TESTIMONY OF
MR. ERIC A. PULSE
PRINCIPAL, EIDE BAILLY, LLP
CONFRONTING THE CHALLENGE OF CYBERSECURITY
U.S. SENATE COMMITTEE ON COMMERCE, SCIENCE AND TRANSPORTATION
SEPTEMBER 3, 2015

Chairman Thune, Ranking Member Nelson, and distinguished members of the Committee. My name is Eric Pulse and I am a Principal with the accounting, tax and consulting firm Eide Bailly LLP and I am the director of our Risk Advisory Services practice, specializing in assisting clients with information, data, and cybersecurity needs. Thank you for the opportunity to appear before you today to discuss the topic of "Confronting the Challenge of Cybersecurity." My testimony today is based solely on my personal experiences over nearly 20 years working with clients assessing, remediating, and implementing their information systems, data and cybersecurity controls.

The National Institute of Standards and Technology (NIST) defines cybersecurity as "the ability to protect or defend the use of cyberspace from cyber-attacks." The U.S. Department of Defense revealed that "**at the top** of the U.S. intelligence community's 2013 assessment of global threats is cyber, followed by terrorism and transnational organized crime." The severity and impact of cyber threats have changed the landscape in which governments, corporations, individuals, and, organizations of all industries, size, and complexities operate. Breaches of customer data, credit card information, employee and customer authentication credentials, etc. are becoming more commonplace. This persistent threat is a societal issue facing everyone with personally identifiable information, health records, banking and/or payment information, intellectual property, etc. At one point considered largely an IT issue, the increase in frequency and sophistication of cyber attacks requires organizations elevate the priority to C-suites and board rooms and an overall cultural shift as it relates to cybersecurity.

The recent cyberattack breaches at U.S. Office of Personnel Management (OPM), Sony, Anthem, Home Depot, Target, JP Morgan, and many others simply emphasizes the importance of cybersecurity. The Identity Theft Resource Center[1] identified that in 2015, through August 18, there have been a total of 505 reported data breaches resulting in an estimated loss of nearly

140 million records – and that number is records **known** to be compromised. Organizations spend millions of dollars on the latest security technologies and infrastructure to protect themselves from becoming the next organization in the news. However, cybersecurity is more than policies, procedures and technologies. It has to be woven into the fabric of how each person, whether employee or customer, thinks about security of data. It begins with a culture. The best security standards, frameworks, policies or procedures aren't able to anticipate every instance they are intended to facilitate. Security should be a part of the fabric of every decision an employee makes in the course of everyday business. Too often organizations sacrifice sound security practices in the name of customer service or process efficiency. The extra step it may take to clearly verify a customer or gain that extra piece of information to validate the legitimacy of the person on the other end of the phone, email, or transaction is overlooked because we are conditioned to provide exceptional customer service or we strive to be more efficient. Simply put, security has taken a back seat and that has to change. That change starts with organizational culture, and to be successful, a culture of IT security has to be in sync with the organizational mission as a whole.

I'd like to highlight four areas that need attention in order to combat cybersecurity challenges: a culture of security, the lack of skilled resources, a common framework, and threat intelligence.

Culture Shift

After September 11, 2001 and the tragic events of that day, the way our society viewed air travel changed dramatically. Restrictions on carry-on contents and long airport security lines are just a few restrictive, and to many degrees, necessary, changes to air travel. On a flight in the months following that fateful day, a passenger near the rear of an aircraft proceeded to the front and nervously informed the flight attendant that he didn't feel safe because there was someone in a seat near him using a set of nail clippers. In short, our entire culture changed overnight as it relates to air travel. Conversely, in light of the many recent data breaches and identified hacks of government, civilian, and private organizational computer systems, resulting in the loss of millions of data records, our society hasn't had the same necessary cultural shift. We are still nonchalant with our sensitive data, whether it be credit cards for card-not-present transactions, participating in a drawing by filling out an entry form with personally identifiable information, or by disclosing health records/information as part of a survey. Given the number of breaches that occur every day because someone clicked on the proverbial phishing link in an email scam, data is being compromised, identities are being stolen, millions of dollars are being lost, and still we have yet to experience the cultural shock and shift to better security practices.

The first "hacker" to be charged and convicted of his crimes was Kevin Mitnick. He was able to effectively contact the companies to which he eventually gained access and simply ask for the access and it was granted. The crime was considered "fraudulent intent" and not the act of gaining access itself. This is still one of the leading threats to the security of organizations today and gets identified publically as an "insider threat." We lose site of the fact that most of the "insider" acts are unknown and unintentional, thus demonstrating the need for an enhanced security culture.

Verizon's 2015 Data Breach Investigations Report[2] indicates that over 99% of all data breaches were successful exploits of vulnerabilities where the CVE (Common Vulnerability and Exposure) – or preventative fix – was over one year old. Nearly all data breaches occur because a fix to an exploitable vulnerability was not applied. This is particularly true with smaller organizations that continue to be targeted as attackers take advantage of frequently non-existent vulnerability and patch management programs, exploiting weaknesses in edge devices, web-based applications, payment card or point of sale systems.

Smaller organizations face include the lack of technical feasibility to immediately apply a software patch that fixes a vulnerability because frequently, a security patch will negatively impact the functionality of a piece of software running on the device being patched. While vulnerability and patch management programs are an integral control in cyber security, the clients I serve span the spectrum, from mature, highly integrated cybersecurity controls to non-existent controls where management has turned a blind eye in the interest of cost containment. The absence of a mature security culture and lack of cyber threat awareness emphasizes the need for further education at the highest organizational levels. The maturation of a security culture in the marketplace should start at the top in the boardrooms and continue with executive management driving it throughout their organizations.

Further educating the citizenry is also critical. Efforts like STOP.THINK.CONNECT by the National Cyber Security Alliance and the Department of Homeland Security highlight the importance of taking security precautions and understanding the consequences of actions and behaviors in order to enjoy the benefits of the Internet. I believe more visible efforts are necessary in order to educate a vast majority of people who simply take for granted the security of their personal and protected information.

Skills Gap

A recent survey by the SANS Institute[3] showed that 66% of respondents cited skills shortage as an impediment to effective incident response and overall cybersecurity. Many security professionals maintain a general technical security skillset tasked with implementing reasonable practices and procedures driven by compliance, however the rise in advanced threats and malware demonstrate the need for a more sophistically trained professional. This shortfall is reflected in my own daily experiences, whether it is with our clients or our firm, we are continually looking for personnel with the proper technical security skillset. The law of supply and demand has driven up the cost of these resources and many organizations simply cannot afford them, if they are even available. Many of the clients with which I work have opted to outsource many of these security functions given the limited availability of these skillsets. Heretofore, many security professionals contain a general technical security skillset tasked with implementing reasonable practices and procedures driven by compliance, however the rise in advanced threats and malware demonstrate the need for a more sophistically trained professional.

According to a poll conducted by Information Systems Audit and Control Association (ISACA) and the RSA Conference, and published in the "State of Cybersecurity: Implications for 2015" study, more than half of the global cybersecurity professionals polled reported that fewer than 25% of cybersecurity applicants are qualified to perform the skills needed for the job.[4]

I commend institutions like Dakota State University (DSU), and the initiation and evolution of their cybersecurity program. I believe we should encourage more institutions to deliver programs to train the security talent needed to adequately confront the cybersecurity challenge. We are only as strong as our weakest link and often the human component is that link. I believe there is also a need for more offensive security through hands-on penetration testing skillsets, requiring those to successfully attack and penetrate various live machines in a safe lab environment. In my opinion, we should be recruiting, educating, and training an army for this new frontier and the program here at DSU is one of many that should be filling that need in order to protect against an unseen attacker that can reside almost anywhere in the world, as long as there is an internet connection.

In the absence of personnel, organizations can invest in a strong security infrastructure using often expensive hardware and software solutions. The gap, however, resides with the manpower to effectively implement, monitor and maintain such an infrastructure. There are a myriad of security-specific certifications available in the marketplace, many focus on security generalities and others are platform-specific. I believe there is also a need for more offensive security hands-on penetration testing skillsets, requiring those to successfully attack and penetrate various live machines in a safe lab environment. In my opinion, we should be recruiting, educating, and training an army for this new frontier and the program here at DSU is one of many that should be filling that need in order to protect against an unseen attacker that can reside almost anywhere in the world, as long as there is an internet connection.

Frameworks = Roadmap

Industries often create or rely upon a standard for securing data, whether it be critical internal data, customer/patient information, intellectual property, trade secrets, financial data, and more. When we work with healthcare organizations, the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH) are utilized as standards for ultimately securing patient health records. Financial institutions rely upon Federal Financial Institutions Examination Council (FFIEC) and Gramm-Leach-Bliley Act (GLBA) guidelines for securing customer information. Federal government agencies and contractors thereto rely to varying degrees on the NIST Special Publication 800-53 – Recommended Security Controls for Federal Information Systems. Cloud computing companies providing services to the Federal government must comply with Federal Risk and Authorization Management Program (FedRAMP), and many federal agencies and contractors must comply with Federal Information Systems Management Act (FISMA), both of which are based on NIST SP 800-53. Retailers and organizations processing, storing or transmitting credit/debit card data utilize the Payment Card Industry (PCI) Data Security

Standard (DSS). Some third party service providers will utilize the American Institution of Certified Public Accountants' (AICPA) Trust Services Principles for security, availability, processing integrity, confidentiality and privacy of data. Still others build information risk and security controls on an ISO 27000 or 31000 framework; or the Council on Cyber Security's 20 Critical Security Controls. These frameworks come in many shapes and sizes, ultimately with the same goal – protection and security of information. Yet it is very common for us to discuss NIST frameworks with IT staff, many with over 10 years experience, who are not familiar with those frameworks, what they provide, or how to use them.

There are a number of private and non-profit organizations that provide guidance on securing data. One such organization, HITRUST, is a collaboration of healthcare, business, technology and information security leaders. HITRUST has established the Common Security Framework (CSF), which is a framework that can be used by organizations, healthcare in particular, to secure personal health and financial information. The CSF is an information security framework that harmonizes the requirements of existing standards and regulations, including federal (HIPAA, HITECH), third party (PCI, COBIT) and government (NIST, FTC)[5]. In the same light, the Cloud Security Alliance (CSA) is an organization "dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. CSA harnesses the subject matter expertise of industry practitioners, associations, governments, and its corporate and individual members to offer cloud security-specific research, education, certification, events and products."[6] Other organizations, like the Multi-State Information Sharing Analysis Center[7], the U.S. Chamber of Commerce[8], and the Federal Trade Commission[9], offer guides for assisting organizations with establishing a security environment designed to secure data. Many organizations have limited resources and others struggle with understanding their specific requirements and a direction for building a secure environment for protecting themselves, and ultimately their data, from cyber attacks. Most depend on their particular industry or their own customer requirements for guidance.

For organizations who are absent a regulated framework, the Council on Cyber Security's 20 Critical Security Controls are, in my opinion, an effective set of items that can be used across industries to build a control structure to combat against cyber threats. Consisting of the following, they provide organizations a much needed roadmap.

- Inventory of Authorized & Unauthorized Devices
- Inventory of Authorized & Unauthorized Software
- Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- Continuous Vulnerability Assessment & Remediation
- Malware Defenses
- Application Software Security
- Wireless Access Control
- Data Recovery Capability
- Security Skills Assessment & Appropriate Training to Fill Gaps
- Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- Limitation and Control of Network Ports, Protocols and Services
- Controlled Use of Administration Privileges
- Boundary Defense
- Maintenance, Monitoring & Analysis of Audit Logs
- Controlled Access Based on the Need to Know
- Account Monitoring & Control
- Data Protection
- Incident Response and Management
- Secure Network Engineering
- Penetration Tests and Red Team Exercises

The key to effective implementation of these controls is the growth and development of a set of skilled resources in the marketplace.

I commend NIST, the Council on Cyber Security, HITRUST, FS-ISAC, and many other organizations, for creating security standards and guidelines for organizations to follow in order to protect themselves. I believe continued dialogue between industry groups and the legislative branch will help stress the importance of cyber security initiatives and further the understanding of security expectations in the marketplace.

Threat Intelligence

With cyber threats on the rise, I believe in the collaboration of public and private resources to share information about the attacks that are on the horizon. Cybersecurity by its nature is more reactive than proactive. Perpetrators are able to advance their tactics more rapidly than the defensive infrastructure. The “Deep Net” contains a number of forums offering free attack tools available to anyone with the goal of initiating any number of attack scenarios. An attacker can launch an attack at any time toward any target and the use of botnets make tracing the attack extremely difficult. The commercialization of malware tools also allows the hacking community to remain a step ahead. However, the more a specific type of attack occurs, the better the chance of recognizing it by collaboratively sharing threat intelligence. Network defense and incident response require a strong element of intelligence and counterintelligence that security teams must understand and leverage to successfully defend their cyber infrastructure, once again highlighting the need for an increase in technically qualified professionals.

The Department of Homeland Security is responsible for protecting our Nation’s critical infrastructure from cyber threats and, according to its mission, information sharing is critical to create shared awareness of malicious cyber activity. The National Cybersecurity and Communications Integration Center (NCCIC) is a 24x7 cyber situational awareness, incident response, and management center for the Federal Government, intelligence community, and law enforcement. The Center shares information among the public and private sectors to provide greater understanding of cybersecurity and communications situation awareness of vulnerabilities, intrusions, incidents, mitigation, and recovery actions.

The Cyber Threat Intelligence Integration Center provides integrated all-source intelligence analysis related to foreign cyber threats and cyber incidents affecting U.S. national interests; support the U.S. government centers responsible for cybersecurity and network defense; and facilitate and support efforts by the government to counter foreign cyber threats.

Public-private partnerships like National Cybersecurity Alliance, HITRUST, FS-ISAC and others provide industry-specific resources for cyber and physical threat intelligence analysis and sharing. Forums like BlackHat and Defcon also provide valuable insight into emerging threats and how to combat them. I encourage the continued evolution of the sharing of threat intelligence between the public and private sectors.

Legislation

For the record, I do not believe additional regulation is necessary. Government has taken notice of the cybersecurity as challenges evidenced by the volume of recent legislation impacting cybersecurity. Recent legislation includes:

P.L. 113-274, Cybersecurity Enhancement Act of 2014
P.L. 113-282, National Cybersecurity Protection Act of 2014,
P.L. 113-246, Cybersecurity Workforce Assessment Act
H.R. 104, Cyber Privacy Fortification Act of 2015
H.R. 234, Cyber Intelligence Sharing and Protection Act
H.R.555, Federal Exchange Data Breach Notification Act of 2015
H.R. 580, Data Accountability and Trust Act
H.R. 1053, Commercial Privacy Bill of Rights Act of 2015
H.R. 1560, Protecting Cyber Networks Act
H.R. 1704, Personal Data Notification and Protection Act of 2015
H.R. 1731, National Cybersecurity Protection Advancement Act of 2015
H.R. 1770, Data Security and Breach Notification Act of 2015
H.R. 2205, Data Security Act of 2015
S. 135, Secure Data Act of 2015
S. 177, Data Security and Breach Notification Act of 2015
S. 456, Cyberthreat Sharing Act of 2015
S. 547, Commercial Privacy Bill of Rights Act of 2015
S. 754, Cybersecurity Information Sharing Act of 2015
S. 961, Data Security Act of 2015
S. 1027, Data Breach Notification and Punishing Cyber Criminals Act of 2015
S. 1158, Consumer Privacy Protection Act of 2015

Bills like H.R. 1770 cite requirements for information security as follows: *"A covered entity shall implement and maintain reasonable security measures and practices to protect and secure personal information in electronic form against unauthorized access as appropriate for the size and complexity of such covered entity and the nature and scope of its activities."* Given the number of security frameworks available, as cited previously, it is apparent that guidance for "reasonable security measures" has been established. I believe other economic incentives will generate additional results. Evidence suggests that contractual implications are driving adherence to standards. Many organizations are being asked to demonstrate the effectiveness of their security controls as part of initiating a contract with a customer. Other economic incentives for the demonstration of "meaningful use" of a cybersecurity framework could prove valuable.

In addition to legislation, litigation is also a factor driving the necessity for more attention to cybersecurity controls. On August 24, a Third Circuit U.S. Court of Appeals panel of judges upheld the FTC's authority to play a key role in regulating cybersecurity relative to consumer data protection against breaches and allowed the FTC to proceed with a lawsuit against a large hotel chain citing "unfair business practice provisions" when it took inadequate security measures to protect consumer data after a breach that exposed over 600,000 payment cards. Litigation like this and a recent Neiman Marcus case, where 7th Circuit Court of Appeals reinstated a lawsuit against them over a 2013 data breach in which hackers stole credit card information from as many as 350,000 customers, could open a virtual Pandora's Box and pave the way for an unending line of class-action lawsuits that could change the economic landscape.

Conclusion

Thank you again for the opportunity to appear before you today to discuss our efforts to confront the challenges of cybersecurity. In conclusion, I highlight four areas that I believe need increased attention in order to combat cybersecurity challenges: a culture of security, the lack of skilled resources, a common framework, threat intelligence and the education, implementation and collaboration thereof.

Foster the Change to a Security Culture

I believe our society needs to experience a cultural shift in the attitude of security consciousness. Organizationally, culture is driven from the top of the organization, in boardrooms, C-suites, and executive management. Public/private sector collaboration should focus on education of businesses and consumers to increase awareness of evolving cyber threats and practices necessary to combat them. There are numerous examples of this effort, one of which is STOP.THINK.CONNECT by the National Cyber Security Alliance and the Department of Homeland Security. Regulated industries like healthcare, government and financial services have provided consumer education as part of mandated efforts.

Emphasis on Increasing Security Personnel

I believe we should invest further in developing programs for educating and training a section of the workforce to adequately address the ever-changing cyber threat landscape. We necessarily invest hundreds of billions of dollars in a military to protect our country and we need to be equipping and training a new "soldier" to protect both public and private entities in this evolving frontier. Programs like those at Dakota State University are leading the way.

Encourage Implementation of a Framework

I believe in the continued evolution of various frameworks, across industries, working to incorporate critical controls that are relevant to combat cybersecurity threats and encourage the implementation of the relative frameworks with the goal of reaching every organizations that handles a consumer's sensitive data.

Threat Intelligence Collaboration

I believe that collaborated information sharing between government agencies and the private sector is essential to confronting the challenges of cybersecurity. I encourage expanded private sector access to threat and intelligence from Federal intelligence and law enforcement agencies. The goal should be to provide organizations, including their third party vendors with information on threats, vulnerabilities, and exploits. The public sector should continue to coordinate information sharing efforts with industry organizations and others, like National Cybersecurity Alliance, HITRUST, FS-ISAC, and others.

Thank you again for this opportunity to present this testimony and I look forward to your questions.

Notes

1 - "Data Breach Reports." *Identity Theft Resource Center* (n.d.): n. pag. 25 Aug. 2015. Web. 28 Aug. 2015. <http://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf>.

2 - "2015 Data Breach Investigations Report (DBIR)." *Verizon Enterprise Solutions*. Verizon, n.d. Web. 28 Aug. 2015. <http://www.verizonenterprise.com/DBIR/2015/>.

3 – Torres, Alissa. "Maturing and Specializing: Incident Response Capabilities Needed." (August 2015): n. pag. *Https://www.sans.org/*. SANS Institute. Web. 28 Aug. 2015. <https://www.sans.org/reading-room/whitepapers/analyst/maturing-specializing-incident-response-capabilities-needed_36162.pdf>.

4 - Richards, Kathleen. "Cybersecurity Skills Shortage Demands New Workforce Strategies." *SearchSecurity*. N.p., Aug. 2015. Web. 28 Aug. 2015. <http://searchsecurity.techtarget.com/feature/Cybersecurity-skills-shortage-demands-new-workforce-strategies>.

5 - "About Us - HITRUST." *Hitrust About Us Comments*. N.p., 23 Jan. 2014. Web. 28 Aug. 2015. <https://hitrustalliance.net/about-us/>.

6 - *About: Cloud Security Alliance*. N.p., n.d. Web. 28 Aug. 2015. <https://cloudsecurityalliance.org/about/>.

7 - *Cyber Security: Getting Started: A Non Technical Guide*. Ely, Cambridgeshire, United Kingdom: It Governance, 2013. Multi-State Information Sharing & Analysis Center. Web. 28 Aug. 2015. <https://msisac.cisecurity.org/resources/guides/documents/Getting_Started_Print.pdf>.

8 - "Internet Security Essentials for Business 2.0." (2012): n. pag. U.S. Chamber of Commerce. Web. 28 Aug. 2015. <https://www.uschamber.com/sites/default/files/issues/technology/files/ISEB-2.0-CyberSecurityGuide.pdf>.

9 - *Start with Security: A Guide for Business* (June 2015): n. pag. Federal Trade Commission. Web. 28 Aug. 2015. <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>.