

FRED UPTON, MICHIGAN
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115
Majority (202) 225-2927
Minority (202) 225-3641

March 27, 2015

Mr. Richard Bejtlich
Chief Security Strategist
FireEye
2318 Mill Road, Suite 500
Alexandria, VA 22314

Dear Mr. Bejtlich:

Thank you for appearing before the Subcommittee on Oversight and Investigations on Tuesday, March 3, 2015, to testify at the hearing entitled "Understanding the Cyber Threat and Implications for the 21st Century Economy."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on Friday, April 10, 2015. Your responses should be mailed to Brittany Havens, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515 and e-mailed in Word format to brittany.havens@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,



Tim Murphy
Chairman
Subcommittee on Oversight and Investigations

cc: The Honorable Diana DeGette, Ranking Member, Subcommittee on Oversight and Investigations

Attachment

Attachment—Additional Questions for the Record

The Honorable Tim Murphy

1. Each witness provided a slightly different perspective on cyber threats and the challenge of cybersecurity, extending from the past, to the present and future.
 - a. Are there areas where you feel there is a common view or shared theme and what is it?
 - b. If there was one fundamental message you want Congress and the public to understand about cybersecurity, what would it be?
 - c. Are there specific issues or areas of this issue that do not receive an appropriate level of attention?
2. As the promise of innovation connects more of our lives to cyberspace – from smart pacifiers to cars that communicate with each other – cyberspace becomes, in theory, a limitless attack surface.
 - a. How do we manage the risks presented by “smart devices” and the Internet of Things while also enjoying the benefits and convenience they offer to society?
 - b. As more devices connect to cyberspace and interact with one another, what challenges does this present for how security professionals or companies anticipate potential vulnerabilities or risks?
 - c. How do we assess the security of individual products relative to the security of the system as a whole?
 - d. In such an interconnected world, how do you draw the line between a potential vulnerability and a realistic vulnerability? In other words, just because something is possible, how important is it to assess the probability that it will occur?
3. Quite a few respected technologists – at Google, and also at the Institute of Electrical and Electronics Engineers Computing Society – have theorized that in the future, the Internet will be so integrated into our daily lives that it will become “invisible” and provide “seamless intelligence.”
 - a. Can you expand a little more on how exactly a world with an “invisible” Internet would work?
 - b. Do you agree with these predictions? Why or why not?
4. No matter how much money a company invests in security software, training and other cybersecurity measures, they still remain vulnerable to the insider threat. This can range from the intentional actor – such as a disgruntled employee stealing information or letting

the bad guys in – to inadvertent actors – such as an employee clicking an infected link in a targeted phishing email.

- a. Will companies ever be able to prevent internal threats – employees lowering the proverbial draw bridge – regardless of whether their actions are intentional or unintentional?
 - b. If it can never be eliminated, does it come down to managing risk? Are there proven strategies to minimize this risk?
 - c. How significant of a challenge is this to those evaluating the cost benefit of security measures?
5. Information sharing, though it has its benefits, is still a reactionary solution. Someone has to first suffer an attack before that threat information can be shared, and oftentimes the attackers change their signatures from target to target.
- a. How does information sharing help reduce the gap between cybersecurity capabilities and threats to cybersecurity described in Dr. Lin's testimony?
 - b. There is a lot of focus on signatures when it comes to information sharing.
 - i. Are signature-based defenses effective? Why or why not?
 - c. How does information sharing fit into the broad picture of the cybersecurity challenge?
 - i. Does it offer opportunity beyond improving our defensive capabilities?
6. Is it possible to quantify the benefits of the Internet and information technology relative to the cost of security?
- a. In other words, is it possible to calculate the economic benefits of these technologies relative to the economic costs of cybersecurity, including prevention and response in the event of a breach?
 - b. How about the social, cultural or other less tangible benefits?
 - c. Is there value in this?
7. Discussions about cybersecurity often focus on prevention or keeping actors out of system - Is this the right way to approach this issue?
- a. If there is no guarantee the bad guys will not get in, should the emphasis shift to a focus on resilience rather than prevention?
 - b. Why is the concept of resilience important to effective cybersecurity?

- c. How does resilience support a risk-based approach to cybersecurity?
 - d. Based on your experience, are companies adopting a risk-based approach to cybersecurity – whether it is the NIST framework or a similar model?
 - i. Do you have a rough approximation of how prevalent this is? Is it the dominant approach? Increasing?
 - ii. Does this vary by industry or size of company?
 - 1. If so, what are the driving factors?
8. In Dr. Lin’s written testimony he stated that “complexity is the enemy of cybersecurity.”
- a. Do you agree with this assessment?
 - b. Is it possible to reduce this complexity?
 - i. If yes, what are the consequences?
 - ii. If no, why not?
9. In the last few years, there have been several significant compromises and vulnerabilities discovered in regards to digital certificates and Certificate Authorities, two of the best well-known being the compromise of DigiNotar and the recent Lenovo/Superfish revelations. This raises questions as to whether the digital certificate model is providing an adequate level of security for users of the Internet.
- a. What are the weaknesses in the digital certificate model?
 - i. How significant are these weaknesses?
 - ii. Can these weaknesses be eliminated or adequately mitigated?
 - b. Are Certificate Authorities subject to any form of oversight?
 - i. If so, by whom and how does this function?
 - ii. If not, would enhanced oversight help address the weaknesses examined in Question 1? Why or why not?
 - c. Are there alternatives to the digital certificate model?
 - i. If so, what are they?
 - ii. If not, how can the current digital certificate ecosystem be improved?
10. In your testimony, you discussed the attribution of threats, and how it is a function of “what is at stake.”

- a. What are the factors that influence the success of attribution, especially if a breach is not considered high-profile?
 - b. How does attribution of the threat help a company or organization recover from a breach?
 - c. What makes attribution so difficult?
11. We often hear about intrusions that effect consumer data but we don't often hear about the threats to Intellectual Property.
 - a. How prevalent are the threats to Intellectual Property?
 - b. How does the economic impact of Intellectual Property theft compare to something like the theft of consumer data?
 - c. Is it possible to quantify the economic effect of stolen Intellectual Property?
 - d. Please describe the types of cyber threats to the U.S. economy (e.g. IP theft, theft of consumer data, etc.) and, to the extent possible, rank them in terms of severity of economic impact.
12. You stated in your written testimony that the average breach goes undetected for nearly seven months, and that we have only gotten marginally better at identifying intrusions over the last three years (38 day reduction).
 - a. Why is it so challenging to identify these threats once they are in a system or network?
 - i. Are certain sectors better at identifying vulnerabilities than others?
 - ii. Is there variation based on the size of the company? If so, why?
 - b. Once a breach is identified, how difficult is it to remediate the threat?
 - i. Based on your experience, do you have a sense of how long, on average, this process takes?
 - c. If it is so difficult and time consuming to identify and remove bad guys from a system, how can we ever expect to keep pace with the threats?
13. In your testimony you described an equation that defines risk as the product of threat, vulnerability and cost. When any of those three factors increase, so does risk, and vice versa. You also described the pitfalls of focusing too heavily on any one factor, like vulnerability. We hear quite a bit about C-suite executives who worry primarily about the cost of security, and about Chief Information Officers and Chief Information Security Officers who worry primarily about vulnerabilities.

- a. Do you believe that this mismatch of priorities is part of the reason why cybersecurity is such a difficult problem to approach?
- b. How can executives and security professionals reconcile their different priorities and views?

The Honorable Markwayne Mullin

1. I know you probably wouldn't naturally associate Oklahoma with advanced cybersecurity, but Oklahoma's Cyber Command Security Operations Center is considered one of the most advanced state security systems out there. Last week, I had a chance to speak with our Chief Security Officer, Mark Gower and Dr. Jerry Dawkins of True Digital Security, which is based out of Tulsa. One of the topics that came up in both of these conversations was how cyber threats are particularly harmful to small and medium-sized businesses. When my wife and I went into business 17 years ago, cybersecurity was pretty low on the list of things we worried about. Mr. Bejtlich, can you briefly speak to the challenges that a small or medium-sized business faces when it comes to cybersecurity that a large business might not have to deal with?
2. What advice would you give to an entrepreneur opening up, say, a retail shop or restaurant?
3. How can businesses be sure that their vendors understand their specific cybersecurity issues and will develop a system that will provide protection?
4. Would you say that security breaches we see in small businesses are an IT problem or a business problem?