**WRITTEN TESTIMONY OF**


**KEVIN MANDIA**
**CHIEF EXECUTIVE OFFICER**
**MANDIANT CORPORATION**

**BEFORE THE**

**PERMANENT SELECT COMMITTEE ON INTELLIGENCE**
**U.S. HOUSE OF REPRESENTATIVES**

# CYBER THREATS AND ONGOING EFFORTS TO PROTECT THE NATION

**OCTOBER 4, 2011**

## Introduction

Thank you Mr. Chairman, Ranking Member Ruppersberger, and Members of the Committee, for this opportunity to share observations my colleagues and I have made while fighting cyber attacks over the past two decades. Today, in our current state of cyber security, security breaches are inevitable. This is an important fact, so I am intentionally repeating it. In our current state of cyber security, security breaches are inevitable. While this sounds defeatist, we are not defeated, and today I would like to offer recommendations for tangible actions that we can take as a Nation, both in the private and public sector, to drastically improve our security posture in cyberspace.

## The Evolution of Cyber-Threats

Virtually my entire professional career has been dedicated to assisting organizations, both private and public sector, in responding to Cyber-security breaches. Over the last two decades I have assisted hundreds of organizations that have suffered security breaches. Most of these victim organizations were Fortune 500 companies.

Following several years as an agent in the Air Force Office of Special Investigations, I founded MANDIANT in 2004 to offer private sector companies the ability to respond effectively to emerging cyber threats. As I testify here today, MANDIANT employees are on the front lines of the cyber battle, responding to active computer intrusions into dozens of American companies.

Through my experience in combating cyber threats, I have seen first hand the evolution in which attackers seek to undermine our cyber infrastructure. Simply put, sophisticated threats are on the rise, and these threats have evolved faster than our ability or willingness to reliably safeguard our assets. Advanced threats are becoming mainstream, and currently outpace the defenses commonly deployed by corporate America.

For the last seven years, our intent as a company has been to respond to every cyber-security incident that matters. Since 2004, we have responded to incidents at hundreds of companies, we have investigated millions of systems, and we receive calls almost every single workday from companies that have suffered a cyber security breach. These cyber intrusions have impacted most industries, including law firms, financial services, blue chip American manufacturers, retailers, the defense industrial base, telecommunications, space and satellite and imagery, cryptograph and communications, government, mining, software, and many others. I have witnessed the unique threats facing each of these industries, and how they can respond to cyber threats.

While previous generations of attacks targeted technology such as networks and servers and exploited vulnerabilities in software, attackers have now evolved to target human inadequacies and weaknesses. Our first-generation defenses – largely the product of a patchwork compliance efforts – can be successful in turning away a direct attack aimed at vulnerable systems and applications. Given these improvements in the "Maginot Line" that protects most of our systems, attackers have shifted their focus from targeting systems and applications to targeting individuals. As Americans increasingly rely on communications and transactions over the Internet, invest more in their online identities and continue to pour their personal details into sites such as Facebook, Google+, Linkedin and personal blogs, attackers are able to personalize their attacks. These targeted and personalized attacks are difficult to prevent because they leverage human vulnerabilities and human trust.

As an example, attackers commonly send communications – an email, an instant message, or a SKYPE message – purporting to come from a friend or colleague the end user is familiar with, and include an attached file, perhaps a Microsoft Word or Adobe document, that piques the end-user's interest. This message exploits the user's trust in ways that more obvious scams or attacks do not. It comes from a "friend". It looks innocuous and interesting. But the attached file compromises the user's computer system as soon as it is opened. The advanced attackers frequently use this method to compromise entire organizations. All it takes is the innocent click of a mouse by a single end-user and an entire company network is compromised. This is just one example of how attackers are leveraging human vulnerability and trust to exploit our networks.

As attackers target end users with tailored threats, security is becoming more decentralized and complex. This change in the attack methods has forced the evolution of Cyber-security products to provide the visibility required to detect and respond to these emerging threats. Current conventional safeguards such as patch management, vulnerability management, firewalls, anti-virus, and outsourced managed security services have yet to adapt to this new landscape.

## The State of Cyber-Security in the Private Sector

Most American organizations can secure their organizations from "consumer-grade" threats by adhering to industry standards and best practices. From a technical perspective, these attacks are conducted using exploits and techniques that are relatively stagnant, unchanging and preventable. It is my intent today to focus more on the growing prevalence of the advanced threats that we are not preventing or detecting. It is these advanced threats that are leading to material losses.

We believe it is reasonable to assume, if an advanced attacker targets your company, that a breach is inevitable. Let me offer some supporting reasons why we have reached this conclusion.

First, the sophisticated front-edge attacks that were previously reserved solely for Government targets have propagated to the private sector. We have witnessed the threat actors shift the application of their sophisticated tools, tactics, and procedures from US Government targets to corporate America. Many American corporations may have been compliant and diligent, but they were not prepared for advanced threats.

Second, we routinely witness attackers circumvent conventional safeguards deployed to prevent and detect security breaches. Virtually all of these intrusions belong to the growing subset of advanced threats that usually evade off-the-shelf technologies that American corporations rely upon – often times exclusively – for their defense. In fact, in over 90% of the cases we have responded to, Government notification was required to alert the company that a security breach was underway. In our last 50 incidents, 48 of the victim companies learned they were breached from the Federal Bureau of Investigation, the Department of Defense or some other third party.

Third, more attacks are coming from the "inside." These are not rogue employees or individual criminals within a company – rather, I refer to attacks that originate or pass through hundreds, if not thousands of trusted, reputable, blue chip American companies through the insertion of malware or other malicious programs onto existing corporate networks. The sheer volume of currently compromised organizations is an enormous contributing factor to our nation's cyber-vulnerability. The attackers consistently leverage the pre-existing infrastructure of compromised networks in the United States to attack and acquire new target companies.

It is common for the attackers to use information or IP addresses from their pre-existing victims to launch their attacks. A pattern that is emerging is that the attackers can compromise smaller companies with fewer security resources, and then "upgrade" their access from the smaller companies to the main target. This area of attack becomes even more pronounced in circumstances where large business "acquire" the infected networks through the corporate merger or acquisition of these smaller enterprises.

Fourth, the cyber threat evolves fast because there are currently few to no risks or repercussions for the attackers. If you can attack American networks with impunity, then the attacks are likely to continue. Without the ability to deter the attacks at the source, the attacker's advancement in capability continues unimpeded. During the last few years, the only deterrence we have seen the private sector embrace is their ability to raise the amount of time and cost an attacker must invest in order to breach their networks.

We also face a critical shortage of skilled security professionals dedicated to the defense of our networks, and imbalance in the resources – particularly shared information – available to those defenders. The unfortunate imbalance is that attacker's usually only need to breach your defenses once to accomplish their goals,

while the victim companies' cyber security staff must prevent 100% of the threats. The advantage usually goes to the attacker.

As a result of these five factors, corporate America continues to be routinely compromised by the growing prevalence of advanced threats, and our nation's intellectual property continues to flow into the wrong hands and erode our global competitiveness. However, there are steps we can take to turn the tide of this torrent of information loss.

## Stepping Up Our Game

To truly create and accelerate a coordinated defense of our system architecture and networks, we need to do more than block today's attacks. We need to promote a system that defends against emerging threats. In my view, this system requires three central attributes:

1- A policy to facilitate the sharing of threat intelligence.
2- Disclosure laws that foster useful outputs "for the greater good."
3- Substantial penalties for those actors who endanger our systems when attribution is possible.

### Sharing Threat Intelligence

It is a critical first principal that actionable intelligence and information is the cornerstone of building a strong cyber defense. We must institute a system that tracks tomorrow's threats and distributes information about those threats to the people on the front lines of this conflict. Both the government and some private sector companies have much of this information, and we need to devise a manner in which they can share actionable intelligence in a codified, standard way, that does not betray or diminish the effectiveness of our intelligence mission. If we do it right, sharing threat intelligence will promote an aggressive, dynamic, "learning system" of cyber-security for the nation. Effective intelligence sharing:

1 – Acts as a potential early warning system of significant threats.
2 – Promotes technologies that provide the situational awareness to use the threat intelligence effectively.
3 – Helps us establish policies to foster proactive detection of advanced compromises.
4 – Empowers the private sector to defend itself more aggressively.

The majority of threat intelligence is currently in the hands of the government. Indeed, more than 90% of the breaches MANDIANT responds to are first detected by the government, not the victim companies. That means that 9 in every 10 companies we assist had no idea they had been compromised until the government notified them.

The significance of that number cannot be overstated. With virtually every other crime, the victim is the first to know that they have been violated. Here, however, we have the government in the unique position of informing victims that they are, in fact, victims. For this to happen so frequently, the government must have access to a large amount of intelligence about the perpetrators of these crimes, their methods and their resources. Threat information, if shared consistently with the right people, could be used to prevent or suppress the impact of these breaches instead of merely notifying victims long after their intellectual property has been stolen.

Information sharing also needs to occur within and among private sector participants. While we have witnessed some advancement in coordination within the private sector, especially in the Defense Industrial Base and the Financial Services sectors, U.S. companies remain at a severe disadvantage until they can utilize all of the information available.

In promoting the sharing of threat intelligence, it is equally critical that we devise a means to standardize the information shared, so it can be provided "at network speed" with appropriate technologies to make use of the intelligence. We will need this codification of threats to safeguard the identities of victims and provide threat intelligence from anonymous sources. If we standardize how we communicate threat intelligence, we will expedite the implementation of our defenses, create more reliable and effective intelligence, and empower the private sector to share amongst themselves in a more productive manner.

Most organizations lack the visibility required to make use of comprehensive threat intelligence. If we enact policy that strongly promotes the sharing of threat intelligence, then we will also create incentives for the advancement and adoption of technologies that can use the information to safeguard our nation's secrets. When these technologies are available, we will see organizations proactively using threat intelligence to detect whether or not they are currently compromised. In short, by providing threat intelligence, we will promote a system where the public and private sector will perform a monthly ultrasound, looking for the evidence of compromises on our infrastructure.

Voluntary Breach Reporting Mechanism

The U.S. has no comprehensive security/data breach disclosure requirement. The current patchwork of laws, regulations, and private industry requirements purport to require disclosure, but often allow victim companies to exercise discretion in a manner that leads to secrecy and nondisclosure. This is unsurprising given the economic and reputational risk facing companies that choose to disclose breaches.

As we at MANDIANT see every day, security breaches are not necessarily evidence of lax security by a victim company. Consistent with that realization, Congress should consider instituting a voluntary breach reporting program that provides incentives in exchange for full disclosure by victim companies.

Incentives to participate in a voluntary reporting program could take many forms. As an initial matter, any such program would have to protect the identity of companies that report breaches. A true incentive, however, could come in the form of a limited safe harbor from liability associated with the breach.

This program would have to be independent from any breach notification obligation that may or may not trigger based on other criteria. By keeping the program separate from existing, more punitive breach notification laws, we could ensure the broad participation necessary to make the information sharing worthwhile. After all, corporate America may choose to hide from the stick, but steps up eagerly for a bite of the carrot.

Hold the Perpetrators Accountable

Unfortunately, there are adversaries who want to steal American intellectual property and other treasures. Until we as a nation determine how to hold these threat actors accountable, we will likely continue to get sucker-punched in cyberspace. We all must be mindful to know, as a Government, what we will do each time we are presented with the names and location of the perpetrators. Will we officially recognize the crimes these individuals performed against the American people? Will we work with the nations currently offering safe harbors to our attackers in order to mitigate these threats?

## Conclusion

Private industry is not always going to win the battle currently being fought in cyberspace. To gain ground against the increasingly numerous and sophisticated attacks draining this nation's most valuable assets, we must encourage and facilitate the public/private exchange of intelligence, enabling private industry to protect itself in cyberspace.

By establishing a system where the private and public sectors share and proactively use threat intelligence, America will build a dynamic cyber-defense system that grows smarter and more capable by the day.

Thank you very much, Mr. Chairman.