Inside Counsel
JANUARY 20, 2017
BUSINESS INSIGHTS FOR THE LEGAL PROFESSIONAL

An ALM Website
www.insidecounsel.com

BY JUSTIN HECTUS

The Presidential Cybersecurity Handoff

An analysis of the current federal cyber landscape may yield insights into how the next administration might prioritize their approach on this important front.

Reasonable minds can disagree on politics, but every professional reading this piece will likely agree on two things:

Donald Trump. (Photo: Shutterstock)

1) the President of the United States has an extremely difficult job; and

2) there are few challenges for our country less understood and developing more rapidly than cybersecurity and data privacy.

Given the pending change in administration and uncertainty around President-elect Trump's priorities on cybersecurity, an analysis of the current federal cyber landscape may yield insights into how the next administration might prioritize their approach on this important front.

Cybersecurity During the Obama Years

The federal government's track record on cybersecurity and privacy concerns during the Obama administration was mixed. Over the course of eight years, the federal government had to deal with the Snowden leaks, the FBI and DOJ's standoff with Apple over device encryption, and major breaches that exposed 26 million total combined records from the IRS, the Office of Personnel Management (OPM) and law enforcement.

Many of those leaked records reportedly contained highly sensitive data, and the OPM's loss of complete dossiers and fingerprints of millions of applicants for security clearances highlighted that even the most powerful government in the world is vulnerable to cyberattacks.

Privacy and data security legislation was introduced in multiple forms in Congress but to mixed reaction and little progress. The White House pushed for the creation of a Consumer Privacy Bill of Rights Act in 2012 and again in 2015, but the idea did not gain traction in Congress. President Obama expressed support for Congressman Jim Langevin's (D-RI) Personal Data Notification and Protection Act (H.R. 1704, 114th Congress) in March 2015, but the bill never made it out of the Republican controlled subcommittee.

The Cybersecurity Information Sharing Act (CISA) was finally passed after years of false starts in Congress as a part of a larger spending bill in December 2015 and is currently being enacted.

Going back to the George W. Bush presidency, the number and scale of breaches and lost consumer data has increased dramatically year-over-year. Congress is still struggling to understand the complexities and evolving nature of cybersecurity, notwithstanding bipartisan and nonpartisan efforts to elevate the conversation and debate.

Despite the increase in attacks, the U.S. military's overall cyber capabilities have been enhanced significantly since the U.S. Cyber Command was created in 2009. The recently passed defense spending authorization and short-term federal funding measure include provisions to elevate Cyber Command to a full, separate combatant unit and to increase overall government spending on cybersecurity by 35%. The federal government is also on pace to meet the goal it set in 2014 to triple its cybersecurity staff by the end of this year.

President-elect Trump on Cyber Issues

President-elect Trump's public stance on these issues has been similarly mixed. His odd commentary on hackers in one of the debates made headlines, but he quickly followed with a detailed speech outlining immediate actions he would support on cybersecurity.

His position on the issue, per his campaign website, is limited to 169 words and light on details, but he does reference his intention to "protect our vital infrastructure from cyber-attack" as part of one of 10 legislative measures that make up an ambitious agenda in his 100-day action plan.

During the campaign, then-candidate Trump weighed in briefly on privacy issues, calling for a boycott of Apple during their fight with the FBI, voicing support for the reinstatement of the NSA's bulk phone metadata collection program, and implying that self-exiled NSA whistleblower Edward Snowden should face execution.

Looking to his business dealings, Trump's hotel chain, like many other public and private entities, suffered a breach in 2014 and was fined $50,000 for delayed notification of customers in the loss of more than 70,000 guest credit card numbers and other personal information.

His golf resort in Aberdeenshire, Scotland also acknowledged failure to comply with UK data protection laws as a result of what it deemed a clerical error. However, it is not clear how much involvement the President-elect may have had in cyber related decisions around his business global business dealings.

The Handoff

On Jan. 20, 2017, Donald Trump will be sworn in as President, and the opportunity for his administration to shape cybersecurity and privacy policy will begin. The President-elect and his team will not have to start from scratch.

There is currently no shortage of recommendations and guidance on these issues; the most comprehensive and timely source of which is the Dec. 1, 2016 report from the Commission on Enhancing National Cybersecurity (the Commission), an initiative set in motion by President Obama's Executive Order in February 2016.

The bipartisan Commission was made up of experts from the military, technology, legal and academic sectors, and they provided detailed and actionable recommendations for "securing and growing the digital economy by strengthening cybersecurity in the public and private sectors."

The report reads like a high-level playbook and stresses the critical importance of immediate action and increased funding. In a sobering note highlighting the lopsided state of play in cyber defense, the report reminds us "a security team has to protect thousands of devices while a malicious actor needs to gain access to only one. The cost to attack a system is only a fraction of the cost to defend it."

The report's six imperatives, which ended up being much more expansive than the cybersecurity mandate, include:

1. Protect, Defend, and Secure Today's Information Infrastructure and Digital Networks.
2. Innovate and Accelerate Investment for the Security and Growth of Digital Networks and the Digital Economy.
3. Prepare Consumers to Thrive in a Digital Age.
4. Build Cybersecurity Workforce Capabilities.
5. Better Equip Government to Function Effectively and Securely in the Digital Age.
6. Ensure an Open, Fair, Competitive, and Secure Global Digital Economy.

At the heart of the report are recommendations that speak to fundamental issues of trust, expectation of privacy, corporate responsibility, transparency and the interdependence of technology, the private sector, the government and its citizens. Some critics have suggested that the report didn't focus on specifics like encryption, but the Commission may have left a clue as to why in stating, "quantum computing has the potential to render useless some of the encryption technology we rely on today."

By shifting the focus from widely understood and accepted tactics to more novel strategies, such as the wholesale move away from passwords, the Commission may have been attempting to jump ahead of the current conversation.

The President-elect and his team will have the option to consider which portions of the report, if any, they would like to champion. Like the report, the President-elect has also weighed in on other issues that will have a significant impact on technology, privacy and cybersecurity, such as employment, immigration, training, leadership, public/private partnerships and establishing international norms for cyber warfare.

For purposes of this article, we focus on the current state of play at the intersection of regulation and cybersecurity.

Cybersecurity Regulation

President-elect Trump has signaled clearly that he prefers less regulation, and he has effectively suggested a method of de-regulation by quota. His reported

position, which continues to evolve, states that he will pursue "a requirement that for every new federal regulation, two existing regulations must be eliminated" on his first day in office.

The Commission's report takes a less blunt approach, but still recommends that "incentives should always be preferred over regulation, which should be considered only when the risks to public safety and security are material and the market cannot adequately mitigate these risks."

The report also suggests that any new regulation should align with the risk-based approach of the National Institute of Standards and Technology (NIST) Cybersecurity Framework to help companies control costs and incentivize innovation.

Specifically, the Commission suggests that "an agency that advances an approach which substantially departs from the baseline framework would be required to make the case that its added cost is outweighed by a public benefit." This might present an interesting test to anything at the federal level that is similar to the "minimum standards" approach that the New York State Department of Financial Services proposed last September.

This may be an area where market forces should not be left untethered. The combination of profit motives and society's proven appetite for innovation with less regard to security may be a recipe that calls out for thoughtful regulation. As the market continues to evolve into a technologically interdependent and entangled ecosystem, it is important for the public and private sector to work together to ensure integrity throughout the system, especially with regard to federal contractors and the nation's critical infrastructure.

Federal Government & Contractors

The OPM data breach in August 2015 was the largest U.S. government data breach of all time and is believed to have involved a compromise of government infrastructure via contractor access. This breach illustrates the elevated importance of the security of private sector networks given the interconnectivity with government networks and critical infrastructure (whether or not the critical infrastructure itself is owned by the private sector).

In the aftermath of the OPM breach, those within the federal government who had been advocating that agencies take a closer look at the current state of their cybersecurity practices finally had the opportunity to start advancing tools to improve cyber hygiene.

Tony Scott, the Obama administration's Chief Information Officer, said "every agency was racing to make improvements, including the use of basic tools like two-factor authentication." At the point in time when that statement was made, multi-factor authentication had been a commonly used security control for over a decade in other industries, demonstrating the level of change required across government agencies to achieve a baseline level of security.

Also in the wake of the OPM breach, the Department of Defense (DoD) implemented new rules governing cybersecurity related to contractors. The Defense Federal Acquisition Regulation Supplement (DFARS) Parts 202, 204, 212, 239, and 252 hold contractors and their subcontractors accountable to implement security controls in alignment with the likelihood of loss, misuse, unauthorized disclosure and alteration of information.

The rules also require that the contractors and subcontractors must provide security controls as provided under NIST Special Publication (SP) 800-171. Some in the private sector have pushed back due to the cost to comply, and the DoD has significantly delayed the date that contractors must be in full compliance with the rules.

Protecting Critical Infrastructure

The vast majority of the critical cyber infrastructure in the United States is owned by the private sector. Critical infrastructure consists of facilities — everything from hospitals to subway and computer systems, including (but not limited to), banking and financial institutions, transportation, power and communications systems.

As a nation, the public and private sector have a shared responsibility for the security and safety of its citizens. In addition to the private ownership of critical infrastructure, more and more devices are increasingly being connected to the Internet, providing myriad entry points and potential vulnerabilities to bad actors from all over the world.

In addition to the risks inherent in this increased interconnectivity, there is also a growing shortage and knowledge gap in the number of employees with the requisite skills to properly access these connected systems. Some companies are responding to this by instituting training programs to educate their employees on common cybersecurity risks, such as phishing, tailgating and sharing private information in social media, which can be used for social engineering.

There are, however, no regulations that govern a minimum level of education required by professionals who will be operating on Internet-connected critical infrastructure.

The cybersecurity supply chain protecting national security interests is often based on commercial off the shelf software. A large majority of this software is developed offshore by foreign corporations and the complexity of these software packages make them difficult to thoroughly examine.

There is currently no regulation or enforcement of best practices like secure coding. This software supply chain has the potential to compromise security intentionally (*i.e.*, software with security flaws baked in purposely to later be exploited by threat actors)

or unintentionally (*i.e.*, a lack of best practices such as secure coding leaving open a greater possibility of unknown vulnerabilities that will later turn into zero day attacks).

Another point of concern is the aging hardware and lack of sophistication of key software that serves as the backbone for much of the critical infrastructure in the United States. Dated and unsophisticated hardware and software, much of which pre-dates the Internet and the requisite security controls for remote access, renders it more susceptible to compromise.

As there are no minimum standards regulating what the private sector must provide in terms of hardware and software, time continues to pass and the backbone of this critical infrastructure remain vulnerable.

Infrastructure owned by the private sector and individuals, but not considered to be critical infrastructure, can also be harnessed and used as a weapon against critical infrastructure. An example of this is botnets, which have been notorious in performing distributed denial of service attacks.

Given the impact that privately owned computers and Internet of Things (IoT) devices could have on critical infrastructure, thoughtful analysis should be given to mandating minimum security standards more broadly.

Dealing with Cyber Crime

Some in the private sector have expressed concern that current laws and federal efforts do not adequately address cybercrime. The Presidential Policy Directive regarding Critical Infrastructure and Resilience focuses on the following imperatives: establishing governance (who does what, who owns what) surrounding critical infrastructure, enabling different groups to effectively share information surround cybersecurity, and establishing a consulting team to analyze critical infrastructure decisions from a cybersecurity lens as an input to decision making.

Similarly, the Federal Information Security Modernization Act (FISMA) "requires that each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source."

The Cybersecurity Information Sharing Act (CISA) of 2015 made it easier to share information about cybersecurity threats. Essentially, it enables private network operators to look for malicious behavior on their network, share such information with third parties while seeking to protect personally identifiable information, provides authorization for the federal government to share classified information with cleared individuals within the private sector, and allows companies to take defensive measures. It was a significant first step, but Congress and the federal government will likely need to revisit cybersecurity and privacy issues as the pace of attacks continues to increase.

Other countries are also grappling with how to respond to and mitigate cybersecurity risks surrounding critical infrastructure. Germany, for example, established minimum standards to which critical infrastructure providers must adhere in 2015.

The current threat landscape demands a greater focus and more resources for improvement in cybersecurity for both government and the critical infrastructure owned by the private sector.

Defining minimum security standards for the government, its services providers and critical infrastructure providers should be considered as part of the foundation of any future cybersecurity regulations.

Call to Action

The next administration will be faced with an unprecedented set of challenges in protecting our nation's information and control systems and critical infrastructure from increasingly sophisticated and persistent cyber threats.

The Trump administration would be well served to make enforcement of minimum standards for government contractors and parties involved in supplying and supporting our nation's critical infrastructure a priority. Until that happens, we won't be prepared to face the threats of today let alone the advanced threats of tomorrow.

CONTRIBUTING AUTHOR

JUSTIN HECTUS is the Director of Information at Keesal, Young & Logan where he oversees a variety of operational functions including the direction of the firm's IT vision, strategy and execution. A member of this newsletter's Board of Editors and a two-time ILTA Distinguished Peer Award winner, Justin and KYL have established a decades-long track record of effectively leveraging leading edge technology to achieve outstanding results on behalf of the firm's clients.