ML STRATEGIES

#MLWashingtonCyberWatch: White House Releases Cybersecurity Report Aimed at New Administration

December 14, 2016 | Blog | By **Cynthia J. Larose**, Michael Katz

The Obama White House has grappled with cybersecurity more than any administration in history: **China's 2009 hack of Google**, the **2015 Office of Personnel Management breach**, and the recent investigation of **Russian cyberattacks during the 2016 election**, to name just a few examples. In the midst of the president-elect's transition efforts, President Obama's administration has published what it considers to be a blueprint for enhancing the cybersecurity capabilities of government institutions and our digital consumer society today and for years beyond Inauguration Day.

The White House's nonpartisan Commission on Enhancing National Cybersecurity (the "Commission") recently released its *Report on Securing and Growing the Digital Economy* (the "Report") after nine months of intensive research. The Report offers the incoming administration 16 key recommendations and 53 associated action items focused on several key imperatives:

- Protect, defend and secure infrastructure and digital networks;
- Innovate and accelerate investment for the security and growth of digital networks and the digital economy;
- Prepare consumers to thrive in a digital age;
- Build cybersecurity workforce capabilities;
- Better equip government to function effectively and securely in the digital age; and
- Ensure an open, fair, competitive and secure global digital economy.

Using Effective Partnerships to Create Proactive Strategies

The Commission's recommendations for immediate action fall under two major prongs: **preparation and partnerships**. Alongside its support of investment in proactive cybersecurity research and development, the Report strongly urges cooperation and information sharing between state and federal government, the private sector, the consumer public, and the international community.

Such public-private collaboration could tackle issues such as hardening infrastructure, increasing the use of strong authentication and identity management, and improving security for small and medium-sized businesses. The Report also encourages the next president to "initiate a national cybersecurity workforce program to train 100,000 new cybersecurity practitioners by 2020." Achieving this goal will largely depend on the federal government's ability to encourage state governments to deploy resources and market incentives to promote cybersecurity training and job opportunities.

The Role of States

In a panel discussion with the New America Foundation following the Report's release, several experts noted that states are frustrated with the federal government's inability to act and are uniquely positioned to play a pivotal role in elevating the rigor of cybersecurity programs. Most state governments currently spend **1-2% of their IT budget on cybersecurity**, leaving room to expand resources and explore innovative policies and practices. The panel also discussed the importance of leveraging local governments in securing critical infrastructure to mitigate the risk of cyberattacks that could affect city-wide power systems or compromise citizen's personal data.

There are many federal activities already in place and the challenge will be to move these efforts strategically forward in parallel with state programs. For example, the White House Office of Science and Technology Policy has already enacted a **Computer Science for All initiative**, and state and local governments are working to incorporate computer science into K-12 curriculums. However, as was mentioned during the panel discussion, "the goal is now to align initiatives to the Cybersecurity Workforce guidelines, so that they feed into centers of academic excellence and keep up with demand." In doing so, creating employment incentives and understanding business behavior will be critical. Ultimately, the key is to ensure that innovation and cybersecurity exist in tandem and not as trade-offs. Panel experts agreed

that states must continue to “learn from each other and implement the best, integrative frameworks that don’t come off as a one size fits all.”

The Role of Citizens and Consumers

The consumer market will also play a vital role in shaping the future of cybersecurity. As the Internet-of-Things (“IoT”) continues to grow, so too do the risks of digital and physical harm caused by manipulation of insecure devices. To keep consumers abreast of device security standards and to help them make optimal product choices that will influence the IoT market, the Report calls for a cyber-security "nutritional label" for impartial product safety ratings. The Report also recommends that the Justice Department and other agencies assess liability schemes for harm caused by insecure internet-connected devices, with a goal of creating an insurance-style model for cyber-related compromises.

Looking Forward

As President Obama advised in remarks the day after the Report was released, the efficacy of the Report’s recommendations depends entirely on the Trump administration’s willingness to embrace them. Currently, Mr. Trump’s cybersecurity positions remain broadly drawn and his public statements on the subject have not clearly indicated how he might confront national security priorities raised by hacking, or online threats to consumers, or thorny concerns around privacy. **Please read Mintz Levin’s recent blog post about what to expect in the realm of cybersecurity under the Trump administration for our forecasts and analysis**.

Perhaps we will not have to wait long to find out. Several of the recommendations made by the Commission urge the president-elect to take action within his first 100 days in office. Whether we see implementation of some of the Report’s recommendations, in the first 100 days or at all, will be quite telling. Follow us at #MLWashingtonCyberWatch.

Mintz Levin Project Analyst Joanne Dynak also contributed to this post.

Authors

Cynthia Larose

Michael Katz