Testimony of Matthew Rhoades

Director
Cyberspace & Security Program
Truman National Security Project &
Center for National Policy

House Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies
April 16, 2014

Chairman Meehan, Ranking Member Clarke, members of the Committee: thank you for inviting me to appear today to discuss how the public and private sectors can work together to increase cybersecurity.

Currently, I serve as the Director of the Cyberspace and Security Program at the Truman National Security Project and Center for National Policy. Together, these two organizations represent more than thirteen hundred members with an expertise in numerous security issues—including cybersecurity—and a dedication to forging strong, smart, and principled national security policy for America.

The rapid development of information networks over the past thirty years has allowed individuals and nations to grow and prosper. Today, our small businesses are global enterprises—reaching markets and customers on the other side of the world with the click of a mouse. The Internet invigorates economic progress and helps people rise out of a cycle of poverty in the developing world.

These tools also enable the expansion of America's mutually supportive ideals: human rights, freedom, and opportunity. Using the Internet, democracy activists in nations ruled by oppressive regimes can organize to petition for their fundamental rights; vulnerable populations in conflict-ravaged areas can show the world the brutality of their own governments; and individuals can seek out new ideas to challenge their own beliefs.

New technologies are providing hope to millions by creating the conditions for innovation and human prosperity to flourish. Unfortunately, they are also being exploited by a variety of actors to further nefarious national, criminal, and ideological objectives.

Hacktivists—or online demonstrators—use information networks to target opponents and draw attention to a political cause. Terrorists use information networks to spread their propaganda and recruit others to help commit acts of violence. Criminal organizations use the Internet to steal from individuals and organizations all over the world and turn another's loss into their financial gain. Finally, nation states leverage these capabilities to spy on, steal from, and potentially attack their adversaries.

Frequently, these groups—hacktivists, terrorists, criminal organizations, and nation states—also overlap, working together towards complimentary interests while utilizing the inherent anonymity of cyberspace to make attribution even more difficult.

With each new day, the number of actors with access to these tools increases and, as a result, so does the number of potential victims. Roughly 90% of the world's data has been generated in the last two years.[1] As more information is generated, confidentiality and privacy grow more vulnerable. Governments are losing once closely-held state secrets; companies are finding their intellectual property suddenly in the hands of competitors on the other side of the world; and individuals are losing control over their private information.

[1] Science Daily, "Big Data, for better or worse: 90% of world's data generated over last two years," 22 May 2013, http://www.sciencedaily.com/releases/2013/05/130522085217.htm.

According to Symantec's "Internet Security Threat Report 2014," the number of breaches increased by 62% in 2013 with a total of over 552 million identities compromised.[2] Additionally, targeted attacks grew by 91% and are increasingly aimed at small businesses.[3]

And as we are all aware, the recent, highly-publicized breach at Target—the second largest retailer in the United States—compromised personal information on 70 million customers by using software that may have cost less than $2,500 at an online marketplace.[4] Today, cyber criminals can use relatively easy-to-find software to make outsized gains.

The Target example shows that even the largest companies with vast resources are vulnerable. Frequently, they are unaware that a breach has even occurred. One security provider recently announced that in 2013 the median number of days attackers were present in a network prior to discovery was 229 days. That is actually 14 days less than the 2012 median.[5]

In short, today's technologies provide an unprecedented opportunity for humans to reach their full potential while simultaneously increasing individual and collective security risks.

These are facts that the members of this Committee know well, and they are broader than the scope of this hearing. But they are worth mentioning in this context because in cyberspace, the difference between espionage, crime, and attack can be as simple as intent, or just a few keystrokes.

Gaining and maintaining access to a network are the most difficult phases of a cyber incident. Adversaries spend a great amount of time, energy, and resources to seek out and secure vulnerabilities that provide access. But once they are in the network, whether they spy, steal, or destroy is a matter of choice.

Furthermore, criminals are developing new tools that are more sophisticated and more intuitive than previous generations, and then selling them in online marketplaces. This reality is lowering the barriers to network entry and giving more malicious actors the capability to threaten critical systems, in both the private and public sectors.

Cyber crime, therefore, is linked to national security and the protection of private information. All of the actors using cyberspace for illegitimate means need vulnerabilities to exploit, and no single entity—whether government or business—can secure a domain that extends beyond traditional geographic boundaries. In cyberspace, one weak link can compromise the security of the entire system. Cybersecurity is a shared responsibility.

To ensure our Nation is safe, the government must coordinate the protection of our country's most critical assets against sophisticated, destructive attacks while law enforcement agencies impose the criminal laws of the United States in the cyber domain. Through the development of new tools and the continued maturation of the National Cybersecurity and Communications Integration Center (NCCIC), the Department of Homeland Security (DHS) is addressing this responsibility.

[2] Symantec Corporation, *Internet Security Threat Report 2014; Volume 19*, p. 5.

[3] Ibid, p.5 & p.18.

[4] Chris Smith, "Expert who first revealed massive Target breach tells us how it happened," 16 January 2004, http://bgr.com/2014/01/16/how-was-target-hacked/

[5] Mandiant, *MTrends: Beyond the Breach,* p.1.

But more can be done. For example, the effectiveness of the NCCIC is directly tied to the level of participation by other Federal Agencies. Yet, those agencies are not currently required to share information with DHS. If we are going to task DHS with the responsibility for leading the protection of federal civilian agencies, then we must give them the authorities required to be successful.

Governments must also find ways to cooperate with one another on investigations. Cyber crimes are often intentionally routed through multiple countries, particularly those who provide sanctuaries against international investigations. When an investigation leads to a new jurisdiction, the investigators are suddenly at the mercy of another government. More must be done in the international arena to build the capacity of nations that do not want to be criminal sanctuaries and to discourage others that are complicit in criminal activities originating in their territory.[6]

Private companies must do their part as well. Most of this country's critical infrastructure is privately owned and operated, but market forces alone have yet to incentivize broad scale use of cyber risk management strategies. Many companies are working to protect their networks, but too many are not doing enough. And in sectors where there is no choice in the consumer market—where a public good is being provided by a private actor—the government should play a larger role in ensuring the security of critical networks.

Additionally, many companies are collecting, storing, and analyzing information on U.S. citizens. This information deciphers everything from our travel habits to our personal interests. Securing our most important networks and protecting our personal information requires the private sector to take better responsibility for their own security.

Finally, individuals have to take responsibility for our online behavior as well. Although there are sophisticated hackers at work, most compromises take advantage of existing vulnerabilities that have not been patched but could have been. The more hardened a target becomes, the more likely a hacker will look for a less secure, peripheral target as a means to get in. This is likely the reason that targeted attacks are increasingly focused on small businesses. We must contribute to a culture of security that is respectful of the rights of others, while contributing to the security of the whole system.

Universities across the country, including Drexel University here in Philadelphia, are developing educational programs to ensure the next generation is prepared to combat cybersecurity threats. These are important initiatives that warrant support. However, it will take a generation for them to fully bear fruit. More also needs to be done to make today's users aware of the risks associated with their online behavior.

Getting this model of collaborative security correct is dependent upon trust. Governments and private entities must work together to mitigate threats. Both, however, are collecting vast quantities of information on individuals. The more information they store in their databases, the more attractive those databases become to criminals. What they share and how they share has serious privacy and civil liberties consequences for individual consumers.

While information sharing programs do not offer a cybersecurity panacea, they can contribute to collective security by creating a fuller picture of the threat landscape. That said, there is a right way to

[6] Richard A. Clarke, *Securing Cyberspace Through International Norms: Recommendations for Policymakers and the Private Sector,* Good Harbor Risk Management, LLC, p.23.

share information and a wrong way to share information. All irrelevant personally identifiable information should be removed before the information is given to the federal government or another private actor. Information coming into the federal government should have previously defined acceptable uses and be given to a civilian agency. And those who participate in the program and exhibit negligent behavior should be held responsible. Getting this right matters: the way we build our domestic programs will have privacy and civil liberties consequences for Americans and for human rights activists and dissidents overseas.

The reality is that given enough time, resources, sophistication, and motivation, an attacker will gain access to a network. And as people become more dependent upon technology, the opportunities for crime, espionage, and physical disruption will only increase. But with collaboration built upon trust, I believe we can reduce our vulnerabilities. By implementing commonly held best practices, we can protect the great majority of our networks, secure our personal information, and allow our security agencies to focus on preventing sophisticated attacks against our most critical networks. And, in the end, we can more fully realize the potential of new technologies to expand freedom and opportunity at home and abroad.

Thank you for the opportunity to join you today, I look forward to answering any of your questions.