Subcommittee on Oversight Hearing - Bolstering the Government's Cybersecurity: Assessing the Risk of Kaspersky Lab Products to the Federal Government

U.S. House of Representatives Committee on Science, Space, and Technology
Subcommittee on Oversight

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

October 25, 2017

Introduction

Chairman LaHood, Ranking Member Beyer, 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 multiple 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 involved in policy formation and execution related to border security, aviation, and infrastructure protection. I was also 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 in my consultancy and as an adjunct faculty member at Johns Hopkins University's Zanvyl Krieger School of Arts and Sciences Advanced Academic Programs, teaching courses on homeland security, cybersecurity policy, and congressional affairs.[1] To be clear however, today I am expressing my personal

[1] The views expressed today are solely my own and are not representative of Johns Hopkins or any other organization.

views. I am appearing in my individual capacity and not as a representative of any company or organization.

The Department's mission is stated simply—"With honor and integrity, we will safeguard the American people, our homeland, and our values"—but in practice it is anything but. To be successful, DHS must be dynamic and possess the ability to evolve ahead of the ever-changing threats we face. It is important to note that DHS was created in response to the devastating terror attacks of September 11, 2001, and, as such, it initially focused on physical threats to the homeland. Emergency management was also a core function of the Department from its inception. But securing the homeland took on additional meaning as cyber attacks emerged as one of the most serious threats to our national security. Over time, the Department has taken on the dual functions of protecting federal civilian networks and of building cybersecurity partnerships with private sector stakeholders. The Department has done an admirable job, and its recent efforts, working with the private sector to blunt the impact of the WannaCry ransomware attack is just one example of its fine work in the cyber arena.

As the Committee is well aware, however, more work remains. The focus of my testimony will be on the internal side of DHS's cyber mission, which is to protect government networks. This portion of DHS's mission is foundational, because the Department cannot be well-positioned to assist the private sector and serve as a model of best practices for state and local governments until it has its own federal systems secure. Additional resources and legislative fixes will be critical in equipping the Department to carry out its mission.

Current Cyber Threat Landscape

Cyber threats pose a real and immediate danger to our federal government and the American people it represents. The increasing volume and sophistication of cyber attacks puts the sensitive information, taxpayer money, and critical systems controlled by the federal government at serious risk. We have seen dramatic and far-reaching consequences from cyber attacks on the federal government in recent years. In 2015, a data breach at the federal Office of Personnel Management exposed the personal information of more than 20 million current, former, and prospective federal employees and contractors.[2] But, only a tiny fraction of cybersecurity incidents garner media attention. The unfortunate reality is that breaches within and attacks on federal government systems are pervasive. In 2016, the federal government experienced 30,899 cyber incidents that led to the compromise of information or system functionality, according to a report from the Office of Management and Budget.[3] Moreover, federal agencies faced thousands of other attempted intrusions that were ultimately unsuccessful.

Importance of Hearing

This hearing comes at a critical moment. 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, and I thank the Committee for its important and continuing work in providing coherence and funding to federal cybersecurity efforts. The Department is resilient and, with the help of Congress, it has dramatically improved its capacities in other areas: Aviation security and emergency

[2] "OPM Hack: Government Finally Starts Notifying 21.5 Million Victims," NBC News, 10/1/2015
[3] Federal Information Security Modernization Act of 2014 Annual Report to Congress – FY2016, Office of Management and Budget, November 2016

management, for example. The same can happen with cybersecurity. With guidance, support, and funding from Congress, DHS could provide the federal civilian network protection that the American people need and deserve.

Challenges at the Federal Level

The first hurdle DHS must clear is the update of its systems and technology. The scope of the cybersecurity challenge has grown exponentially over the past decade. The Government Accountability Office (GAO) found that the number of annual information security incidents affecting the federal government has grown by more than 1,300 percent since fiscal year 2006.[4] But the cybersecurity infrastructure at the federal level has not kept pace. While I served at DHS, one of my responsibilities was to work as a DHS representative with the initial group of individuals at the national cyber security division to establish relationships with the other agencies, the private sector, and leaders on Capitol Hill to create the early cybersecurity framework to guide departmental operations. Programs that are still in operation today – like Einstein, which detects and blocks cyber attacks and allows DHS to use threat information detected in one agency to protect the rest of the government – were born during those early days and, unfortunately, the Department is still using technology and strategy from 15 years ago. The GAO recently concluded, "Einstein was largely ineffective at thwarting hackers" because it "could only detect known cyber threats and lacked the ability to suss out sophisticated hackers."[5]

Another challenge to be addressed is the organization of DHS's cybersecurity function. The cyber organization was initially buried in the now-defunct Information

[4] Testimony Before the Subcommittee on Research and Technology, Committee on Science, Space, and Technology, House of Representatives – Cybersecurity: Actions Needed to Strengthen US Capabilities, United States Government Accountability Office, 2/14/2017

[5] "DHS cyber chief defends expansion of criticized software," The Hill, 2/11/2016

Analysis and Infrastructure Protection bureaucracy. When DHS was reorganized in the wake of Hurricane Katrina, several agencies, including the Office of Biometric Identity Management, the Federal Protective Service and the cyber functions, were left without a home and were all grouped together into a new sub-organization at DHS called the National Protection and Programs Directorate (NPPD). As a result, it is not apparent from the cybersecurity operation's organizational status that cybersecurity is a top priority for DHS. Cybersecurity operations lack the organizational muscle, credibility and political support they need in order to lead on cyber. For example, the procurement of the more than one billion dollar "Domino" program was delayed for almost three years, undermining DHS' ability to increase its cybersecurity capacity. DHS should be reorganized to create a standalone cybersecurity component agency; a critical first step is the appointment of an Undersecretary of NPPD who can serve as a point person for the Department's cyber functions.

This important hearing is focused on the removal of potentially problematic software – this issue is partly the result of massive confusion about who, specifically, is in charge at DHS. Without a dedicated cyber organization to set policy, different Chief Information Officers (CIOs) are independently responsible for purchasing software and other cybersecurity tools – leading to a system that relies on many different products with differing levels of quality and security. Reorganization would allow cybersecurity authority to be both concentrated within the Department—in the leadership of a standalone agency—and exerted across DHS and the federal civilian operations—through cybersecurity leadership that possesses the requisite authority and clout.

Returning to software acquisitions, a compounding factor to the current challenge is the fact that – as a result of sequestration – many CIOs are forced to abide by the lowest price technically acceptable (LPTA) standard, which often means they don't end up with the best products. In order to have a first-class civilian cyber organization, the Federal government needs to spend money and provide consistent guidance on high-quality, secure products. Funding is a key issue when it comes to cybersecurity infrastructure across the federal government. When President Trump signed an Executive Order ("EO") 13800 - "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" – he indicated a commendable focus on the security of federal networks. Two key provisions of the EO are the requirement that all Federal agencies use the National Institute of Standards and Technology Cybersecurity Framework and the direction to all federal agencies to identify ways to improve cybersecurity in critical infrastructure. But without funding, these well-intended orders become unenforceable mandates. The protection of federal civilian networks therefore hinges on support and funding that must be initiated in this Chamber.

Recommendations

In the face of rapidly increasing and evolving threats to cyber infrastructure, there are certain concrete steps Congress and the federal government can take to protect critical systems:

1. There is currently legislation pending – H.R.3359, the Cybersecurity and Infrastructure Security Agency Act of 2017 – that would reorganize DHS and create a dedicated cyber agency. Centralizing civilian cyber operations within

DHS will create a more coherent chain of command for addressing cybersecurity issues and will help leverage limited resources more effectively. Establishing a trusted organization that has research and development capabilities, and the ability to share information in real time will only be possible with a new, fully-funded organization. Congress should act quickly to implement such a reorganization.

2. Budget cuts across the Federal government – specifically as a result of sequestration – have forced CIOs and other officials to rely on the lowest price technically acceptable (LPTA) standard when acquiring cybersecurity software and other tools. When it comes to critical cybersecurity infrastructure, sacrificing quality for short-term savings has the potential to leave open vulnerabilities and cost more money in the long-term as a result of intrusions. CIOs and other officials across federal agencies should be empowered with the resources necessary to invest in high-quality, reliable cybersecurity tools.

3. The quality of cybersecurity software and other tools is tremendously important, but there are many different options available to federal, state, and local officials. As the current situation demonstrates, implementing problematic software and later removing it creates significant disruption. The federal government should take the lead on developing a "trusted vendor" list that provides guidance on approved cybersecurity vendors with a secure supply chain that agencies can have confidence in. While this list should

certainly consider the risks associated with sourcing foreign cybersecurity tools, it should recognize that many trusted allies produce high-quality products that would benefit the United States.

4. Prevent Redundancy - The White House, Office of Management and Budget and the Congress should work together to prevent redundancy across the federal government so that competing cyber organizations do not arise in other federal agencies and, instead, centralize federal resources in DHS.

Conclusion

Thank you very much for the opportunity to testify, and I welcome your questions.