Shawn Henry
President,
CrowdStrike Services
(Former Executive Assistant Director, FBI)

House Committee on Homeland Security
"A New Perspective on Threats to the Homeland"

Wednesday, February 13, 2013

Good afternoon Chairman McCaul, Ranking Member Thompson, and members of the Committee. Thank you for having me here today to discuss the cyber threats facing our nation, how these threats impact our government and private sector networks, and the significant risk posed to our economic and national security. I sincerely believe this is one of the most critical issues facing our nation, and I appreciate the level of attention this Committee is affording it.

The Cybersecurity Threat

We have spoken of the cyber threats for far too long, but it is too important and cannot be overemphasized. So I'll state it again, emphatically…foreign adversaries have targeted every major organization in this country, and have stolen untold billions of dollars of intellectual property, research and development, and corporate strategies and secrets. The volume and sophistication of cyber attacks has increased dramatically over the past five years, and in the current environment it will continue to grow.

Given enough time, motivation, and funding, a determined adversary will penetrate any system that is accessible directly from the Internet. Even systems not touching the network are susceptible to attack via means other than remote access, including the trusted insider using devices such as USB thumb drives, and the supply chain.

I have stated publicly that 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. Many 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. Organizations must, therefore, actively and constantly hunt for the adversary on their network.

Alarmingly and increasingly, attackers are moving beyond mere exfiltration or theft of data. With the breadth and depth of access they have, adversaries can and have manipulated, disrupted, or destroyed data and infrastructure. Those with malicious intent can take devastating actions, and 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.

A Paradigm Shift in Strategy

My colleagues at CrowdStrike, George Kurtz and Dmitri Alperovitch, have talked about the deterrence of threat actors
for years. Steven Chabinsky, my colleague at the FBI for 17 years, and currently with me at CrowdStrike as SVP of Legal Affairs, also discusses the paradigm shift necessary in cybersecurity strategy.

Vulnerability mitigation is the current cybersecurity approach in the private sector, and has been for the past 20 years. We continuously focus on hardening our networks by "Defense-in-Depth", using firewalls, anti-virus software, patching vulnerabilities, and employing intrusion prevention systems. This approach generally stops those actors who do not care who their specific targets are, but are simply like burglars who are willing to rob anybody's house and take anybody's jewelry.

Our mistake, however, is that we are using the same approach against Advanced Persistent Threat actors who actually have specific targets in mind, and are not going to stop until they have reached their goals. These modern day cyber burglars are targeting the equivalent of the Hope diamond, quite specifically, not fungible engagement rings. For our most advanced and well-funded adversaries, there are no substitutes for their targets, regardless of how many, and they will continue their onslaught until they achieve success.

Ironically, our own defensive efforts have actually made the problem worse, by encouraging our adversaries to outperform us, while we outspend them. Although many are not prepared to consider this possibility, the result of our failure to distinguish between the novice and the professional adversary has been a proliferation of more capable malware, created by nation state adversaries and organized crime groups, and an escalation of their activities in order to defeat our defenses.

What Does This Mean?

Employing a threat mitigation strategy requires an increased ability to detect and identify our adversaries, and to penalize them. <u>This is the identical strategy we employ in the physical world every single day to thwart criminals, spies, and terrorists.</u>

Achieving these goals in the cyber environment, however, will require unprecedented coordination between private industry – which as a whole has the ownership and ability to achieve these goals, and governments, which are primarily authorized to investigate and penalize them.

Inevitably we must bring the private sector and the government together to achieve the goal of threat deterrence. The vast majority of the intelligence that will lead to identification of the adversaries resides on private sector networks; they are, in essence, "crime scenes", and the evidence and artifacts of the breach are resident on those networks. That threat intelligence, too, can't be shared periodically via e-mail at human-speed; it needs to be shared among all victims, in real-time, at network speed. The private sector, then, can fill tactical gaps that the government

is blind to. This can be done while respecting privacy, a critical and absolutely necessary element of intelligence sharing.

The Department of Homeland Security (DHS) naturally has the responsibility for developing and promulgating necessary vulnerability reduction strategies and guidelines. Likewise, they are responsible for consequence management after a breach. Additionally, though, with a threat mitigation model, DHS is a potential intermediary between other government agencies and the private sector to facilitate the analysis and dissemination of "big data" -collected intelligence - leading to identification and attribution of adversaries.

Likewise, the government has intelligence collection on the threat actors that is different from, and additive to, that collected by the private sector. Knowing what I do about that intelligence, and how it's collected, I am certain the government can share much more data with industry than is currently shared today. That intelligence will add infinite value, and it can be packaged and shared with the private sector without threatening the integrity of the sources and methods through which it's collected. Again, privacy is and must remain a key tenet of any intelligence sharing strategy.

When the adversary is identified, the government can then use its resources and actions – whether it's Law Enforcement, the intelligence community, diplomatic, or financial – to mitigate the threat posed by these sophisticated opponents. The consistent threat posed by adversaries will subside only when the cost to operate outweighs any potential gain.

.

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.

We must start, however, by opening the debate on the limitations of the existing defensive-only security model and the necessity of a threat deterrence model. Further, we need a public discussion of how government and industry can jointly work together to achieve a safer cyber environment by shining a light on our adversaries instead of consistently telling victims to "just do more."

I look forward to assisting the Committee, 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 do us irreparable harm.

I encourage our further collaboration, and I'm happy to answer any questions.