Who will fight against cyber crime?

James J. Giszczak, Dominic A. Paluzzi | Friday, February 27, 2015

The cyber threat is real and growing every day, and finding solutions will require partnership and collaboration. President Barack Obama and leaders from technology, law enforcement, industry, Congress, and education recently convened at the **Summit on Cybersecurity and Consumer Protection** at Stanford University to work together and explore partnerships that will help develop the best ways to bolster cybersecurity. The most resounding statement of the day, which truly identifies the scope of cyber threats: “Everybody is online, and everybody is vulnerable.”

Collaboration is needed between the government, tech companies, and private companies, which were each identified as necessary partners in the fight against cyber crime.

As Stanford President, John Hennessy aptly noted:

> "Cybersecurity poses one of great challenges of our time. Sooner or later it touches every aspect of our lives, public and private, social and economic. And the problems we face have changed dramatically just in the span of the last five years. From loan hackers to well-financed and determined state actors, and professional cyber criminals. From minor but annoying break-ins, to massive compromises of databases containing personal, health, and financial information of hundreds of our thousands of our citizens. All are occurring at a time when we as a society around the world are more intimately linked by technology and we have more information on

> line than every before. And while the Internet and World Wide Web have delivered enormous benefits to society, the growing threats of cyber attacks could rob us of many of these benefits if we do not act decisively to contain and reduce the threat."

Hennessy also noted the three characteristics of cyber threats that make them such a difficult enemy.

- **Anonymity.** It is hard to track down hackers who can hide via proxies and intermediate hosts.
- **Stealth Nature of Attacks.** Intrusions occur over long periods of time and, most times, before the host even knows it is being attacked.
- **Lack of Physical Assets.** In a cyber attack, there are no physical assets to control. It is hard to control what you cannot see or physically hold in your hand. The threat can easily be contained in an email transmitted anywhere in the world.

Homeland security advisor

Lisa Monaco, homeland security advisor to the president, who deems herself the "Bearer of Bad News," reiterated the necessity of collaboration and partnership being the only way to address very difficult challenges of cybersecurity threats that challenge not only national and homeland security, but economic security as well.

Monaco went on to note that cyber threats are increasing in their frequency (five times since the last annual report), scale, sophistication, and severity of impact, and are coming from an expanded group of actors that are more dangerous. As a result, "No one connected to the Internet is immune. From business and consumers, to governments and private citizens. Each hour we know that state and non-state actors, terrorists, hackers, and criminals, are probing networks to steal, spy, manipulate, and to destroy….The cyber threat is becoming more sophisticated, more diverse and more dangerous."

*"No one connected to the internet is immune. From business and consumers, to governments and private citizens. Each hour we know that state and non-state actors, terrorists, hackers, and criminals, are probing networks to steal, spy, manipulate, and to destroy….The cyber threat is becoming more sophisticated, more diverse and more dangerous." – **Lisa Monaco**, February 13, 2015*

According to Monaco, unless we develop a collective way of dealing with cyber threats, malicious attacks could become the norm.

Monaco stressed that the government wants to work with the private sector to better protect against cyber threats. She identified four steps the private sector can take now:

1. Employ basic preventive cybersecurity measures, like using the framework that was put out last year;
2. Strengthen their ability to respond to cyber threats, which will help the private sector be more resilient to threats;
3. Enhance international cooperation so when users in the world target the United States, they are held accountable; and
4. Make cyber space more secure through the use of better passwords and enhance consumer protections online.

The president's keynote address

*"The first computer viruses hit personal computers in the early 1980s, and essentially, we've been in a cyber arms race ever since." – **President Obama**, February 13, 2015*

The highlight of the summit was President Obama's keynote address. In it, the president noted the precarious paradox of technology: "[T]he very technologies that empower us to do great good can be used to harm us. The same information technologies that help make our military the most advanced in the world are targeted by hackers from China and Russia who go after our defense contractors and systems that are built for our troops. The same social media we use in government to advocate for democracy and human rights around the world can also be used by terrorists to spread hateful ideologies. So these cyber threats are a challenge to our national security."

With that, the president continued the focus on collaboration, and spoke on the need for public-private partnerships to fight cyber crime. He laid out four principles to do this:

1. **A shared mission.** So much of our computer networks and critical infrastructure are in the private sector, which means government cannot do this alone. But the fact is that the private sector can't do it alone either, because it's government that often has the latest information on new threats. There's only one way to defend America from these cyber threats, and that is through government and industry working together, sharing appropriate information as true partners.
2. **Focus on our unique strengths**. Government has many capabilities, but it's not appropriate or even possible for government to secure the computer networks of private businesses. Many companies are cutting-edge, but the private sector doesn't always have the capabilities needed during a cyber attack, the situational awareness, or the ability to warn other companies in real time, or the capacity to coordinate a response across companies and sectors. So we need to be smart and efficient and focus on what each sector does best, and then do it together.
3. **Constant evolution**. Noting that we've essentially been in a cyber arms race every since the first computer viruses hit personal computers in the early 1980's, we must design new defenses. Whether it's phishing or botnets, spyware or malware, and now ransomware, these attacks are getting more and more sophisticated every day. So we have got to be just as fast and flexible and nimble in constantly evolving our defenses.
4. **Protect the privacy and civil liberty of the American people.** When consumers share their personal information with companies, they deserve to know that it's going to be protected. When government and industry share information about cyber threats, we've got to do so in a way that safeguards your personal information. When people go online, we shouldn't have to forfeit the basic privacy we're entitled to as Americans.

The president signs executive order "Promoting Private Sector Cybersecurity Information Sharing"

The president ended his keynote by signing an executive order "**Promoting Private Sector Cybersecurity Information Sharing**". As the president explained, the executive order is to promote even more information sharing about cyber threats, both within the private sector and between government and the private sector. The order is set up in six key sections and aims to encourage more companies and industries to set up organizations — hubs — so information can be freely shared. It calls for a common set of standards, including protections for privacy and civil liberties, so that government can share threat information with these hubs more easily. It will also help make it easier for companies to get classified cybersecurity threat information they need to protect themselves.

The order builds upon the foundation established by Executive Order 13636 of February 12, 2013 (Improving Critical Infrastructure Cybersecurity), and Presidential Policy Directive-21 (PPD-21) of February 12, 2013 (Critical Infrastructure Security and Resilience).

Consumer Privacy Bill of Rights to be announced later this month

In addition, the president announced that later this month, the White House will be proposing new legislation called the Consumer Privacy Bill of Rights. It remains to be seen what this new Consumer Privacy Bill of Rights will specifically entail, but according to the president, it would give Americans baseline protections, like the right to decide what personal data companies collect from them, and the right to know how companies use that information.

The state of federal cybersecurity protections

The executive order and the soon-to-be proposed Consumer Privacy Bill of Rights are just two new arrows in the federal government's quiver to pass federal cybersecurity and data privacy legislation this year. The White House already unveiled **two proposed laws** on data privacy to establish a national data breach notification standard and provide protection to companies who share information with the government.

The introduction of these two proposed laws was followed by the State of Union Address, during which President Obama called on Congress to pass cybersecurity legislation by noting, "No foreign nation, no hacker, should be able to shut down our networks, steal our trade secrets or invade the privacy of American families."

This was then followed by the president unveiling the new Cyber Threat Integration Center, which will gather information about cyber threats. This single entity seeks to connect the dots and analyze, integrate, and quickly share intelligence about cyber threats across government so all involved can act on threats even faster.

"The cyber world is sort of the wild, wild West. And to some degree, we're asked to be the sheriff." – ***President Obama***, *February 13, 2015*

Takeaways

Cybersecurity is and will continue to be a concern. It is everyone's concern. No one is immune. Everyone and every company are at risk. There are steps organizations can take to protect themselves to stave off or respond to a breach, including the four items identified by Monaco.

In addition, the White House has made clear that cybersecurity is a pressing federal issue, an issue of national, homeland, and economic security.

Companies that continue to strive to protect digital information will be the companies consumers trust to shop at and buy their services. In addition, as America as a whole becomes better equipped to deal with cybersecurity threats, other countries will seek out American companies for their products and services. This is the economic security piece of the puzzle – a very important piece where companies can truly see the economic advantage of having a proper data privacy protection plan in place.

For more information, please contact one of the attorneys listed below.

James J. Giszczak

Dominic A. Paluzzi