Securing Consumers' Credit Data in the Age of Digital Commerce

U.S. House of Representatives Committee on Energy and Commerce
Subcommittee on Digital Commerce and Consumer Protection

Testimony of James Norton
Founder and President, Play-Action Strategies LLC

November 1, 2017

Introduction

Chairman Latta, Ranking Member Schakowsky, and members of the Subcommittee, thank you very much for inviting me to testify before you today.

My name is James Norton, and I am the founder and president of Play-Action Strategies LLC, a homeland security and cybersecurity consulting firm here in Washington, D.C. Previously, I served in several positions at the Department of Homeland Security ("DHS") under President George W. Bush, including as Deputy Assistant Secretary of Legislative Affairs. During the stand up of DHS, I was deeply engaged in the creation of the Department's first team dedicated to confronting the then-nascent cybersecurity threat. After my service at DHS, I continued to work extensively on cybersecurity issues, both in my consultancy and as an adjunct faculty member at Johns Hopkins University's Zanvyl Krieger School of Arts and Sciences Advanced Academic Programs, where I teach courses on homeland security, cybersecurity policy, and congressional affairs. To be clear however, today I am expressing my personal views. I am appearing in my individual capacity and not as a representative of any company or organization.

In early October, this Subcommittee held a hearing to examine the recent Equifax data breach that exposed the potentially sensitive information of more than 140 million Americans. I applaud the Subcommittee for convening this subsequent

hearing to discuss how – given what we know now – we can work together to better protect personal information that is in the hands of credit reporting agencies (CRAs) and other consumer institutions. My testimony will focus on how attacks like the one that led to the Equifax breach fit into the larger cybersecurity context and what can be done to strengthen cybersecurity protections on the front end.

Current Landscape

Today, cybersecurity threats are pervasive, and any company or institution that houses large amounts of personal data is a potential target. Each year, hackers and other bad actors launch millions of attacks on cyber infrastructure maintained by governments, businesses, and individuals. One analysis estimates that the impact of cybercrime will cost $6 trillion annually by 2021, including "damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm."[1]

Current cyber threats take many forms and target a range of vulnerabilities, increasing the complexity of the cybersecurity mission. Attackers may leverage existing software vulnerabilities to gain access to data – as happened in the Equifax attack, they may use "spear phishing" or other means to introduce malware that will infect a computer or network, ransomware can lock individual user data until a "ransom" is paid and the information unlocked by the attackers, and increasingly, bad actors are perpetrating denial of service attacks intended to massively disrupt

[1] 2017 Cybercrime Report, Cybersecurity Ventures, October 19, 2017

web service. Along with multiple types of attacks, the profusion of networked devices offers bad actors multiple entry points to perpetrate attacks. The complexity of the cyber threat landscape, and the speed with which new threats evolve, represents one of the greatest challenges facing officials, businesses, and consumers is the rapidly changing cyber threat landscape. Attacks like the Equifax breach, the WannaCry ransomware attack, and the Yahoo breach in 2013-14 are more widespread and complex than earlier intrusions, demonstrating that bad actors are becoming more sophisticated in their efforts. So far, cybersecurity protections have largely failed to keep pace.

The private sector's cybersecurity problems cannot be blamed solely, or even mostly, on a lack of federal regulation. Instead, a root cause of the problems is a failure of organizations, private sector and governmental, to establish a culture of cybersecurity awareness. Organizations should not assume that employees understand cybersecurity and, as such, must be diligent about training employees on their role in keeping information protected — with an emphasis on recognizing phishing and spear phishing emails that are designed to trick them into giving away credentials or installing malware. Training should also cover smart social media practices, ground rules for downloading software, and the importance of strong passwords. Beyond formal training sessions, talking about security regularly at staff meetings, encouraging workers to think about security at the front end of projects, and displaying policies and tips around the office can help build a cybersecurity culture.

Federal Role

While the federal government has an important role to play in supporting private sector cybersecurity efforts and protecting consumer information, it is important to acknowledge that the government is still working to secure its own systems – for example, I recently testified in front of the House Science, Space, and Technology Committee regarding the issues surrounding the federal government's use of Kaspersky software. While security frameworks like those laid out in the Gramm-Leach-Bliley Act (GLBA) and the Fair Credit Reporting Act (FCRA) are important guideposts and should be maintained, federal lawmakers should resist the temptation to put in place rules or regulations that require companies and institutions to take specific, federally-prescribed actions to address cybersecurity issues, resulting in limited flexibility for private sector companies to respond to emerging threats. In other contexts, we have seen critical infrastructure sectors struggle to balance the implementation of federal requirements with emerging threats, with a notable example being airport security. Creating restrictive cybersecurity requirements would likely have an adverse impact on the marketplace, and any specific steps developed now would likely become quickly obsolete.

Instead, federal lawmakers and officials should commit themselves to working collaboratively with businesses and consumers to share best practices and raise awareness about the scope and sophistication of cyber threats. Many of the cybersecurity challenges faced by companies and consumers are a direct result of a lack of knowledge and resources; as the Equifax breach demonstrates, our cybersecurity posture largely remains reactive, rather than proactive. Those of us

who follow cybersecurity issues have long wondered when the tipping point will be reached. That is, when does the cyber threat become real and tangible enough for us to stop being reactionary and finally dedicate sufficient resources and talent to get ahead of it? I believe that moment is now.

Recommendations

- The federal government should take the lead in convening relevant stakeholders to develop and share best practices, including an examination of how efforts currently underway within the federal government and in the private sector can be adapted for applications in other sectors. In order to expedite the flow of information, the government should consider innovative solutions, potentially including the expansion of existing exchange programs that allow federal employees work on-site with private cybersecurity companies and specialists from those companies work with agency and department personnel to strengthen their cybersecurity infrastructure.
- Government officials and private sector leaders must make a more concerted effort to ensure that consumers (and even other businesses, especially small business owners) are aware of the threats and the tools that are publicly available in the market place to reduce vulnerability. Comparatively simple steps – like regularly changing passwords and ensuring that security software is up to date – can meaningfully reduce the vulnerability of individual devices to cyber attacks. In addition, consumers can take common sense steps, like regularly monitoring their credit reports, to ensure they are

aware of any irregularities that may indicate an intrusion. Finally, federal, state, and local officials can work together to ensure that individuals impacted by cyber attacks know the process for responding, based on the type of attack and what information may have been compromised – financial, medical, etc.