

Statement for the Record

Richard Bejtlich

Chief Security Strategist

FireEye, Inc.

Before the

U.S. House of Representatives Committee on Oversight and  
Government Reform Subcommittee on Information Technology

Cybersecurity:

The Evolving Nature of Cyber Threats Facing the Private Sector

March 18, 2015

Chairman Hurd, members of the Committee, thank you for the opportunity to testify. I am Richard Bejtlich, Chief Security Strategist at FireEye. I am also a nonresident senior fellow at the Brookings Institution, and I am pursuing a PhD in war studies from King's College London. I began my security career as a military intelligence officer in 1997 at the Air Force Information Warfare Center.

My employer, FireEye, provides software to stop digital intruders, with 3,100 customers in 67 countries, including 200 of the Fortune 500. Our Mandiant consulting service, known for its 2013 report on Chinese PLA Unit 61398, helps companies identify and recover from intrusions.

Today I will discuss digital threats, how to think about risk, and some strategies to address these challenges.

Who is the threat?

We have discovered and countered nation-state actors from China, Russia, Iran, North Korea, Syria, and other countries. The Chinese and Russians tend to hack for commercial and geopolitical gain. The Iranians and North Koreans extend these activities to include disruption via denial of service and sabotage using destructive malware. Activity from Syria relates to the regional civil war and sometimes affects Western news outlets and other victims. Eastern Europe continues to be a source of criminal operations, and we worry that the conflict between Ukraine and Russia will extend into the digital realm.

Threat attribution, or identifying responsibility for a breach, depends on the political stakes surrounding an incident.<sup>1</sup> For high-profile intrusions, such as those in the news over the last few months, attribution has been a priority. National technical means, law enforcement, and counter-intelligence can pierce anonymity. Some elements of the private sector have the right experience and evidence to assist with this process. Attribution is possible, but it is a function of what is at stake.

Who is being breached?

---

<sup>1</sup> Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *The Journal of Strategic Studies*, 2014; <http://bit.ly/attributing-cyber-attacks>

In March 2014, the Washington Post reported that in 2013, federal agents, often the FBI, notified more than 3,000 U.S. companies that their computer systems had been hacked.<sup>2</sup> This count represents clearly identified breach victims. Many were likely compromised more than once.

Serious intruders target more than government, defense, and financial victims. No sector is immune. FireEye recently published two reports, showing that 96% of organizations we could observe had suffered compromise during two six-month periods.<sup>3</sup> The best performing sector was aerospace and defense, with “only” 76% of sampled organizations suffering a breach. All of the retail, automotive, transportation, healthcare, pharmaceutical, construction, and engineering clients we passively monitored over a six-month period were breached at least once.

In 2014, the top sectors assisted by our Mandiant consultants included business and professional services, finance, media and entertainment, and construction and engineering. Many of these attacks are driven by strategic national imperatives. For instance, we anticipate that certain foreign governments will continue to steal clean energy and biotechnology solutions, so long as their citizens suffer polluted cities and rising cancer rates. Some actors specifically target the healthcare sector. Criminal groups appear to steal data for financial gain, while nation-state hackers may steal data to improve the healthcare systems of their own countries, or to support national commercial champions.

How are victims breached?

Intruders use spear phishing, attacks against Internet-connected devices, and other methods to compromise victims. Last year we observed a rise in the proportion of phishing emails that impersonated IT staff, from 44% in 2013 to 78% in 2014.<sup>4</sup> The threat is going mobile as well. We recently completed a study of vulnerable mobile applications that can hijack entire devices, without the user’s knowledge. We have seen malicious applications, pretending to offer banking services, harvest credentials and steal two-factor authentication codes and virtual private network passwords.

---

<sup>2</sup> Ellen Nakashima, “U.S. notified 3,000 companies in 2013 about cyberattacks,” Washington Post, March 24, 2014; [http://www.washingtonpost.com/world/national-security/2014/03/24/74aff686-aed9-11e3-96dc-d6ea14c099f9\\_story.html](http://www.washingtonpost.com/world/national-security/2014/03/24/74aff686-aed9-11e3-96dc-d6ea14c099f9_story.html)

<sup>3</sup> [https://www.fireeye.com/blog/executive-perspective/2015/01/the\\_maginot\\_linedee.html](https://www.fireeye.com/blog/executive-perspective/2015/01/the_maginot_linedee.html)

<sup>4</sup> [https://www.fireeye.com/blog/threat-research/2015/02/get\\_a\\_view\\_from\\_the.html](https://www.fireeye.com/blog/threat-research/2015/02/get_a_view_from_the.html)

How do victims learn of a breach?

In 70% of cases, someone else, likely the FBI, tells a victim about a serious compromise. Only 30% of the time do victims identify intrusions on their own. The median amount of time from an intruder's initial compromise, to the time when a victim learns of a breach, is currently 205 days, as reported in our 2015 M-Trends report. This number is better than our 229 day count for 2013, and the 243 day count for 2012.<sup>5</sup> Unfortunately, it means that, for nearly 7 months after gaining initial entry, intruders are free to roam within victim networks.

What is the answer?

Before talking about solutions to digital risk, we need to define it. Always ask "Risk of what?" Are we talking about the risk of a teenager committing suicide due to "cyber bullying," or the risk of a retiree's 401k being emptied due to electronic theft, or the risk of a week-long power outage due to state-sponsored attack?

Step one is to define the risk, and step two is to measure progress by combining ways and means to achieve defined ends. This is exactly the role of strategic thinking, meaning the application of strategies, campaigns, tactics and tools to achieve organizational goals.

For example, a company may worry about the risk of losing intellectual property to foreign hackers. The board and management team works with the chief security officer (CSO) to define a company goal of minimizing loss due to digital intrusions. To accomplish the goal, they agree on a strategy of rapid incident detection and response. To achieve the strategy, the CSO develops a campaign to hunt for intruders in the company using network security monitoring (NSM) operations. To prosecute the campaign, the security team implements tactics to collect, analyze, escalate, and resolve intrusions based on NSM principles. Finally, the security team uses tools, or security software, to bring their tactics to life.<sup>6</sup>

---

<sup>5</sup> <https://www.mandiant.com/resources/mandiant-reports/>

<sup>6</sup> <http://taosecurity.blogspot.com/search/label/strategy>

To measure success, the security team should track the number of intrusions that occur per year, and the amount of time that elapses from the initial entry point to the time of discovery, and from the time of discovery to the removal of the threat. This strategic approach is the reason Mandiant calculates these metrics when helping breach victims.

Security professionals define Risk as the product of Threat, Vulnerability, and Cost, which is the impact of a security incident. We use a pseudo-equation where  $R = T \times V \times C$ . We're not trying to calculate a number. We're trying to show how Threat, Vulnerability, and Cost influence Risk. If any factor increases, Risk increases, and if any factor decreases, Risk decreases. We appear to live in an environment where Threat, Vulnerability, and Cost continue to rise, driving up Risk, but note that reducing any component -- Threat, Vulnerability, or Cost -- helps lower Risk.

Too often the more engineering-focused members of the security community fixate on Vulnerability. We hear of "game-changing technologies" promising to remove flaws, reduce attack surfaces, and so on. While I accept the need for more secure software, we must not neglect the role of reducing the Threat and the Cost they impose.

Law enforcement and counter-intelligence operations are the primary means by which we can mitigate the Threat. In an editorial for the Brookings Institution titled "Target Malware Kingpins," I asked "what makes more sense: expecting the two billion Internet users worldwide to adequately secure their personal information, or reducing the threat posed by the roughly 100 top-tier malware authors?"<sup>7</sup> Along those lines, I applaud the FBI's recent announcement of a \$3 million bounty for information leading to the arrest of a Russian hacking suspect who stole more than \$100 million since 2011.<sup>8</sup>

Reducing the Cost of security incidents takes somewhat more creative approaches. One step in progress is the "tokenization" of the payment card system, whereby strings of numbers, or "tokens," replace traditional credit card numbers. A second step would be eliminating the value of Social Security numbers to identify thieves. I recommend reading the Electronic Privacy Information Center's suggestions on "effective SSN legislation" for policy changes.<sup>9</sup>

---

<sup>7</sup> Richard Bejtlich, "Target Malware Kingpins," The Brookings Institution; <http://www.brookings.edu/research/opinions/2015/02/02-cybersecurity-target-malware-kingpins-bejtlich>

<sup>8</sup> <http://www.fbi.gov/wanted/cyber/evgeniy-mikhailovich-bogachev>

<sup>9</sup> <https://epic.org/privacy/ssn/>

In brief, defenders win when they stop intruders from achieving their objectives. It's ideal to stop the adversary from entering the network, but that goal is increasingly difficult. If traditional defenses fail, you must quickly detect the intrusion, and respond to contain the adversary, before he steals, changes, or destroys the data or system under attack.

Finally, we must appreciate that the time to find and remove intruders is now. There is no point in planning for theoretical, future breaches until you know your own, current, security posture. If a company hired me to be their CSO, the first step I would take would be to hunt for intruders already in the network.

I look forward to your questions.

# Richard Bejtlich

Chief Security Strategist at FireEye, Inc.

taosecurity@gmail.com

---

## Summary

Richard Bejtlich is Chief Security Strategist at FireEye, and was Mandiant's Chief Security Officer when FireEye acquired Mandiant in 2013. He is a nonresident senior fellow at the Brookings Institution, a board member at the Open Information Security Foundation, and an advisor to Threat Stack, Sqrrl, and Critical Stack. He is also a Master/Doctor of Philosophy in War Studies Researcher at King's College London. He was previously Director of Incident Response for General Electric, where he built and led the 40-member GE Computer Incident Response Team (GE-CIRT). Richard began his digital security career as a military intelligence officer in 1997 at the Air Force Computer Emergency Response Team (AFCERT), Air Force Information Warfare Center (AFIWC), and Air Intelligence Agency (AIA). Richard is a graduate of Harvard University and the United States Air Force Academy. His fourth book is "The Practice of Network Security Monitoring" ([nostarch.com/nsm](http://nostarch.com/nsm)). He also writes for his blog ([taosecurity.blogspot.com](http://taosecurity.blogspot.com)) and Twitter (@taosecurity).

---

## Experience

### **Master/Doctor Of Philosophy In War Studies Researcher at King's College London**

August 2014 - Present (7 months)

Researching application of strategic thought, especially operational art, to counter-intrusion campaigns.

The research will identify elements of a successful computer network defense campaign, inspired by both classical and modern thinkers.

### **Advisor at Critical Stack**

August 2014 - Present (7 months)

Advises Critical Stack on business strategy, product opportunities, communications, and other commercial organizational issues.

### **Advisor at Sqrrl**

June 2014 - Present (9 months)

Advises Sqrrl on business strategy, product opportunities, communications, and other commercial organizational issues.

### **Chief Security Strategist at FireEye, Inc.**

January 2014 - Present (1 year 2 months)

Empowers policy makers, international leaders, global customers, and concerned citizens to understand and mitigate digital risk through strategic security programs.

**Nonresident Senior Fellow at The Brookings Institution**

January 2014 - Present (1 year 2 months)

Researches integrating strategic thought into private sector cyber defense. Investigates the extent to which detection and response scales beyond the enterprise.

**Advisor at Threat Stack, Inc**

October 2013 - Present (1 year 5 months)

Advises Threat Stack on business strategy, product opportunities, communications, and other commercial organizational issues.

**Board Member at The Open Information Security Foundation**

March 2011 - Present (4 years)

Advises OISF on business strategy, product development, communications, and other non-profit organizational issues. Advocates use of OISF open source software like Suricata to complement computer security programs worldwide.

**Chief Security Officer at Mandiant**

April 2011 - January 2014 (2 years 10 months)

Managed Mandiant's digital risks, advocated defenses against advanced threats, and helped customers detect and respond to intrusions using the company's methods, products, and services. Transitioned to FireEye after acquisition of Mandiant in December 2013.

**Director, Incident Response at General Electric**

July 2007 - April 2011 (3 years 10 months)

Built and led GE Computer Incident Response Team (GE-CIRT, [ge.com/cirt](http://ge.com/cirt)) from 0 to 40 analysts, defending 300,000 employees and 500,000 nodes in over 100 countries.

**President & CEO at TaoSecurity LLC**

June 2005 - June 2007 (2 years 1 month)

Provided independent digital security consulting and services for military, government, and commercial clients worldwide.

*I recommendation available upon request*

**Technical Director at ManTech International Corp.**

February 2004 - June 2005 (1 year 5 months)

Performed computer forensics and intrusion analysis for government clients, and network security monitoring for corporate customers.

**Principal Consultant at Foundstone**

April 2002 - January 2004 (1 year 10 months)

Led incident response engagements for Fortune 100, tier one ISPs, and other organized crime and corporate espionage victims.



*1 recommendation available upon request*

**Senior Security Engineer at Ball Aerospace & Technologies Corp.**

February 2001 - April 2002 (1 year 3 months)

Designed, hired, trained, and led a twelve-person, 24x7 team to detect intrusions on commercial networks.

**Chief, Real Time Intrusion Detection at AFCERT**

September 1998 - February 2001 (2 years 6 months)

Led Air Force CERT's security monitoring mission, supervising 60 civilian and military staff; conducted hands-on technical analysis.

*2 recommendations available upon request*

**Intelligence Officer at Air Intelligence Agency**

February 1997 - September 1998 (1 year 8 months)

Created and coordinated information warfare plans and policies, and executed operations during Bosnia conflict.

---

## Skills & Expertise

**Computer Forensics**

**Intrusion Detection**

**Corporate Security**

**Security Operations**

**Security Services**

**Managed Security Services**

**Cyber Security**

**Security Management**

**Information Security Management**

**Internet Security**

**CISSP**

**Computer Security**

**Network Security**

**Security Research**

**Network Forensics**

**Security**

**IDS**

---

## Patents

**Network intrusion detection visualization**

United States Patent Application 20110067106

Inventors: Richard Bejtlich, Scott Evans, Et al

**Network attack visualization and response through intelligent icons**

United States Patent Application 20110066409

Inventors: Richard Bejtlich, Scott Evans, Et al

---

## Publications

### **The Practice of Network Security Monitoring**

No Starch July 22, 2013

Authors: Richard Bejtlich

In *The Practice of Network Security Monitoring*, Mandiant CSO Richard Bejtlich shows you how to use NSM to add a robust layer of protection around your networks — no prior experience required. To help you avoid costly and inflexible solutions, he teaches you how to deploy, build, and run an NSM operation using open source software and vendor-neutral tools.

### **Extrusion Detection**

Addison-Wesley November 8, 2005

Authors: Richard Bejtlich

### **Real Digital Forensics**

Addison-Wesley September 23, 2004

Authors: Richard Bejtlich, Keith Jones, Curtis Rose

### **The Tao of Network Security Monitoring**

Addison-Wesley July 12, 2004

Authors: Richard Bejtlich

---

## Education

### **Air Force Intelligence Officers Training Course**

14N1, Military intelligence, 1996 - 1997

### **Harvard University, John F. Kennedy School of Government**

Master of Public Policy (MPP), National Security, 1994 - 1996

### **United States Air Force Academy**

Bachelor of Science (BS), History, Political Science, 1990 - 1994

Grade: 3rd of 1024

Activities and Societies: French and German minors

---

**Committee on Oversight and Government Reform**  
**Witness Disclosure Requirement – “Truth in Testimony”**  
**Required by House Rule XI, Clause 2(g)(5)**

Name: **Richard Bejtlich**

---

1. Please list any federal grants or contracts (including subgrants or subcontracts) you have received since October 1, 2012. Include the source and amount of each grant or contract.

FireEye has multiple contracts with numerous US Federal government agencies and foreign governments for cybersecurity products and services which are relevant to the subject matter of this hearing. Pursuant to these agreements, FireEye is subject to non-disclosure provisions.

---

2. Please list any entity you are testifying on behalf of and briefly describe your relationship with these entities.

I represent my employer, FireEye, Inc.

---

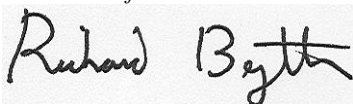
3. Please list any federal grants or contracts (including subgrants or subcontracts) received since October 1, 2012, by the entity(ies) you listed above. Include the source and amount of each grant or contract.

FireEye has multiple contracts with numerous US Federal government agencies and foreign governments for cybersecurity products and services which are relevant to the subject matter of this hearing. Pursuant to these agreements, FireEye is subject to non-disclosure provisions.

---

*I certify that the above information is true and correct.*

Signature:



Date: 2 March 2015

---