Global Information Security Workforce Study," *Frost & Sullivan,* (April 2015), https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-%28ISC%29%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf.

8. "New Zogby/CyberVista Survey Reveals Cybersecurity Education & Training Gaps Among Boards, C-Level Executives," *Business Wire*, January 25, 2016, http://www.businesswire.com/news/home/20160225005193/en.

9. "Cyber Security Incident Response: Are we as prepared as we think?," *Lancope and Ponemon Institute* (January 2014), http://www.ponemon.org/blog/cyber-security-incident-response-are-we-as-prepared-as-we-think.

10. Spidalieri, "Professionalizing Cybersecurity," 5.

11. Greg MacSweeney, "10 Financial Services Cyber Security Trends for 2013," Wall Street & Technology, December 5, 2012, http://www.wallstreetandtech.com/data-security/10-financial-services-cybersecurity-tre/240143809.

12. Peter W. Singer and Allan Friedman, "Cybersecurity: What Everyone Needs to Know," Oxford; New York: Oxford University Press, 2014: 10.

13. "2016 Data Breach Investigations Report," Verizon, http://www.verizonenterprise.com/verizon-insights-lab/dbir/.

14. "2016 Data Breach Industry Forecast," Experian Data Breach Resolution, (November 2015), http://www.experian.com/assets/data-breach/white-papers/2016-experian-data-breach-industry-forecast.pdf.

15. "Cyber Risk Report 2016: Threat Landscape, Vulnerabilities," Hewlett Packard Enterprise, (February 2016), http://www8.hp.com/us/en/software-solutions/cyber-risk-report-security-vulnerability/.

16. "Tone at the Top and Third Party Risk," Ponemon Institute & Shared Assessments, (May 2016), https://sharedassessments.org/summit/SA-2016-Ponemon-Study-Tone-At-The-Top-And-Third-Party-Risk-Final.pdf.

17. James Lewis, "Raising the Bar for Cybersecurity," Center for Strategic and International Studies, February 12, 2013.

18. "Tone at the Top and Third Party Risk," Ponemon Institute & Shared Assessments.

19. Michael Andreozzi, "Information Security & Risk Management," (presentation delivered at the Executive Seminar: Understanding Cyber Threats in the Boardroom, Providence, May 4, 2016).

20. Kevin Ricci, "Understanding Cyber Threats in the Boardroom: 5 Key Issues," (presentation delivered at the Executive Seminar: Understanding Cyber Threats in the Boardroom, Providence, May 4, 2016).

21. "A Framework for Improving Critical Infrastructure Cybersecurity," National Institute for Standards and Technology (February 2014), http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm.

22. For more on the National Institute for Standards and Technology Special Publication 800 series, see: http://www.nist.org/nist_plugins/content/content.php?cat.17.

23. "CIS Controls for Effective Cyber Defense, Version 6.0," Center for Internet Security, https://www.cisecurity.org/critical-controls.cfm.

24. For more on the International Organization for Standardization (ISO) standards, see: http://www.iso.org/iso/home.html.

25. For more on the Control Objectives for Information technology (CoBIT) standards, see: http://www.isaca.org/knowledge-center/cobit/pages/overview.aspx.

26. ICS-CERT, "Assessments," https://ics-cert.us-cert.gov/Assessments.

27. For more on the Health Information Trust Alliance (HITRUST) Common Security Framework (CSF), see: https://hitrustalliance.net/understanding-leveraging-csf/.

28. For more on the Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool, see: https://www.ffiec.gov/cyberassessmenttool.htm.

29. U.S. Department of Homeland Security, "Cybersecurity Workforce Development Toolkit," May 2016, https://niccs.us-cert.gov/sites/default/files/documents/files/Cybersecurity_Workforce_Development_Toolkit.pdf.

30. Steve Morgan, "One Million Cybersecurity Job Openings in 2016," *Forbes*, January 2, 2016, http://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#5e7e881d7d27.

31. "The HR Professional's Guide to a Cyber-Secure Workforce," *Center for Internet Security*, https://www.cisecurity.org/workforce/workplace/HR.pdf.

32. "National Cybersecurity Workforce Framework," National Initiative for Cybersecurity and Education, (April 2014), http://csrc.nist.gov/nice/framework/.

33. U.S. Department of Homeland Security, "Cybersecurity Workforce Development Toolkit."

34. "Cybersecurity Workforce Handbook: A Practical Guide to Managing your Workforce," *Council on Cyber Security,* (October 2014) https://www.cisecurity.org/workforce/images/Workforce.pdf.

35. "The HR Professional's Guide to a Cyber-Secure Workforce."

36. Author's interview with Steve Katz, President of Security Risk Solutions LLC and Executive Advisor at Deloitte, July 7, 2014.

37. Michel Lies, "How Do You Insure Against Cybercrime?," *The Wall Street Journal,* April 21, 2015, http://blogs.wsj.com/experts/2015/04/21/how-do-you-insure-against-cybercrime/.

38. Matt Cullina, "Cyber Liability Insurance," (presentation delivered at the Executive Seminar: Understanding Cyber Threats in the Boardroom, Providence, May 4, 2016).

39. Lisa Brownlee, "Cyber Risk Insurance: Preparing to Obtain Coverage with Standards and Frameworks, *RSA*, December 23, 2015, https://blogs.rsa.com/cyber-risk-insurance-preparing-to-obtain-coverage-with-standards-and-frameworks/.

PELL CENTER
for INTERNATIONAL RELATIONS
and PUBLIC POLICY

About the Pell Center

The Pell Center for International Relations and Public Policy at Salve Regina University is a multi-disciplinary research center focused at the intersection of politics, policies, and ideas. Dedicated to honoring Senator Claiborne Pell's legacy, the Center promotes American engagement in the world, effective government at home, and civic particpation by all Americans.

www.pellcenter.org