The Software Alliance

BSA

Hearing on

"Examining the Current Data Security and Breach Notification Regulatory Regime"

House Committee on Financial Services
Subcommittee on Financial Institutions and Consumer Credit

February 14, 2018, at 10:00 a.m.
Rayburn House Office Building
Room 2128
Washington, DC

Testimony of Aaron Cooper
Vice President, Global Policy
BSA | The Software Alliance

Testimony of Aaron Cooper

Vice President, Global Policy, BSA | The Software Alliance

Hearing on "Examining the Current Data Security and

Breach Notification Regulatory Regime"

February 14, 2018

Washington, DC

Good morning Chairman Luetkemeyer, Ranking Member Clay, and distinguished members of the Subcommittee. My name is Aaron Cooper, and I am Vice President for Global Policy of BSA | The Software Alliance.

BSA is the leading advocate for the global software industry in the United States and around the world.[1] Our members are at the forefront of the development of cutting-edge cloud-enabled data services that have a significant impact on U.S. job creation and the global economy. I commend the Subcommittee for holding a hearing on this important topic, and I thank you for the opportunity to testify on behalf of BSA.

BSA has for more than a decade supported Congressional action to establish a federal standard for data security and data breach notification. The need for a national standard is now more urgent than ever. The steady drumbeat of high profile security incidents that expose consumers to heightened risks of identity theft threatens to undermine public trust in the digital economy.

Federal legislation can play an important role in restoring that trust by setting expectations for good data stewardship, ensuring consumers receive timely and meaningful notification about security risks, and reducing the complexity of compliance in the aftermath of a breach.

The time to act is now. The need is clear, as are the solutions. We urge you to pass a data security and data breach notification bill this Session.

I. Growth of the Digital Economy

Over the last 20 years, consumers, businesses and governments around the world have moved online to conduct business, and access and share information. This shift to a digital world has transformed commerce, helping companies enter new markets and compete on a global scale. It has delivered unprecedented efficiencies and considerable cost savings to every industry sector.

[1] BSA's members include: Adobe, ANSYS, Apple, Autodesk, Bentley Systems, Box, CA Technologies, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Microsoft, Okta, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, Trimble Solutions Corporation, The MathWorks, Trend Micro and Workday.

The software industry, and BSA members in particular, are at the forefront of the development of cutting-edge technologies and services that are driving the digital economy, such as predictive analytics, cloud computing, AI, and blockchain technologies. These technologies spur job creation and economic growth, provide significant benefits to businesses, and improve the quality of life for many Americans, as well as people around the globe. These benefits will grow substantially in the coming years.

Last September, Software.org: The BSA Foundation released a study with data from the Economist Intelligence Unit (EIU) that showed the software industry alone contributed more than $1.14 trillion to the U.S. GDP in 2016—a $70 billion increase in the past two years.[2] The study also showed that the software industry is a powerful job creator, supporting over 10.5 million jobs, with a significant impact on job and economic growth in each of the 50 states.

Our economy today—and economic growth and job creation in the foreseeable future—are rooted in digital data. The dropping costs of data storage, alongside the acceleration of data driven innovation by BSA member companies and others, have led to profound new uses of data by enterprises across the economy. Every industry today is improved through the use of software.

In every industry, the analysis of data has made businesses more agile, responsive, and competitive, boosting the underlying productivity of many key pillars of our economy. The economic implications of this software and data innovation are enormous. Economists predict that making better use of data could lead to a "data dividend" of $1.6 trillion in the next four years, and that data-enabled efficiency gains could add almost $15 trillion to global GDP by 2030.[3]

II. The Size and Nature of the Challenge

The public's embrace of the digital economy cannot be taken for granted. Ensuring that customers have faith in the security and privacy of their personal data is vital to ensuring their trust in digital services. And, if consumers do not trust technology, they will not use it.

Unfortunately, the spate of recent high-profile security incidents threatens to erode that trust. These concerns are not just theoretical. In fact, a 2017 Pew Research Center study found that nearly two-thirds of Americans (64%) have personally been affected by a major data breach, and nearly half of all Americans (49%) now feel that their personal information has become less secure in recent years.[4]

[2] Software.org: The BSA Foundation, *The Growing $1 Trillion Economic Impact of Software* 5 (Sept. 2017), *available at* https://software.org/wp-content/uploads/2017_Software_Economic_Impact_Report.pdf

[3] *See* BSA | The Software Alliance, *What's the Big Deal with Data?*, 14 (Oct. 2015), available at http://data.bsa.org/wp-content/uploads/2015/12/bsadatastudy_en.pdf

[4] Kenneth Olmstead and Aaron Smith, *Americans and Cybersecurity,* Pew Research Center (Jan. 26, 2017), available at www.pewinternet.org/2017/01/26/americans-and-cybersecurity/.

Over the past several years, there has been an increase in significant security breaches. The numbers are sobering:

- Symantec estimates that more than 7 billion identities have been exposed in data breaches over the last 9 years.[5]
- A 2017 Ponemon-IBM Security study indicates that the average cost for a company that experiences a data breach is now $7.35 million, up 5% from the prior year, and nearly twice as expensive as the global average ($3.62 million).[6]
- The costs associated with notifying consumers in the aftermath of a breach is just the beginning. The average cost to US enterprises that are the victims of cybercrime now exceeds $20 million per year.[7] Experts forecast that the global cost of cybercrime will eclipse $6 trillion per year by 2021, surpassing the global drug trade and equivalent to nearly half of today's US GDP.[8]
- Consumers also bear the considerable costs of cybercrime. In just the last year, more than 978 million individuals were the victims of cybercrime at an average cost of more than $140 per incident.[9]
- In light of these costs, perhaps the most staggering figure is that experts suggest that 93% of all data breaches are preventable through basic cyber hygiene.[10]

III. Anatomy of a Data Breach

Not long ago, the primary threats to security online were vandals and amateur hackers. They chased notoriety and relished the challenge of defeating security systems. Their calling cards were breaches and denial of service attacks to bring down or deface popular websites. While these problems persist, the stakes are now much greater. The threats are now global, the adversaries increasingly sophisticated, and the motivations far more complicated.

According to the most recent data, insider threats, of both the malicious and careless varieties, continue to account for about one-quarter of all breaches.[11] Breaches involving insiders run the gamut – from the innocent loss of a laptop filled with unencrypted customer data to the outright theft and sale of proprietary corporate data to unauthorized third-parties.

[5] Symantec, *Internet Security Threat Report* (April 2017) at pg. 45, available at https://digitalhubshare.symantec.com/content/dam/Atlantis/campaigns-and-launches/FY17/Threat%20Protection/ISTR22_Main-FINAL-JUN8.pdf?aid=elq_ .

[6] Ponemon -IBM Security, *2017 Cost of Data Breach Study*, available at https://www.ibm.com/security/data-breach

[7] Ponemon-Accenture*, 2017 Cost of Cyber Crime Study*, https://www.accenture.com/t20171006T095146Z__w__/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf#zoom=50

[8] Cybersecurity Ventures, 2017 Cybercrime Report, available at https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf

[9] Norton by Symantec, *2017 Norton Cyber Security Insights Report Global Results*, https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf

[10] Online Trust Alliance, Cyber Incident & Breach Trends Report (January 2018), available at https://otalliance.org/system/files/files/initiative/documents/ota_cyber_incident_trends_report_jan2018.pdf

[11] 2017 Verizon Data Breach Investigations Report at pg. 3, available at www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_en_xg.pdf

Enterprises must also defend against external threats from actors who leverage the interconnectedness and anonymity of the Internet to commit financially motivated crimes and other forms of espionage. Cybercriminals often use socially engineered spear phishing attacks to lure employees into clicking on links or attachments that infect the organization with malware, or they leverage unpatched vulnerabilities as an initial access point into the targeted network. In their most extreme form, often referred to as "advanced persistent threats," these adversaries can burrow into a victim's network for months, or even years, surreptitiously extracting high value data in a manner that is almost impossible to detect. These so-called APTs are conducted by well-resourced teams of specialists that often are linked to nation state actors.

Despite the variety of threat actors, there remains a high degree of overlap in terms of the tactics that give rise to most data breaches. According to the 2017 Verizon Data Breach Report, an astonishing 81% of hacking-related breaches relied upon compromised and/or weak user credentials.[12] Unpatched software is another common vector of attack, with one study concluding that timely patching could prevent nearly 80% of security incidents.[13]

IV. Business Response to the Data Security Challenge

Organizations that hold sensitive data need to incorporate high standards of risk management. This does not always require adopting extraordinary, excessively costly or particularly cumbersome security measures. In fact, reasonable diligence could make a considerable dent into this problem.

For instance, adoption of robust identity management and access control measures could help to address the 81% of hacking-related breaches that rely on compromised user credentials as the vector of attack.[14] Likewise, adoption of transparent and verifiable software asset management (SAM) practices would help enterprises remain aware of product updates and security alerts that require timely patching to lock-down known vulnerabilities.[15] More effective use of encryption could also greatly mitigate the impact of many data breaches when they occur.[16]

For its part, the technology industry has important responsibilities to respond to this, and BSA's members are leading on several important efforts.

[12] Id.

[13] Rob Lemos, *Software Patches Could Prevent Most Breaches, Study Finds* (March 2017), available at www.eweek.com/security/software-patches-could-prevent-most-breaches-study-finds.

[14] Mordecai Rosen, *Cybersecurity Executive Order Targets Two Common Attack Vectors* (May 2017), available at https://www.ca.com/en/blog-highlight/cybersecurity-executive-order-targets-two-common-attack-vectors.html.

[15] Ashley Gatehouse, *What is the Role of SAM in Protecting against Network Breahces?* (September 2015) available at https://blog.crayon.com/what-is-the-role-of-sam-in-protecting-against-network-breaches/ ("[S]oftware asset management can be used to validate that software is patched and updated regularly. These patches fix security vulnerabilities that software has. If it is unpatched an organization should consider it unsafe. According to the Verizon Data Breach Investigations Report (DBIR) for 2015, 99.9% of the exploited vulnerabilities were compromised more than a year after the common vulnerabilities and exposures (CVE) was published.")

[16] Rick Robinson, *The Impact of a Data Breach Can Be Minimized Through Encryption* (October 2014), available at https://securityintelligence.com/the-impact-of-a-data-breach-can-be-minimized-through-encryption/

First, BSA recently released a "Cybersecurity Agenda for the Connected Age."[17] This cybersecurity agenda addresses five important pillars:

1. promoting a secure software ecosystem
2. strengthening government's approach to cybersecurity
3. supporting international standards
4. developing a 21st Century cyber workforce, and
5. embracing emerging technologies.

Each of these pillars includes more specific policy recommendations, many of which are key to minimizing the risk of data breaches. They include developing an industry software security benchmark, strengthening identity management, promoting security research and vulnerability management, providing incentives to adopt the NIST Framework, and targeting investments in emerging technologies to enhance security.

Second, BSA members have been leading advocates of "security-by-design" principles and secure development lifecycle approaches to developing software. This is consistent with the Administration's recent draft "Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats," which highlights that the technology industry should develop and adopt better tools for building security into the design and development of information technology products, systems and services. Broader adoption of these approaches is critical to defending against the vulnerabilities malicious actors exploit in attacks, including those leading to breaches of personal information. Encouraging broader adoption of security-by-design principles and secure development lifecycle approaches, including by emphasizing them with software developers as well as organizations evaluating software suppliers, can pay significant long-term dividends in defending against data breaches. BSA recently suggested that future versions of the NIST *Framework for Improving Critical Infrastructure Cybersecurity*, include such guidance for organizations evaluating software suppliers.

Third, the technology industry must prioritize the development and adoption of more sophisticated tools for managing risks to sensitive networks, including technologies for advanced identity management and authentication, continuous monitoring, data loss prevention, analytics-driven security information and event management, and other emerging approaches to security. BSA members are global leaders in this area. Customers in every industry sector rely on BSA members for innovative solutions that provide layered defenses – from protection at the data and document level to the network and perimeter level – that are adapted to the threats they face and the value of the assets they need to protect.

Fourth, the adoption of cloud-based services and technologies offers another important path for organizations to meet the data security challenge. Cloud computing allows organizations of all sizes to leverage the economies of scale that emerge when computing resources are pooled and the overhead costs associated with the management and maintenance of those resource shared between multiple users. These economies of scale often make cloud computing cheaper and more efficient than the traditional on-premises model. Perhaps most importantly, cloud computing can also be a more secure

[17] BSA | The Software Alliance, *A Cybersecurity Agenda for the Connected Age*, available at http://www.bsa.org/~/media/Files/Policy/BSA_2017CybersecurityAgenda.pdf

option for many enterprises. Just as a bank can better protect the individual financial assets of its patrons, cloud service providers can provide a level of protection for their customers' digital assets that exceeds what most individual companies can efficiently provide on their own. Small and medium-sized enterprises (SMEs) are often unable to invest in significant cybersecurity expertise. Cloud services can help SMEs maintain world-class security while remaining nimble.

Common security features of cloud services include:

- ***Physical Security:*** Certified personnel carefully monitor servers 24/7 to prevent physical breaches. Access to servers protected by systems requiring multifactor authentication (e.g., biometric) and monitored using motion sensors and video surveillance.
- ***Data Security:*** Data integrity ensured through use of state of the art encryption protocols for data at-rest and in-transit. Redundant backups of data in geographically dispersed data centers mitigates risk of loss in the event of power outage or natural disaster.
- ***Advanced Threat Detection:*** Access to enhanced security intelligence leveraged to track, prevent and mitigate the risks of cyber threats. Regular penetration testing to simulate real-world attacks and evaluate security protocols against emerging threats.
- ***Automated Patch Deployment:*** Automated updating of network security protocols to protect systems from newly identified vulnerabilities.
- ***Incident Management and Response:*** Cloud service providers maintain global teams of incident response professionals to respond and mitigate the effects of attacks and malicious activity.
- ***Enhanced Administrative Controls:*** Importantly, customers remain firmly in control of their own data and can establish access and use policies tailored to their organization's needs and regulatory profile. Customers retain control over the data location, encryption key management, and data retention/destruction policies. At the same time, cloud service providers also ensure that the storage of customer data complies with applicable international, regional and industry-specific compliance standards.

While cloud services offer significant opportunities for enterprises to improve their cybersecurity posture, it is important to remember that the responsibility for safeguarding customer data does not end when it is placed onto cloud infrastructure. Indeed, there is no "set it and forget it" cloud security model. Regardless of the cloud deployment model, security remains a shared responsibility for both the cloud provider and the tenant.[18]

V. The Role of Federal Legislation

Federal legislation can improve consumer trust in the digital economy by establishing expectations for data stewardship that will reduce the risk of future breaches and ensure that consumers receive timely and meaningful information when their personal information is compromised. A uniform national framework would benefit businesses and consumers alike. It would replace the patchwork of state laws that are now creating confusion and difficulties, allowing businesses to focus their resources on incident response rather than unraveling the current thicket of compliance requirements.

In BSA's view, the value of a federal standard should be measured against three goals:

[18] Microsoft, *Shared Responsibilities for Cloud Computing* (April 2017), available at https://gallery.technet.microsoft.com/Shared-Responsibilities-81d0ff91

1. Minimizing the risk of data breaches;
2. Mitigating the impact of breaches when they do occur; and,
3. Reducing the complexity of compliance.

1. Minimizing the Risk of Data Breaches: Reasonable Data Security Safeguards

Federal legislation should promote better risk-management practices by requiring companies that collect or maintain sensitive personal information to implement reasonable data security practices. The practices should be scoped and sized to the complexity, sensitivity, and volume of personal information on a company's systems, and the nature and scope of its business activities.

It is particularly important to avoid imposing technology mandates, which can undermine strong data security by foreclosing innovative and adaptive approaches to combatting evolving threats. Organizations must be able to deploy appropriate and cutting-edge security measures and technologies to protect themselves and their customers' sensitive data effectively against current and future threats. This would not be possible if the law mandated the use of specific products or technologies. Laws and regulations should focus instead on requiring the implementation of reasonable and appropriate security measures. To the extent specific data security practices are required, they should be technologically neutral and outcome-oriented. To provide consumers and enterprises with added certainty, the Committee should consider whether to provide a safe harbor, or presumption of compliance, for organizations that comply with recognized industry standards for data security risk management.

2. Mitigating the Impact of Breaches: Timely and Meaningful Notification

Because there is no such thing as perfect security, the risk of potential data breaches can never be entirely eliminated. Federal legislation should therefore ensure that consumers receive timely and meaningful notification when data breaches do occur. The notification standard should be risk-based, ensuring consumers receive actionable information that enables them to mitigate the potential impact of data breaches that create risks of identity theft or financial fraud. The standard should also promote good data storage practices by clarifying that data rendered indecipherable to unauthorized entities through use of encryption or other obfuscation technologies does not create such risks.

To ensure that the information consumers receive is meaningful, the notification standard should encourage companies that have experienced a breach to focus their immediate resources on performing a thorough risk assessment and restoring the integrity of potentially compromised systems. Affording companies a reasonable time frame for such efforts helps prevent additional collateral damage and ensures that affected consumers receive the information they need protect themselves from identity theft and financial fraud.

Finally, consumers should generally expect to receive notification from the organization with whom they have a direct relationship. Such a principle promotes good data stewardship, ensuring that entities who collect personal information take a life cycle approach to managing the associated privacy and security risks.

3. *Reducing the Complexity of Compliance: Preemption and Meaningful Enforcement*

In 2003, California became the first state to enact data breach legislation. Variations of data breach legislation have since been enacted by 47 other states, the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands, creating a patchwork of 52 data breach notification standards that is complicated for businesses and confusing for customers. The variations between the state laws are not trivial. In fact, many states include unique requirements on fundamental issues, including what is considered "personal information," the particular circumstances that trigger the notification obligation, the appropriate method for communicating notices to affected individuals, the required content of those notifications, and even who must be notified and on what timeline.

In the aftermath of a potential security breach, the thicket of state laws creates perverse incentives. At a time when organizations should be singularly focused on remediation, the patchwork of state laws forces them to divert resources to evaluating their obligations under 52 different standards. Federal legislation can help clarify and improve the process and allow industry to do what it does best – focus on improving the security of online systems to prevent future attacks and diminish the harm of any actual breach.

The effort to streamline compliance must be coupled with meaningful enforcement mechanisms. A federal standard should ensure that vigorous enforcement can take place to defend consumers against businesses that fail to provide fair protection of sensitive personal data, without interfering with legitimate businesses. The FTC has a strong track record in that respect. We also support the inclusion of state Attorneys General as enforcers when the FTC has not acted. Enforcement by state Attorneys General in federal courts is an important force multiplier that will improve consistency in the application of the federal standard throughout the country.

VI. <u>The Path Forward</u>

The breach of Equifax last year, which exposed personally identifiable information of roughly 145.5 million Americans, served as a wake-up call about the scope and risk of malicious cyber activity. BSA's members are engaged in daily combat to defend consumers, businesses, and government agencies against these malicious actors, from developing innovative new security technologies to maintaining robust real-time monitoring and intervention against threats. As cybersecurity threats grow increasingly dangerous, it is critical that we establish rational, collaborative approaches to protecting the interests of affected stakeholders to include individual consumers. A uniform federal data breach standard will decrease uncertainty and facilitate rapid and robust responses to significant security incidents; federal guidance on data security will drive stronger security measures across the Internet ecosystem. BSA strongly supports these goals, and we look forward to working with the Subcommittee to achieve them.