

Shawn Henry  
President, CrowdStrike Services,  
Former Executive Assistant Director, FBI  
Washington, D.C.  
April 24, 2012

Good afternoon Chairman McCaul, Ranking Member Keating, and members of the subcommittee. I'm pleased to be here today to discuss the cyber threats facing our nation and how these threats impact our government and private sector networks. It is difficult to overstate the potential harm these threats pose to our economy, our national security, and the critical infrastructure upon which our country relies.

### **The Cybersecurity Threat**

As the subcommittee is aware, the number and sophistication of cyber attacks has increased dramatically over the past five years and is expected to continue to grow. The threat has reached the point that, given enough time, motivation, and funding, a determined adversary will likely penetrate any system that is accessible directly from the Internet. Even systems not touching the network are susceptible to attack via other than remote access, including the trusted insider using devices such as USB flash drives, and the supply chain.

It is difficult to say with confidence that our critical infrastructure—the backbone of our country's economic prosperity, national security, and public health—will remain unscathed and always be available when needed. In fact, I have stated publicly that with the depth and breadth of the intrusions I've seen, I believe it is necessary for network administrators to assume they have already been breached rather than waiting for their intrusion detection systems to alert them to an infiltration.

## **Criminal Cyber Threats Against the Private Sector**

Cyber criminal threats to the U.S. result in significant economic losses. Cyber criminals are forming private, trusted, and organized groups to conduct cyber crime. The adoption of specialized skill sets and professionalized business practices by these criminals is steadily increasing the complexity of cyber crime by providing actors of all technical abilities with the necessary tools and resources to conduct cyber crime. Not only are criminals advancing their abilities to attack a system remotely, they are becoming adept at tricking victims into compromising their own systems.

Once a system is compromised, cyber criminals will use their accesses to obtain Personally Identifiable Information (PII), which includes online banking/brokerage account credentials and credit card numbers of individuals and businesses that can be used for financial gain. As cyber crime groups increasingly recruit experienced actors and pool resources and knowledge, they advance their ability to be successful in crimes against more profitable targets and will learn the skills necessary to evade the security industry and law enforcement.

The potential economic consequences are severe. The sting of a cyber crime is not felt equally across the board. A small company may not be able to survive even one significant cyber attack.

Often, businesses are unable to recoup their losses, and it may be impossible to estimate their damage. Many companies prefer not to disclose that their systems have been compromised, so they absorb the loss, making it impossible to accurately calculate damages. As a result of the inability to define and calculate losses, the best that the government and private sector can offer are estimates. Over the past five years, estimates of the costs of cyber crime to the U.S. economy have ranged from millions to hundreds of billions. A 2010 study conducted by the Ponemon Institute

estimated that the median annual cost of cyber crime to an individual victim organization ranges from \$1 million to \$52 million.

According to a 2011 publication released by Javelin Strategy and Research, the annual cost of identity theft is \$37 billion. This includes all forms of identity theft, not just cyber means. The Internet Crime Complaint Center (IC3), which aggregates self-reported complaints of cyber crime, reports that in 2010, identity theft schemes made up 9.8 percent of all cyber crime.

### **The Tip of the Iceberg**

A colleague of mine recently used an analogy where an iceberg represents the totality of threats to the information infrastructure. “Cyber crime”, as described above, is merely the tip of the iceberg; the biggest threats are “below the water line”, just like the vast majority of an iceberg. The public sees “the tip” because the cyber “crime” is regularly reported in the media; stolen credit cards, lost identities, Eastern European Organized Crime groups; and breached bank accounts. The “water line” is the separation between the unclassified and classified environment; thus, the most sophisticated and damaging attacks occur primarily out of the public’s sight.

I would offer that only a very small group of individuals...primarily those in the intelligence community...have ever seen “below the water line”, and the real threat is grossly underappreciated by the public. The most significant cyber threats to our nation are those with high intent and high capability to inflict damage or even death in the U.S.; to illicitly acquire substantial assets; or to illegally obtain sensitive or classified U.S. military, intelligence, or economic information. These are the threats from foreign intelligence services, and for those I have seen below the waterline.

## **Cyber Threats to U.S. Critical Infrastructure**

The threat continues unabated. U.S. critical infrastructure faces a growing cyber threat due to advancements in the availability and sophistication of malicious software tools and the fact that new technologies raise new security issues that are not always addressed prior to adoption. The increasing automation of our infrastructures provides more cyber access points for adversaries to exploit, and the target set grows daily as more and more data is pushed, transmitted, or stored on the network.

New “smart grid” and “smart home” products, for example, designed to provide remote communication and control of devices in our residences, businesses, and critical infrastructures, must be developed and implemented in ways that will also provide protection from unauthorized use. Otherwise, each new device will become a doorway into our systems for adversaries to use for their own purposes.

Industrial control systems, which operate the physical processes of the nation’s pipelines, railroads, and other critical infrastructures, are at elevated risk of cyber exploitation. We need to be concerned about the proliferation of malicious techniques that could degrade, disrupt, or destroy critical infrastructure. Though likely only advanced threat actors are currently capable of employing these techniques, as we have seen with other malicious software tools, these capabilities will eventually be within reach of all threat actors.

### **What Does All This Mean?**

I believe most major companies have already been breached or will be breached, resulting in substantial losses of information, economic competitiveness, and national security. Many are breached and have absolutely no knowledge that an adversary was or remains resident on their network, often times for weeks,

months, or even years. While I was EAD at the FBI, our agents regularly knocked on the door of victim companies and told them their network had been intruded upon and their corporate secrets stolen, because we found their proprietary data resident on a server in the course of another investigation. We were routinely telling organizations they were victims, and these victims ranged in size and industry, and cut across all critical sectors.

### **Addressing the Threat**

Although our cyber adversaries' capabilities are at an all-time high, combating this challenge needs to be a top priority for both the public and the private sector. We need to continue to develop partnerships within industry, academia, and across all of government to have a dramatic improvement in our ability to share intelligence to combat this threat.

The adversary is persistent. It's not enough to stop their attack once or twice; they will keep trying until they get in. The problem with existing technologies and threat-mitigation tactics is they are too focused on adversary tools (malware and exploits) and not on who the adversary is and how they operate. Ultimately, until we focus on the enemy and take the fight to them to raise their cost of attack, we will fail because they will always get thorough.

This requires us to stop relying solely on "defense." The sophisticated adversary practices crafty offense, and the offense outpaces the defense. While we certainly need to continue defense...we cannot let our guard down...we need to be more proactive and strategic in our approach.

We cannot stand by and wait for them to trip an alarm as they shake the proverbial fence; sophisticated adversaries jump OVER the fence, bypassing the intrusion detection "alarm" entirely. We must assume they are already inside the perimeter, and we must constantly hunt them on our networks to identify and mitigate their

actions.

Hunting necessitates us acquiring a better site picture of the adversary...what assets are they targeting, what techniques are they employing, and who, exactly, are they? This is where intelligence sharing is critical; using advanced intelligence technology, companies can share information enabling them to learn the human aspects of the attack, become more predictive, and thus preventative. Technology is a piece of the solution, not the sole solution, because what we really have is an adversary problem.

### **Conclusion**

We face significant challenges in our efforts to combat the cyber threat. I am optimistic that by strengthening partnerships, effectively sharing intelligence, and successfully identifying our adversaries, we can best protect businesses and critical infrastructure from grave damage.

I look forward to assisting the subcommittee and Congress as a whole to determine a successful course forward for the nation that allows us to reap the positive economic and social benefits of the Internet while minimizing the risk posed by those who seek to use it to do us irreparable harm.