Written Testimony of Dr. Kevin F. Streff

Dakota State University, Faculty and Department Chair – Cyber Operations and Security

Faculty – University of Wisconsin, Graduate School of Banking

Founder and Managing Partner – Secure Banking Solutions, LLC

Founder and Managing Partner – HELIX Security, LLC

Before the

United State Senate

Committee on Commerce, Science and Transportation

Hearing on

Confronting the Challenge on Cybersecurity

September 3, 2015

WITNESS STATEMENT

Kevin Streff, Ph.D. is an Associate Professor and Department Chair at Dakota State University in Madison, SD and conducts cybersecurity education and research in the financial services sector, with a particular focus on understanding the security issues of small and medium-sized financial institutions. Dr. Streff works with the banking associations all across the United States to understand rural banking vulnerabilities and solutions to mitigate them. Dr. Streff has over 25 years of experience working in insurance, banking and credit operations.

Professor Streff teaches managerial elements of information security, including risk management, security policy, information security management systems, disaster recovery, business continuity planning, auditing, and incident response planning. Dr. Streff has numerous publications in peer-reviewed journals such as *Journal of Information Warfare, Journal of Computer Information Systems, Journal of Autonomic and Trusted Computing, Journal of Computing Sciences in Colleges,* and *Issues in Information Systems*. He is the recipient of over $7.5 million in grants and contracts over the past ten years. Dr. Streff serves on several conference program committees, including International Conference on Information Warfare, and Cybersecurity, Network, Database and Software Security. Dr. Streff was session chair at several prestigious systems science conferences over the past several years, including organizing and chairing a mini-track on Information Assurance and Computer Security at the International Conference on Information Warfare. Dr. Streff was a keynote speaker at several national security conferences, presented over two hundred times at state, regional and national banking conferences, and published in both America's Banker and Community Banker. He has been featured on *ABC News, Forbes Magazine* and *National Public Radio*.

Dr. Streff is Founder of Dakota State's security program, and currently serves as Department Chair for the Cyber Operations and Security department, which has been recognized by The Department of Homeland Security and The National Security Agency as a Center of Excellence in Information Security Education, Research and Cyber Operations. He is also Founder and Past-President of InfraGard South Dakota, an FBI outreach program to promote the protection of critical infrastructure in SD, ND and MN. He is also Founder and Past-President of Secure Banking Solutions, an information security consulting firm focused on improving information security in community banks and credit unions in the U.S. SBS assists over 900 small and medium-sized financial institutions in 48 states with their information security and compliance needs. Dr. Streff is on faculty at the Graduate School of Banking at the University of Wisconsin where he helped develop the recently launched Bank Technology Management School and Bank Security School.

Introduction

Chairman Thune, Ranking Member Nelson and Members of the Senate Committee on Commerce, Science, and Transportation, I am pleased to appear before you today on behalf of Dakota State University to share our views on the current state of data/cyber security. These comments will be made to address our country's readiness to identify and thwart attacks on businesses and our nation's critical electronic infrastructure. Particular emphasis will be placed upon small business security and the cybersecurity readiness level of the banking sector.

My name is Dr. Kevin Streff and I am Department Chair of the Cyber Operations and Security Program at Dakota State University, which has been recognized by The Department of Homeland Security and The National Security Agency as a Center of Excellence in Information Security Education, Research and Cyber Operations. Along with Dr. Pauli, I am here today representing one of the top cybersecurity programs in the nation. We appreciate the invitation to appear before the committee on this important issue, and thank the committee for their leadership and foresight in dealing with these issues before a crisis state.

Background

Systematic and repeated cyberattacks occur daily against our defense, government, academic, and industry networks looking to carry out a variety of electronic crime and disruption of our nation's digital infrastructure. In 1998, Presidential Decision Directive 63 identified 18 critical infrastructures, which America depends upon daily. Are we prepared to handle a digital attack against our cyber infrastructure? 4.5 million small and medium-sized businesses are also under heavy attack and constitute substantial risk of loss to our economy. In fact, most small and medium-sized business lack the requisite skills and resources to combat these cyber threats.

In this testimony, we will review the current legal and regulatory environment in which financial institutions and small and medium-sized businesses must operate (SECTION I), communicate technology trends to consider (SECTION II), discuss security and privacy experiences in the financial services sector that have impacted small and medium-sized financial institutions (SECTION III), and discuss cybersecurity concerns and recommendations for the President and Commerce Committee to consider (SECTION IV).

SECTION I. Overview of Current Data Protection Laws, Regulation, and Policy Statements in Financial Services

A. 1970 - Bank Secrecy Act

In 1970, Congress passed the Bank Secrecy Act (BSA). BSA requires U.S. financial institutions to assist U.S. government agencies to detect and prevent money laundering. The act specifically requires financial institutions to keep records of cash purchases of negotiable instruments, file reports of cash transactions exceeding the daily aggregate amount of $10,000, and to report suspicious activity that might signify money laundering, tax evasion, or other criminal activities. Several anti-money laundering acts, including provisions in title III of the USA PATRIOT Act, have been enacted up to the present to amend the BSA. (See 31USC 5311-5330 and 31 CFR

Chapter X (formerly 31CFR Part 103)). The documents filed by financial institutions under BSA are used by law enforcement agencies, both domestic and international, to identify, detect and deter money laundering whether it is in furtherance of a criminal enterprise, terrorism, tax evasion or other unlawful activity.

B. 1999 - Financial Industries Modernization Act of 1999 (Gramm-Leach-Bliley)

The Gramm-Leach-Bliley Act (GLBA) 15 U.S.C. §§ 6801-6810 (disclosure of personal financial information), 15 U.S.C. §§ 6821-6827 (fraudulent access) repealed the Glass-Steagall Act of 1932, and is part of broader legislation which removes barriers to banks engaging in a wider scope of financial services. GLBA applies to financial institutions' use and disclosure of non-public financial information about consumers. Section 501(b) requires administrative, technical, and physical safeguards to protect covered non-public personal information. Federal banking agencies have published Interagency Guidelines Establishing Standards for Information Security for financial institutions subject to their jurisdiction. 66 Fed. Reg. 8616 (February 1, 2001) and 69 Fed. Reg. 77610 (December 28, 2004). The Guidelines are published by each agency in the Code of Federal Regulations, including:

- Federal Deposit Insurance Corporation, 12 C.F.R., Part 364, App. B;
- Office of the Comptroller of the Currency, 12 C.F.R., Part 30, App. B;
- Board of Governors of the Federal Reserve System, 12 C.F.R., Part 208, App. D-2 and Part 225, App. F;
- Office of Thrift Supervision, 12 C.F.R., Part 570, App. B; and
- National Credit Union Administration, 12 C.F.R., Part 748

The Federal Trade Commission has issued a final rule, Standards for Safeguarding Customer Information, 16 C.F.R. Part 314, and the Securities and Exchange Commission promulgated Regulation S-P: Privacy of Consumer Financial Information, 17 C.F.R. Part 248 for financial institutions within their respective jurisdictions. These requirements mean that all financial institutions must develop, document and operationalize a comprehensive information security program. The administrative, technical and physical safeguards are sweeping and expansively interpreted by federal and state regulators to include everything from the physical security of buildings, data security at service providers, to the types of authentication used during online banking sessions. Each bank must report annually to the Board of Directors on the status of the information security program. The Guidelines require a risk assessment designed to: "identify reasonably foreseeable internal and external threats" to customer information, assess the likelihood and potential damage of these threats, and to assess the effectiveness of a wide variety of information security controls. GLBA is significant because of the extensive requirements and regulatory oversight imposed upon the financial industry and carried out by federal and state regulators.

C. 2001 - USA PATRIOT Act

The USA PATRIOT (Patriot Act) was enacted in 2001 and reduced restrictions on law enforcement agencies' ability to search telephone, e-mail communications, medical, financial, and other records; eased restrictions on foreign intelligence gathering within the United States; and expanded the Secretary of the Treasury's authority to regulate financial transactions. Section 314(b) of the USA PATRIOT Act permits financial institutions, upon providing notice to the US Department of the Treasury, to share information with one another in order to identify and report to the federal government activities that may involve money laundering or terrorist activity.

D. 2002 - Sarbanes Oxley Act

The Sarbanes-Oxley Act of 2002 (SOX) was enacted to restore confidence in the integrity of the financial reporting process at publicly traded companies, influenced by high profile accounting scandals at firms such as Enron and WorldCom. However, each publically-traded financial institution that is affected by the Sarbanes-Oxley Act has some level of reliance on automated information systems to process, store and transact the data that is the basis of financial reports, and SOX requires financial institutions to consider the IT security controls that are in place to promote the confidentiality, integrity, and accuracy of this data. SOX states that specific attention should be given to the controls that act to secure the corporate network, prevent unauthorized access to systems and data, and ensure data integrity and availability in the case of a disaster or other disruption of service. Also, each system that interfaces with critical financial reporting data should have validation controls such as edit and limit checks built-in to further minimize the likelihood of data inaccuracy.

E. 2006 - Payment Card Industry Standard

The Payment Card Industry (PCI) Security Standards Council is an Industry group formed to manage and maintain the Data Security Standard (DSS), which was created by the Council to ensure the security of payment card information. Sensitive data is involved in card transactions, including account number, cardholder name, expiration date, and PIN. The intent of the PCI DSS is to ensure that card transactions occurring across multiple private and public networks are subject to end-to-end transaction security. The payment card industry consists of Card Issuers, Card Holders, Merchants, Acquirers, and Card Associations. From the collection of card information at a point of sale, transmission through the merchant's systems to the acquiring bank’s systems, then on to the card issuer, the PCI DSS requirements attempt to ensure sufficient security safeguards are in place on the card data from beginning to the end of a card transaction. Enforcement of the security requirements is done by the card associations and through a certification process of each association member. The certification process is carried out by Qualified Security Assessors (QSA) who audit systems and networks to ensure the mandatory controls are in place. Certification does not guarantee that an organization will not suffer a data breach, as several PCI certified organizations have suffered data breach incidents.

F. 2013 - Identify Theft Red Flags Rule

The Identify Theft Red Flags Rule (Red Flags Rule) requires financial institutions to implement a written Identity Theft Prevention Program that is designed to detect the warning signs of identity theft in their daily operations. By identifying red flags in advance, financial institutions will be better able to identify suspicious patterns that may arise, and take steps to prevent a red flag from escalating into identity theft.

A financial institution Identity Theft Red Flags Program should enable the organization to:

1. Identify relevant patterns, practices, and specific forms of activity – the “red flags” – that signal possible identity theft;
2. Incorporate business practices to detect red flags;
3. Detail appropriate response to any red flags you detect to prevent and mitigate identity theft; and
4. Be updated periodically to reflect changes in risk from identity theft.

Shortly after promulgation of the rule, regulatory agencies began issuing examination procedures to assist financial institutions in implementing the Identity Theft Red Flags, Address Discrepancies, and Change of Address Regulations, reflecting the requirements of Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003.

G. 2015 Cyber Security Guidance

The recent focus of the bank examiners has been cybersecurity readiness. In fact, in 2013 and 2014, the Federal Financial Institutions Examination Council (FFIEC) conducted a 500 bank study to examine the preparedness level of the U.S. banking system and documented their findings which included some major shortcomings, especially in the risk management, awareness, information sharing and leadership domains. They subsequently documented a cybersecurity risk-based approach which most banks are examining as we speak to determine next steps. The study also focused on the Board and management team being able to set “the tone at the top” as it relates to cybersecurity.

H. Miscellaneous Regul atory Guidance

The FFIEC is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the federal financial regulatory agencies. As such, the FFIEC publishes the Information Technology Examination Handbook, which is used by banking regulators in executing examinations of information technology and systems of financial institutions. The Handbook includes ten (10) booklets, one of which is the "Information Security Booklet”, which provides a baseline against which a financial institution subject to GLBA can be evaluated. The "Information Security Booklet" attempts to provide a high level, comprehensive overview of the major types of information security controls one would necessarily expect to be operating effectively within a financial institution. The types of controls are not limited in applicability to just financial institutions, and are derived from the same principles underpinning all major information security frameworks.

I. Third Party Self-Regulation

Small and medium-sized financial institutions depend heavily on hardware and software vendors for nearly all banking products. In addition, many of these vendors become service providers offering to host and manage their products for the small and medium-sized financial institution (SMFI). The service provider industry has experienced several significant data breaches affecting the financial services industry in the past several years, including Target (40 million data records) and Office of Personnel Management (21.5 million data records), etc. When companies choose to outsource data processing to a third party, they typically perform information security due diligence on the third party to understand how the data will be protected. A very common standard for third party assurance has been the SSAE16 standard. BITS, a non-profit organization, has also attempted to standardize the assessment of third-party service providers by developing the "BITS Framework for Managing Technology Risk for Service Provider Relationships", which includes two tools to help service providers in control selection and implementation. In summary, SMFIs operate in an increasingly complex regulatory environment, with community banks regulated aggressively and credit unions a little less. This regulation is necessary, but causes significant financial, resource, and other issues in SMFIs who must leverage technology to compete. Increasing regulation is likely as additional technologies are deployed and the cybersecurity stakes grow, but all increased regulation must be tempered with a SMFI's ability to stay in business and meet the needs of their customers. The majorities of SMFI's are in rural locations and may be the only local funding source for a community.

SECTION II. Technology Trends

Technology is advancing faster than SMFIs' ability to respond with appropriate mitigating security controls. For example, the use of cell phone cameras to take a picture of a check as the basis for making an electronic deposit into an account, or P2P payment transactions by cell phones create security exposures for which there are inadequate controls to prevent fraud. Fortunately, most SMFIs are not first adopters of new technology, but rather prefer to wait until the systems become more seasoned before embracing newer technologies. Moreover, the timeline between introduction, implementation and adoption of new technology by consumers continues to shrink. Just ten years ago, data processing was the buzz where computers were essentially back-office equipment designed to promote efficiency in the financial institution. Today, technology is front-line differentiators for banks and businesses, with customers demanding to use mobile technologies and social media to conduct commerce. The risk profile ten years ago included someone breaking into the bank's computer to get customer records, while the risk profile today is someone breaking into cell phones, laptops, mobile devices, social media sites, merchants who deposit checks via imaging systems, service providers who host critical banking applications, websites which validate flood plains or credit bureau information, etc. This list goes on and on regarding the technologies typical in a SMFI. The next generation of technologies will exponentially increase the risk profile because information and Infrastructure will be further distributed, and not partitioned off by the walls of the bank. Banks leverage Brinks trucks to secure the delivery of cash to their bank. The financial industry needs to devise "cyber Brinks trucks" to perform the same role in cyberspace.

Two major trends will likely drive technology and security over the coming decade. First, the Internet of Things (IoT) is an environment in which objects, animals or people are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. IoT has evolved from the convergence of wireless technologies, micro-electromechanical systems and the Internet. By 2020, there will be a quarter billion connected vehicles on the road, enabling new in-vehicle services and automated driving capabilities, according to Gartner. All cities will (eventually) be smart**.** With more than one-half of the world's population living in cities, innovative new IoT solutions, such as smart parking, connected waste, and traffic management, hold great promise for combatting the major challenges of rapid urbanization. We are unlikely to see many smart cities of the future appearing overnight. However, like in the past with the adoption of revolutionary technologies such as sewers, electricity, traffic lights, and the Internet, mayors will slowly implement IoT solutions to save money, shape the future and make their cities better places to live. We will be trading mobile dollars for IoT pennies**.** It is no wonder that the mobile operators are salivating at the prospect of a windfall of new revenue to be earned from connecting the projected 50 billion devices, or things, to the Internet (today there are approximately 10 billion things connected to the Internet). However, it is not that straightforward. While some of the traffic will flow over mobile networks, the majority of the connections will be made over wireline or unlicensed wireless networks. And, many of the IoT devices require very low bandwidth – simply conveying their status on an occasional basis and then remaining dormant until this status changes. Mobile operators will need to do more than just sell mobile connectivity to inanimate objects to reap the full rewards of IoT. It will be about much more than the "things". The currency of IoT will be "data". But, this new currency only has value if the masses of data can be translated into insights and information which can be converted into concrete actions that will transform businesses, change people's lives and effect social change.

The second major trend is digital currency. While no digital currency will soon dislodge the dollar, Bitcoin (and other digital currencies) are much more than a currency. It is a radically new, decentralized system for managing the way societies exchange value. It is, quite simply, one of the most powerful innovations in finance in 500 years. It's already proven that bitcoin has contributed a lot to the world. For example, PayPal recently urged everyone to use digital currencies in their transactions and predicted that these currencies will be accepted by the majority of the population and establishments in the US within 12 months. However, the shadowy fact remains that bitcoins and digital currencies have been risky. Frustrations have mounted when the price of the Bitcoin came crashing down. Mt. Gox closing down, China banning their use, laws provided by states against it and more – these all contributed to the gradual decline of bitcoin's popularity and price value. The number of attacks involving Bitcoin mining malware tripled: from 360,065 attacks in 2013 to 1,204,987 in 2014. But the reality is these digital currencies are in their infancy and the issues of today will get solved for mass acceptance and use in our economy. Put together with the Internet of Things where 50 billion devices will be connected to the Internet by 2020, it is easy to see how digital currencies could be deployed as the backbone currency in the digital age.

SECTION III. Data Security and Privacy Issues in the Financial Sector and Small Businesses

Over 850 million data records have been breached over the past ten years:

857,702,257 Records
4584 Breaches

How many of these data records and breaches involved the **financial sector**?

349,188,179 Records
608 Breaches

How many of these data records and breaches involved the **retail sector**?

257,514,157 Records
547 Breaches

Note that these numbers from PrivacyRights.org are likely dramatically understated as universal notification laws are not in place and punishment for not disclosing is often not a deterrent. For example, the JP Morgan Chase breach is not accounted for on this site. The breach numbers are likely a fraction of the actual activity that is occurring. It is also interesting to note that healthcare and government (which receive much security attention) have fewer breaches than small businesses and/or retail. Claims that the PCI standard are sufficient seem to be overstated as retail accounts for the highest percentage of data records breached in 2014.

U.S. SMFIs and small and medium-sized entities (SMEs) are important as millions of consumers depend upon community banks, credit unions, accounting firms, tax-preparation firms, investment offices, insurance agencies, and the like. When issues in the financial system exist, confidence erodes and consumers are left paralyzed wondering what to do. The margin for error in SMEs is relatively small, and one such data breach can shut the doors on viable businesses.

Further, if terrorists would target these vulnerable SMFIs or SMEs, they would find a soft underbelly of relatively under-protected targets. A plethora of nefarious activities are then possible, including stealing and selling customer data, extorting ransoms, "owning" the computer, making these systems unavailable, etc. Stated directly, these activities could be enough to put a SME or SMFI out of business. The reality is that, while it is nearly impossible to challenge the importance of SMEs and SMFIs in the U.S., it is equally difficult to convince security experts that either are prepared to protect their critical systems, important customer information and do their part to battle against the war on terror.

The federal government identified banking and finance as a critical infrastructure that requires protection, yet most of the attention is paid to the large financial institutions. SMFIs and SMEs store and transmit much non-public data, with limited resources to fend off a well- equipped, well-funded enemy. A recent survey of bank executives called out this very fact. When asked what their top technology concern was over the next two years, risk management and compliance topped the list. A black market drives insiders and hackers to steal information because of its value. My experience in working in the industry as that the majority of data breaches in SMEs could be easily avoided with basic preventative controls consistently applied. SMFIs and SMEs have a wealth of non-public, sensitive data that cyber thieves are targeting with increasing regularity.

Cyber security is a broad and pervasive issue leading to at least two national issues: critical information protection and identify theft. Critical information protection is guarding our electronic infrastructures as an issue of national security. Incidents are classified, but it is well established that China and others are interested in technology disruptions that affect the United States' ability to conduct commerce. President Obama is on record stating that the United States is not prepared for critical infrastructure protection (CIP) and, despite national budget pressures, the administration created in 2013 a division within the armed forces (U.S. Cyber Command) to begin focusing on this new national issue.

Identity theft remains a fast growing crime in America and the risks of not protecting such information can be catastrophic to SMEs in communities. When identities of good U.S. citizens are stolen by cyber criminals, the good citizen can be humiliated, lack good credit, and spend significant time and money in an attempt to partially restore their good name. Information risk management is the first step in resolving the broad and pervasive issues of CIP and Identity Theft. Public Law 111-24 was signed by the President establishing a Small Business Information Security Task Force to look into the issue.

The Ponemon Institute, an independent research firm which conducts research on privacy, data protection and cyber security, calculates in 2014 businesses paid an average of $230 per compromised record. Consequently, for a small company with 500 compromised customer records, this would amount to $115,000. Companies may keep inactive customers in their database as well, magnifying the number of customers impacted and the resources to manage through a breach. Simply said, a data breach can be so costly that it can put a company out of business or halt expansion plans. This issue is amplified in America where there is very limited information security expertise, offering unprotected businesses as easy targets for organized cyber criminals with financial motivation.

Electronic Crimes in Commercial Banking with Small and Medium-Sized Financial Institutions

Organized cyber-gangs are increasingly preying on small and medium-sized companies in the U.S., setting off a multi-million-dollar online crime wave and grave concerns that critical infrastructure government and business depends upon each day may become compromised. It appears there are three contributing reasons they are growing so fast: (1) Low threat of arrest in foreign-based "safe havens", (2) High payout for the crime, and (3) Victim sharing data on these attacks has been minimal. The attacks are amazingly simple and the amount of money taken, information stolen, or infrastructure compromised is concerning. SMEs do not know how to protect themselves. In some cases where credit card theft has occurred, they have had to shut down because they lost the ability to process credit cards. Small businesses are being affected greatly by poor security practices. It is not a risk issue, but rather an issue of survival.
Cyber criminals view SMEs as easy targets without the resources or knowledge to fend them off or prosecute them if caught. Consequently, cyber criminals are turning their attention to perceived easy targets in America. Identity thieves can cost SMFIs and SMEs their basic ability to stay in business (i.e., financial losses, bad publicity of a data breach, significant costs of recovering from a data breach, inability to process credit cards, etc.). Even if there were no measurable damages to customers, the notification costs alone can put the SME out of business. One-third of companies have said that a significant security breach could put their company out of business. Many SMEs are having a difficult time in this economy, and even the smallest of distractions can be devastating. SMFIs, too, are struggling with increased assessment fees, limited deposits, limited fee-based products, and overwhelming compliance expenses, which is spurring closures and consolidation in the industry.

While SMFIs have struggled to keep pace with hackers, the SMEs have clearly fallen short. In a study I completed of SMEs, 7 out of 10 SMEs lack at least one basic security control, such as a firewall, antivirus software, strong passwords, or basic security awareness for staff. Many SMEs simply lack the basic security most of us expect on our home PCs. As evidence, I provide a statistic. I am founder of Secure Banking Solutions, LLC, a security/ privacy firm focused on information security and compliance for SMFIs. As such, SBS is regularly hired to conduct penetration tests on SMFIs where SBS security personnel run (after authorization) hacking tools to see if they can break into the bank's network and systems. SBS is effective in 24% of SMFIs (meaning that SBS personnel were able to gain access to Information and systems they were not authorized for). To contrast, SBS is effective in 100% of SME penetration tests. The question is "why?" and the answer is simple: SMFIs are regulated to a certain level of security that is far superior to a SME. Most anyone can download hacking tools from the Internet, point them at a SME, and gain unauthorized access, zombie the machine, steal data, or disrupt the environment.

Traditionally, most SMEs have viewed security as a problem faced solely by large organizations, government agencies, or online intensive operations, as large organizations possess large, prolific information targets and are generally more regulated than SMEs. However, cyber criminals are finding easy targets in SMEs that have limited security. The financial gain for cyber thieves targeting SMEs is obviously less than that of large organizations, but they can be hacked in significantly less time with little to no effort. Tools to conduct these attacks on SMEs are freely downloadable from the Internet.

The FBI previously issued an alert to all SMFIs and SMEs of this issue. These attacks are working because of a lack of security controls at the SME whereby fraudulent transactions are directly taken out of commercial customer's bank accounts. The current generation of banking products work because of technology, including remote deposit capture, Internet banking, mobile Banking, item imaging, and on-line account origination. However, USA Today quoted Amrit Williams, a chief technology officer, "Any organization that cannot survive a sudden five- or six-figure loss should consider shunning Internet banking altogether." Banking security analyst at Gartner, Avivah Litan, tells acquaintances that run small businesses to switch from commercial online accounts to an individual consumer account to take advantage of consumer-protection laws under Regulation E. Regulation E protection does not exist for corporate accounts; consequently, SMEs have no legal protection if commercial account fraud occurs. Unlike individual accounts that protect individual consumers to a maximum exposure of $50 if fraud occurs, corporate accounts have no such protection. The SME can sue or go to the media, but these approaches likely do not get the money back and drain even more resources from SMEs, which are typically resource challenged.

New fees levied by financial institutions on paper-based banking products are likely to push more small businesses in to banking online, whether or not they are aware of and prepared for the types of sophisticated cyber-attacks that have cost organizations tens of millions of dollars in recent months. Gartner analysts say banks should not be pushing more businesses into online banking without adequately informing them of the risks. The reality is that the perfect small-business storm is occurring: heaving attacks are already beginning and significantly more technology will be deployed by SMFIs over the next five years, creating a fertile cyber ground for cyber criminals, nation states, and terrorists to create problems.

The latest Business Banking Trust Study provides insights from the SME perspective on the pervasiveness of fraud, the state of security at banks and businesses, and the impact fraud has on businesses' relationships with their banks. The study found:

- 74% of businesses surveyed experienced online fraud;
- 52% of businesses reported experiencing payments fraud or attempted payments fraud in the last 12 months;
- In 72% of fraud cases, banks failed to catch fraud involving the illegal transfer of funds or other nefarious practices such as information identity theft; and
- 70% of SMEs have diminished confidence in their financial institution or take their banking business elsewhere.

More than nine out of ten small business owners in the study cited cybersecurity as a concern. This is not an unfounded fear: Half of them report they've already suffered a cyber-attack, with 61 percent of those attacks taking place in the last 12 months. The National Cyber Security Alliance conducted the National Small Business Security Study with Visa Inc. to analyze small business' cyber security practices and attitudes. Results include:

- 94% of small business owners report being very or somewhat concerned about cyber security; and
- Nearly half of businesses surveyed report they already have been a victim of a cyber-attack.

In summary, there is little doubt that the financial services sector is under attack for identity theft and infrastructure corruption motives. There is also little double that the small and medium-sized businesses and financial institutions are coming in the cross-hairs of cyber criminals. The number and significance of data breaches and attacks is growing, and only a comprehensive approach that looks at all infrastructure holistically (from government, academia, and industry) can ward off these for cyber criminals, nation states, and terrorists.

SECTION IV. Observations and Recommendations

This section outlines several observations and summarizes recommendations to address cybersecurity as a nation, and in both banks and small businesses alike.

CONCERNS

1. Lack of a National Cyber Security Strategy – The lack of regularly updated, comprehensive, bilaterally supported national security strategy is problematic at best. When the President and Congress are on record time and time again declaring the imminent danger the Internet represents, then shouldn't it follow that resources area aligned to this grave danger? The current administration seems to understand the magnitude of the issue but has been remiss to draft a comprehensive strategy to lead our digital infrastructure into a more secure future.
2. Internet of Things and Digital Currencies will Accelerate Internet Traffic and Growth – It is fair to say that we cannot manage the internet environment of today with 10 billion connections and an architecture that doesn't scale well. It took nearly 45 years to get to

these 10 billion connections; yet, by the end of 2020, the Internet will include 50 billion connections. Add to this the use of digital monies (i.e., bitcoin) to settle the transactions and this seems like a perfect storm where cyber criminals will wreak havoc on our electronic systems like we have never seen before. Refer to Appendix A and B for Internet and Internet of Things growth statistics.

3. Cyber War (or Cyber in War) is Imminent – The power grid represents tremendous risk to American citizens as aggressive nation states continue to ready to attack our SCADA infrastructures. While it is foreseeable that a multi-variant attack coordinated across sectors to simultaneously interfere with power, telecommunications, oil/gas and banking infrastructure is plausible, more likely is a single deep rooted attack on a single infrastructure to ingest cyber terror into our citizens' consciousness. It is also plausible that cyber war will lead to kinetic war (or some combination of the two). Specifically, an offensive cyber-attack by a nation on our power infrastructure could be met with a kinetic attack on their nation's physical target (or vice versa).
4. Banking Continues to be the Most Attacked Sector – Based upon volume (number of data records, number of attacks, etc.), the financial sector continues to be the most attacked of our infrastructures. The interconnected nature of this sector has caused the banking regulators to become very concerned about vendor management and corporate account takeover. With the growth of Internet of Things, it is possible that there could be a shift in attention from the hackers; however, it is fair to say that banking and financial services are under attack today and this will likely continue over the next five to ten years.
5. Small Business Security Continues to Lag Behind – Small businesses lack the resources to understand and mitigate these cyber threats. The PCI standards are clearly not working, and for the most part based on voluntary compliance and self-audit. Today, the best mitigation strategy seems to be to educate individuals and SMEs to the risks and controls that are essential to minimize the potential for major cyber loss or disruption. Moreover, we do not think it is appropriate or reasonable to shift the burden of loss from the person or organization that had inadequate controls in place to detect and deter cyber hacking attacks, to the financial institutions that process the withdrawals by the crooks, generally through ACH debits.
6. Information Sharing is Lacking but Improving – The Information Sharing and Analysis Centers (ISACs) were devised over ten years ago, yet it is really only this year that the FS-ISAC is gaining momentum. With the banking regulators getting behind FS-ISAC, banks and credit unions have increased membership rates. The system really only works if many are participating, and we are finally getting to a scale where there is value.
7. Data Breach Notification is Inconsistent – 48 states have data breach notification laws; however, every state law is different. This lack of uniformity makes it difficult to measure breach rates and makes it difficult for the consumer to understand what is going on.
8. Security Awareness (or the lack thereof) is the Number One Issue
    a. Citizens
    b. Business Owners
    c. Investors
    d. Policymakers

e. Executives

A recent study in the banking sector determined that the number one cyber security issue in banking is the reality that senior management and boards are simply not in position to establish “the tone from the top” as it relates to cyber security. They lack the requisite skills to set the direction and manage their organizations to achieve cyber security objectives.

9. The Internet of Today Can Not Be Secured – The Internet was not built for the purpose it carries out today. The Internet was not conceived to become the backbone for commerce. While today countries and companies alike are adopting technologies to grow their interests, the Internet lacks fundamental controls that large-scale networks must have. As the Internet-of-Things explodes over the next ten years and our cyber adversaries grow in both number and strength, the problems of today will seem like child’s play. Infrastructures like the Internet takes years to change because of its pervasive and invasive nature. The time is now to determine how the infrastructure we know today must be secured and/or fundamentally changed so that cyber resources remain available, accurate and private to those who depend upon them for social and economic well-being.
10. Industry Will Continue to Underinvest in Cyber Security Solutions - Digital Infrastructure is Infrastructure. When an ice storm occurs in North Dakota, icing up power lines and taking out power, the region is paralyzed until power is restored. It can sometimes take weeks and months to complete this task, depending upon the tenacity of Mother Nature. What would happen to these financial institutions, our economy, and our consumer confidence level if malicious nation-states disrupted our power instead of an ice storm? How long would it take for power to be restored on power grid infrastructure dating back centuries? Power, water, transportation, and the Internet just to name a few are all required to conduct banking commerce. While SMFIs are required to devise business continuity, incident response, and pandemic prepared ness plans, no SMFI could operate if essential infrastructure we all depend up (such as the power grid) was compromised. The job is much larger than any one SMFI. To the degree major and minor changes are needed at SMFIs or SMEs, we urge the Administration and Congress to consider this infrastructure and fund it. There may need to be discussion about a mindset shift away from industry paying for everything in this infrastructure (because they created it and are the users of it) to some shared cost model. If this infrastructure is truly a matter of national security then the Federal government has a funding responsibility. Just as tanks, planes, and weapons are funded to protect our interests, we urge the Administration to consider their financial responsibilities as it relates to this vital electronic infrastructure.
11. Securing Our Digital Infrastructure Will Take Cooperation and Resources – Nearly 20 critical infrastructures are identified and would take trillions of dollars to “secure”. This resource allocation is likely unreasonable so little will be done to remarkably improve our nation’s cyber security posture.
12. Cyber Security Risk Management Practices are Insufficient – A lack of agreed upon cyber security risk management practices, frameworks, tools, methods, etc. is leading to confusion. Cyber security risk management science is in its infancy, but hacker techniques are sophisticated.
13. There is a National Shortage of Security Experts. Most organizations do not have an

expert who understands the emerging security threats, threat actors, vulnerabilities, and the like, as it takes time and expertise and cannot simply be assigned to existing staff. The large companies and government agencies are "buying" their experts, leaving most of U.S. companies with insufficient expertise. Government, private and public sectors are all facing an enormous shortage in cybersecurity talent. The subject of cybersecurity is showing up in classrooms all over the nation to fill a worldwide shortage of 1 million openings. Symantec, the world's largest security software vendor, recently reported that the demand for the cybersecurity workforce is expected to rise by 6 million professionals globally by 2019, with a projected shortfall of 1.5 million. That will leave companies and information less protected than they should be against hackers. While technology is vital to preventing, detecting and responding to security attacks, equally important are the people who determine security strategy, devise and operationalize security programs, and skillfully deploy the technologies that wall-off our critical infrastructures and information. According to CIO Magazine, cybersecurity professionals report an average salary of $116,000 which is nearly three times the national median income for full-time wage and salary workers, according to the Bureau of Labor Statistics. We need to expand our cyber security workforce.

RECOMMENDATIONS

1. Think through the Global Nature of the Issue – An international group should study the cybersecurity issues and draft a series of issues and recommendations which could feed our National Strategy. The Internet is not a U.S. thing. It is a global infrastructure with global reach and implications.
2. Develop a National Cyber Security Strategy – The Federal Government should work with government, academia, corporate America and the small business community to devise a regularly updated, comprehensive, bilaterally supported national security strategy that includes goals, objectives and funding sources. Establishing a front line of defense against today's immediate threats and to defend again a full spectrum of future threats is so massive that only the Federal government could take this on. Improved awareness needs to be at the center of this strategy.
3. Focus on Power and Telecommunications – while there are many more "critical infrastructures" which need protection, all infrastructures depend upon Power and Telecommunications. Melissa Hathaway, previous Director of the Joint Interagency Cyber Task Force at the Office of the Director of National Intelligence during the George W. Bush administration, mentioned at Harvard's 2015 class entitled, Cybersecurity – The Intersection of Policy and Technology, that these two infrastructures should be the first order of priority protection in the United States and around the world. Funding the improved security of 20 infrastructures has proven impossible, so a strategy to focus resources on power and telecommunications seems reasonable.
4. Pass Cybersecurity Information Sharing Act of 2015 (CISA) – Congress should pass a cybersecurity bill that encourages and incentivizes private companies to share data with the federal government. While the ISACs are improving information sharing, companies are still reluctant to share. A bill that would incentivize the sharing of cybersecurity threat information between the private sector and the government and among private sector entities and responds to the massive and mounting threat to national and economic

security from cyber events is needed. The bill should also look to improve the cyber security of both public and private computer networks by increasing awareness of both threats and countermeasures.

5. Pass Federal Data Breach Notification Law of 2015 – allow for uniform definition and application of data breach policy, while providing exemptions to improve the flexibility to hone the law to meet specific needs. Consistent with the February 5, 2015 testimony of American Bankers Association Senior Vice President Doug Johnson, we support 1) pre-empting inconsistent state laws and regulations in favor of strong Federal data protection and notification standards, 2) strong national data protection and consumer notification standards with effective enforcement provisions, and 3) the costs of a data breach should ultimately be borne by the entity that incurs the breach.
6. Improve grant opportunities and funding for research in cyber security, with an emphasis on risk management practices and security awareness solutions. The National Science Foundation and others could be equipped with the resources to focus on these two very important areas. While cyber security technology-based research funding is available, these two important focus areas should be emphasized. Small Business Innovation Research (SBIR) programs can also look to write these two areas into their solicitations. Applied research should be emphasized.
7. Consider Requiring Cyber Insurance – Organizations which operate a digital capability might need to carry cyber insurance. Many businesses have been resistant to spend money in this area. Congress may consider either 1) requiring a basic level of cyber insurance for those organizations that meet a certain profile, or 2) requiring a specific set of mitigating controls that all organization should implement. Examples are already documented in the SBA Small Business Security Standard and the NIST Small Business Security Standard.
8. Build Upon Existing NSA/DHS Center of Academic Excellence Program (CAE) – This program is a tremendous success story and should be enhanced to include many other audiences (i.e., industry, high schools, veterans, etc.). Scholarships and financial support must be made available to make the cyber security field an attractive career choice to close the gap on the million job shortage we are facing. The CAE program is a huge success and the credit goes to the thought leaders in the federal government that anticipated the cybersecurity issue and the resource shortage it would create. We advise the President and Congress to consider expanding this program with funding, so that more educational, research, and outreach capacity is created to serve the needs of government and industry (companies small and large). We advise the expansion of the Scholarship for Service Program (SFS) at NSA, DoD, and NSF, including expanding the number of scholarships and the places scholarship students can pay back their scholarship. For example, can we make it possible for a SFS student to complete his/her service at a critical infrastructure owned and operated by the private sector such as a power supplier or an Internet Service Provider?
9. Devise More Effective (and Affordable) Cyber Security Training and Educational Programs – Citizens and businesses alike must be trained to run technology securely in this digital age. Making cyber security training and education available and affordable is the key. One such example is the Program in Bank Technology Management that

Kirby Davidson at the Graduate School of Banking at the University of Wisconsin has developed. This Program launched in April, 2011 and was capped at 50 students (which filled in two weeks). The Program is a blend of technology and security honed specifically to the community banking audience. The program includes 12 hours of "ethical hacking", where students download and execute common hacking tools so they understand what tools the adversary has in the arsenal. After the training is completed, they have a better understanding of the adversary and more importantly can return to their businesses and help secure our infrastructure.

Conclusion

Electronic products and delivery systems are the future in banking and beyond, and if businesses cannot understand and resource their technology and security requirements then they will likely be left behind. We agree with the White House's conclusion in their recent cyber security legislative proposal that, at least with respect to cyber terrorists, the vulnerability of the electricity grid poses one of the most severe exposures to our country's critical infrastructure. The fact that a computer Programmer or hacker in another country could cause the partial or complete disruption of this nation's grid is, to say the least, extremely disturbing, but is beyond the scope and expertise of businesses to respond. However, small and medium-sized financial institutions need representation at the table, and we encourage the President and Congress to consider including this voice as small and medium-sized financial institutions and businesses are the majority, not the minority, of America n businesses.

We conclude with this thought. In 2009, President Obama stated:

> *We count on computer networks to deliver our oil and gas, our power and our water. We rely on them for public transportation and air traffic control… Butjust as wefailed in thepast to invest in ourphysical infrastructure – our roads, our bridges and rails – we'vefailed to invest in thesecurity of our digital infrastructure... This status quo isno longer acceptable -not when there's so much at stake. We can and we must do better.*
>
> *Source: President Obama, May 29, 2009*

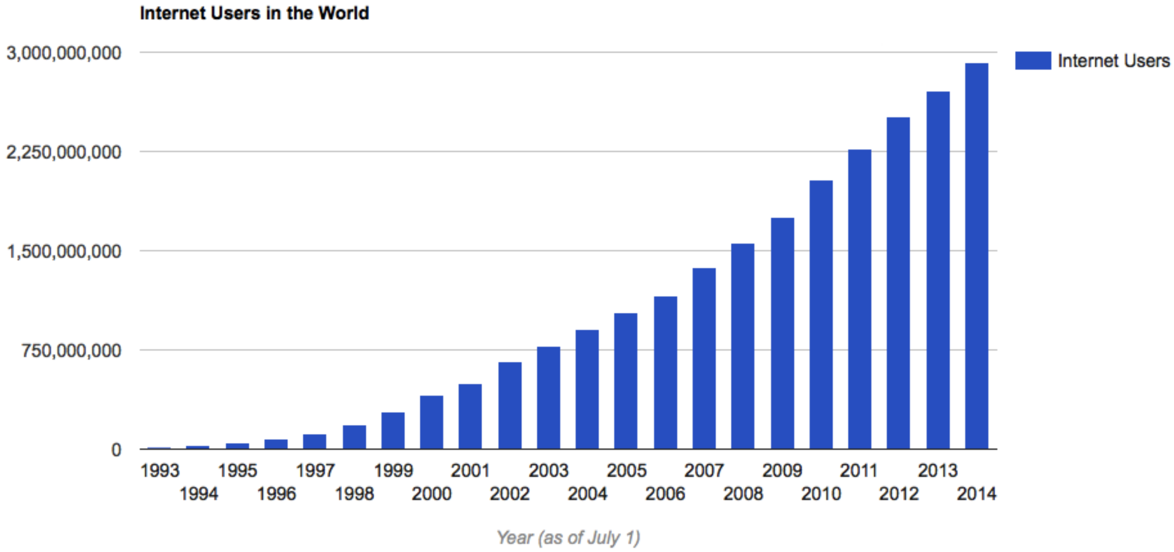
The first question is, “have we made enough progress over the past six years”? No doubt we are improved, but so have the capabilities of our cyber adversaries. With the explosion of the Internet, digital currencies, and the next generation of networked technologies, organizations will become more dependent upon technology to grow their businesses and reach more customers. The second question is, “are we prepared for the future”? Customers will interact with technology even more frequently and intimately than today, and cyber criminals will be more savvy and well-funded than ever before. The risk to our nation is clear that a cyber-terrorist thousands of miles away can hold a citizen, organization or country hostage with binary attacks. When this happens, it is not simply Microsoft or Oracle who must respond. We need a strategy that focuses resources, builds capabilities in the areas we need, informs consumers and business leaders of their responsibilities, promotes information sharing and customer notification, and builds the cyber workforce of tomorrow.

Chairman Thune, Ranking Member Nelson and Members of the Senate Committee on

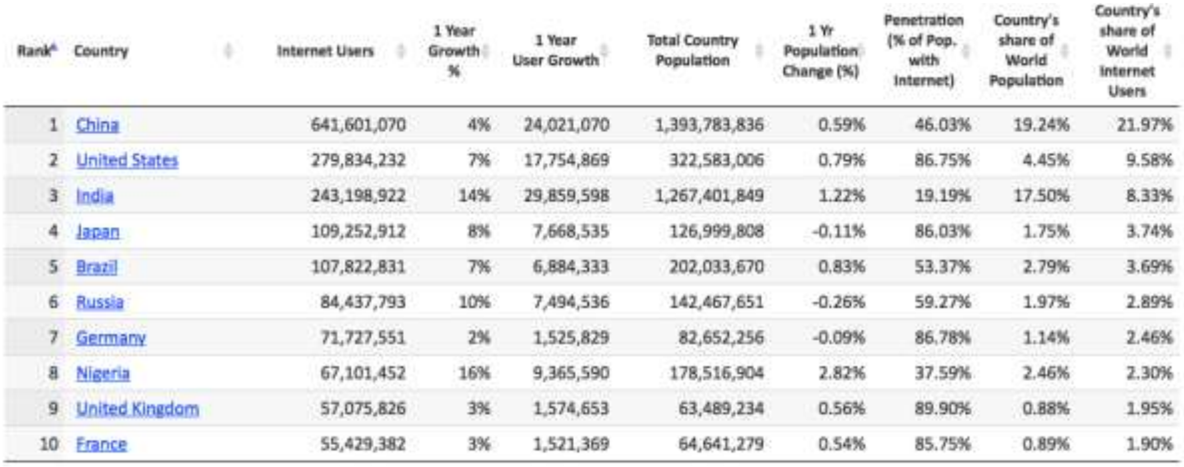
Commerce, Science, and Transportation, thank you for the opportunity to participate in this important and timely hearing. Dakota State University looks forward to working with all stakeholders to improve the security of the electronic infrastructure all businesses and Americans use. We applaud the President and Congress for making cybersecurity a priority, and concur with the President's comments that the "cyber threat is one of the most serious economic and national security challenges we face as a nation”.

We want to thank you again for your leadership and this opportunity to appear before you.

Appendix A
Growth of the Internet



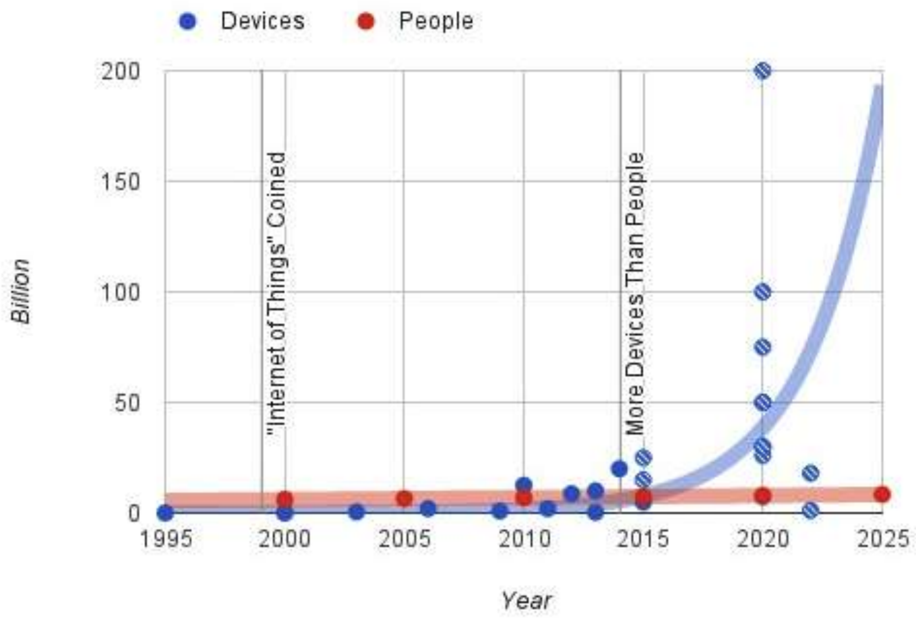
-



Rank	Country	Internet Users	1 Year Growth %	1 Year User Growth	Total Country Population	1 Yr Population Change (%)	Penetration (% of Pop. with Internet)	Country's share of World Population	Country's share of World Internet Users
1	China	641,601,070	4%	24,021,070	1,393,783,836	0.59%	46.03%	19.24%	21.97%
2	United States	279,834,232	7%	17,754,869	322,583,006	0.79%	86.75%	4.45%	9.58%
3	India	243,198,922	14%	29,859,598	1,267,401,849	1.22%	19.19%	17.50%	8.33%
4	Japan	109,252,912	8%	7,668,535	126,999,808	-0.11%	86.03%	1.75%	3.74%
5	Brazil	107,822,831	7%	6,884,333	202,033,670	0.83%	53.37%	2.79%	3.69%
6	Russia	84,437,793	10%	7,494,536	142,467,651	-0.26%	59.27%	1.97%	2.89%
7	Germany	71,727,551	2%	1,525,829	82,652,256	-0.09%	86.78%	1.14%	2.46%
8	Nigeria	67,101,452	16%	9,365,590	178,516,904	2.82%	37.59%	2.46%	2.30%
9	United Kingdom	57,075,826	3%	1,574,653	63,489,234	0.56%	89.90%	0.88%	1.95%
10	France	55,429,382	3%	1,521,369	64,641,279	0.54%	85.75%	0.89%	1.90%

Appendix B
Growth of Internet of Things

How big is the Internet of Things?



Source: Author's calculations based on data from ABI Research (2013), Business Insider (2013), Cisco (2013, 2015), EMC (2014), Ericsson (2011), Forbes (2013), Gartner (2013), Hammersmith Group (2010), Intel (2014), Internet Census (2012), Internet World Stats (multiple), Machina Research (2013), Navigant Research (2013).