**WRITTEN TESTIMONY OF**

MANDIANT®

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

**BEFORE THE**

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

# ADVANCED CYBER THREATS FACING OUR NATION

**FEBRUARY 14, 2013**

## Introduction

Thank you Mr. Chairman, Ranking Member Ruppersberger, and Members of the Committee, for another opportunity to share my observations and experience with you. As I indicated in my testimony before this Committee in October, 2011, security breaches are inevitable. Unfortunately, there currently exists a sizeable gap between what our safeguards can prevent and the ability of motivated attackers to circumvent those safeguards. While the United States cannot stop each and every cyber security breach, we can resist these attacks fiercely and effectively.

Today, I will discuss why the security gap exists, and how sharing threat intelligence can narrow this security gap to more tolerable levels. My suggestions will, if implemented, both decrease the number of effective attacks against the United States and significantly mitigate the damage caused by those attacks we cannot prevent.

## Background

Following several years as a Computer Security Specialist and 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 at dozens of the largest American companies and other organizations important to our nation, including attacks at the *New York Times* and the *Washington Post*.

Mandiant has responded to incidents at hundreds of companies. We have investigated millions of systems, and we receive calls almost every single day from companies that have suffered a cyber-security breach. These cyber intrusions continue to impact virtually every industry, including law firms, financial services, blue chip American manufacturers, retailers, the defense industrial base, telecommunications, space and satellite and imagery, cryptography and communications, government, mining, software and many others. I have witnessed the unique threats facing each of these sectors, and continue to help companies respond to these advanced cyber threats.

## Why the Security Gap Exists

Through my experience in combating cyber threats, I have seen firsthand the methods attackers use as they seek to undermine and exploit our nation's infrastructure. Simply put, these sophisticated threats have evolved faster than our ability or willingness to reliably safeguard our assets.

Most American organizations can secure their networks 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 well known and preventable. These attacks are usually not advanced enough to exploit the gap in our security.

Today, I focus instead on the advanced threats that we are not preventing or detecting. It is reasonable to assume that, if an advanced attacker targets your company, a breach is inevitable. That surprises many people, but it is the undeniable truth, and a direct result of the gap between our ability to defend ourselves and our adversaries’ ability to circumvent those defenses. There are at least six reasons why attackers continue to successfully exploit this gap in security:

First, the sophisticated, cutting-edge attacks that were previously reserved solely for government targets have spread to the private sector. Advanced threat actors have shifted the application of their sophisticated tools, tactics and procedures from U.S. Government targets to corporate America. Many American corporations, though compliant with cyber-security regulations and best practices, were not prepared for these advanced threats.

Second, the attackers are targeting people, not computer systems. While previous generations of attacks targeted technology and exploited vulnerabilities in software, attackers have now evolved to target human inadequacies and weaknesses. 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 personal blogs and sites such as Facebook, Google+, LinkedIn and Twitter, attackers are able to target their attacks at individuals. These personalized attacks are difficult to detect and prevent because they exploit human vulnerabilities and human trust.

Third, more attacks are coming from the “inside.” Advanced attackers consistently leverage the pre-existing infrastructure of compromised networks in the United States to target and attack new companies. It is common to see attackers compromise smaller companies with fewer security resources, and then “upgrade” their access from the trusted, smaller companies to the main target. This is also a problem where large businesses “acquire” the infected networks through a corporate merger or acquisition of these smaller enterprises.

The fourth reason attacks continue to be successful involves the imbalanced nature of cyber attacks and the number of defenders in the U.S. A single attacker can generate work for hundreds, if not thousands of defenders. Also, while a single attacker need only breach his target’s defenses once to accomplish his goals, the victim company’s entire cyber security staff must attempt to prevent 100% of the threats. This imbalance is compounded by the critical shortage of skilled security professionals here in the U.S.

Fifth, many advanced attackers reside in nations that not only refuse to hold attackers accountable for their crimes, but provide resources and direction to the attackers.  So long as state-sponsored criminals can infiltrate American networks and steal American intellectual property without risks or repercussions, these attacks will continue unabated.

Finally, one of the most valuable resources in detecting and responding to cyber-attacks – accurate and timely threat intelligence – is often unavailable to many defenders.  The U.S. needs an effective framework for sharing information among commercial entities, and between corporate America and the government.  Too often attackers are finding success using resources and methods that are known by some, but have not been shared with potential victims because of a lack of authority and mechanisms to accomplish the communication.

As a result of these six factors, corporate America continues to be routinely compromised by the growing prevalence of advanced threats. However, there are steps we can take to significantly narrow the security gap and increase the costs and effort required to steal our intellectual capital.

## How Sharing Intelligence Will Narrow the Security Gap

We need to promote a system that helps companies defend against emerging threats.  In my view, this system requires a strong national policy that promotes the sharing of threat intelligence and protects companies that share this valuable information.

We must establish a system that tracks the most recent advanced 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 create a way in which they can share actionable intelligence in a standard, codified, machine-readable 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 an early warning system giving potential victims advance notice of significant threats;

2 – Promotes technologies that facilitate the effective use of threat intelligence;

3 – Empowers the private sector to defend itself more effectively; and

4 – Significantly reduces the duration and impact of breaches, should they occur.

The private sector cannot do this alone. While many industry players have extremely capable security programs, the majority of threat intelligence is currently in the hands of the government. Indeed, about two-thirds of the breaches Mandiant responds to are first detected by a third party – usually the government – not the victim companies. That means that a majority of the companies we assist had no idea they had been compromised until law enforcement or a business partner 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 mitigate 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 access and 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” to make timely use of the intelligence. We will need this codification of threats to effectively safeguard the identities of victims and share freely 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. Fortunately, we have seen many organizations adopt Mandiant’s OpenIOC format and compatible standards like the STIX schema from NIST, accelerating the intelligence sharing process.

Most organizations lack the ability to make effective use of comprehensive threat intelligence. If we implement policy that promotes the sharing of threat intelligence, then we will also create incentives for the advancement and adoption of technologies that can use that information to safeguard our nation’s secrets. By facilitating the free but careful flow of threat intelligence, we will promote a system that enables the public and private sector to perform the equivalent of a routine cyber-ultrasound, looking for evidence of compromise on our infrastructure.

## Conclusion

In conclusion, while private industry will not always win the battles being fought in cyberspace, we can drastically narrow the security gap by sharing threat intelligence.  To gain ground against the increasingly numerous and sophisticated attacks draining this nation of its most valuable assets, we must encourage and facilitate the public/private exchange of threat intelligence, enabling private industry to protect itself in cyberspace.  By establishing a system where the private and public sectors share and proactively use accurate and timely 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.