Response to Questions

from the

U.S. House of Representatives

Committee on Energy and Commerce

Subcommittee on Oversight and Investigations

by

Richard Bejtlich

Chief Security Strategist

FireEye, Inc.

13 April 2015

Thank you for the opportunity to answer questions for the record, prompted by the hearing "Understanding the Cyber Threat and Implications for the 21st Century Economy," 3 March 2015. I have answered those that fall within my area of expertise, to the best of my ability.

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?**

"Cyber security" is as expansive a topic as "health" or "crime" or "war." No one achieves a level of excellence, or approaches some degree of understanding, without concentrating on one or two specialties. One can approach the topic from different levels, such as technology, tactics, operations, strategy, and policy. There are few, if any, shared definitions, measurements of success, or even terminology. There is no digital security equivalent to the "Generally Accepted Accounting Principles" (GAAP) of the financial world.

Given this background, it is difficult to find shared themes. However, many security professionals would agree that, in the digital world, offensive actors have an inherent advantage over defensive actors.

    b. **If there was one fundamental message you want Congress and the public to understand about cybersecurity, what would it be?**

Constituents should expect organizations to be compromised by malicious actors. However, it is the speed and quality of the incident detection and response process that determines if the intrusion results

in serious damage to the organization or the information it holds. Defenders win when they stop intruders from accomplishing their mission, not necessarily because defenders keep every invader from gaining unauthorized access.

All organizations should prioritize identifying and removing intruders from their networks. Only after an organization makes incident detection and response the primary security focus should they allocate resources to preventive measures, such as by mitigating software vulnerabilities and misconfigurations. Intruders are already infiltrating targets. It does no good to build higher walls when an invader is already on the inside.

Unfortunately, it is impossible for all organizations to defend themselves using this strategy. Every organization connected to the Internet cannot individually defend itself from mid- to high-level threat actors, such as organized criminal groups and nation-state hacking units. Only the best-resourced, best-led, and best-postured organizations can successfully implement a strategy that frustrates adversary operations.

This situation is not unique to the digital world. One finds the same situation in the physical world. Therefore, we must apply the same range of defensive measures found in the physical world, and abandon the notion that technical measures alone will "solve" the problem. I agree with the message in Bruce Schneier's book Liars and Outliers. He asserts that technical solutions, or "security systems," constitute about 10% of risk mitigation in the physical world. The remaining 90% is a result of "societal pressures," namely moral, reputational, and institutional forces. We must apply more of these other forces to digital security, and stop expecting technical systems to implement most of the security we need in cyber space.

c. Are there specific issues or areas of this issue that do not receive an appropriate level of attention?

Congress should support research for a United States Cyber Corps, or Cyber Guard. Possible roles for this organization include helping domestic and foreign allied organizations defend themselves in cyberspace. Research would determine if this group is needed, and how it would be organized, trained, and equipped.

Congress should also support research for a United States Cyber Force. This unit would be the next step for the existing Cyber Command. Research would determine if this group is needed, and how it would be organized, trained, and equipped.

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?

As a starting point, all vendors should adopt secure software development lifecycles, and other practices, from the Building Security In Maturity Model (www.bsimm.com). Organizations processing information should adopt the Critical Security Controls (www.counciloncybersecurity.org/critical-controls) and consider cyber insurance to better manage risk.

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?

Digital security is not strictly a technical problem. Many elements of society can play a role. We need to write histories of security incidents to provide examples for students, practitioners, and policy makers. We need courses and seminars that teach business and agency executives how to lead organizations under constant digital attack. We need to support the development of research-driven and field-tested strategies to defend information and users.

c. How do we assess the security of individual products relative to the security of the system as a whole?

Assuming the developers build software following principles such as BSIMM, the next step should be inviting security researchers to test software using bug bounties and similar exercises. Once deployed in the field, owners must monitor interactions with the software. Vendors must provide responsive support mechanisms to accept and act on security problems discovered in real-life conditions.

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?

History has shown that, over time, someone will identify and eventually exploit vulnerabilities in all software. The more popular the product, the more scrutiny it will receive.

Therefore, developers and owners must prioritize the attention they give to the most critical systems and data. It is more important to develop and defend a system that operates industrial control systems, or that processes financial or sensitive personal data, than it is to develop and defend an Internet-connected toy. While it may be possible to exploit an Internet-connected toy to gain access to more important resources, defenders must prioritize their time and effort.

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?

No comment. Please ask the original source.

b. Do you agree with these predictions? Why or why not?

No comment.

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?

No. If it is possible for an authorized user to access an information resource, it is possible for an unauthorized user to eventually do so as well.

b. If it can never be eliminated, does it come down to managing risk? Are there proven strategies to minimize this risk?

I recommend referencing the The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (resources.sei.cmu.edu/library/asset-view.cfm?assetID=30310).

Everyone is familiar with the insight that an intruder only needs to exploit one victim in order to compromise the enterprise.

However, few are familiar with the insight that the defender only needs to detect one of the indicators of the intruder's presence in order to initiate incident response within the enterprise.

I call this situation the "intruder's dilemma" (taosecurity.blogspot.com/2009/05/defenders-dilemma-and-intruders-dilemma.html). Therefore, one defensive strategy is to audit and log user actions, thereby introducing more artifacts that an attacker must avoid creating in order to remain stealthy.

A second strategy is to reduce the amount and value of data collected by an organization, and to compartmentalize access to the data that remains.

c. How significant of a challenge is this to those evaluating the cost benefit of security measures?

It is a question of relative risk. The likelihood of an insider event is statistically less than that of an outsider event. However, insiders cause more damage in some cases. Also, once within a network, outsiders often act and appear as insiders.

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?

Threat intelligence can help defenders more quickly resist, identify, and respond to intrusions, but only if the organization is postured to succeed. Until one invests in sound strategy, processes, people and technology, no amount of information sharing or threat intelligence will be sufficient.

I recommend organizations start their information sharing programs by taking advantage of free offerings. For example, Critical Stack (www.criticalstack.com) provides a marketplace for nearly 60 free intelligence feeds (intel.criticalstack.com). Defenders can integrate these sources before evaluating commercial sources.

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?

Some aspects of intruder activity can be codified into signatures. When defenders apply these signatures to threat activity, they can identify and perhaps stop some malicious behavior. Intruders, however, learn to bypass many signature-based approaches. In those cases, defenders need to use tactics, techniques, and technologies that do not rely on signatures. For example, so-called detonation chambers can safely execute malicious code, observe subsequent behavior, and derive new ways to detect and stop intrusions.

c. How does information sharing fit into the broad picture of the cybersecurity challenge?

i. Does it offer opportunity beyond improving our defensive capabilities?

Sharing threat intelligence refers to three cases: 1) from the government to the private sector; 2) within the private sector; and 3) from the private sector to the government. All three face challenges.

In the government-to-private scenario, I encourage officials to grant clearances to private security teams not working on government contracts. The government should also augment its narrative style intelligence reports with digital appendices that list threat data in machine-readable form, similar to that offered by the OpenIOC format (www.openioc.org).

In the private-to-private case, I recommend creating information sharing groups. Adversaries often target whole sectors at once, so it helps to have peer companies compare notes.

The private-to-government case is the most contentious, for two reasons.

First, companies are reluctant to publicize security breaches, beyond what is necessary to comply with laws and standards. The private sector fears penalties if they disclose incidents to the government. Companies should not be held liable for voluntarily reporting incidents. Accordingly, the White House proposal prohibits the use of so-called “cyberthreat indicators” in any regulatory enforcement action.

Second, some privacy advocates believe that liability protection will let companies submit customer personal information to the government. This position does not reflect the reality of threat intelligence as defined earlier. Proper threat intelligence contains tactics, tools, and procedures used by intruders to abuse software and networks. It does not contain personal data from or about customers, if properly formatted.

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?

I recommend discussing these issues with companies who write breach insurance policies.

b. How about the social, cultural or other less tangible benefits?

While it may not be possible to quantitatively measure the benefits, it is qualitatively possible. Following recent intrusions, for example, corporate executives have lost their jobs.

c. Is there value in this?

No comment.

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?

It depends on the definition of "resilience." I fear too many advocates define resilience as "continuing to work despite being compromised." If that is the definition, we already operate "resilient" systems, at least when intruders choose only to steal information, and not modify or destroy it.

Organizations should always seek to prevent as many intrusions as possible, but they should not limit their security program, or defensive mindset, to prevention.

b. Why is the concept of resilience important to effective cybersecurity?

I prefer to define resilience in terms of process and operations. For example, an organization operates a resilient security program when it can detect and remove intruders before they accomplish their mission.

In some cases, resilience means using backup systems that do not rely on the Internet. For example, a soldier in the field should know how to use a map and compass if she loses Global Positioning Satellite contact. A company should have a means to communicate with employees that does not require email and Internet Protocol-based phones.

c. How does resilience support a risk-based approach to cybersecurity?

It depends on the definition of a "risk-based approach." I fear too many advocates define the phrase as "decide what we think is a problem, and try to prevent it." That is a failing strategy. I recommend security leaders start by addressing the problems they are already facing. They should prioritize defenses based on what is happening, not what they fear might be happening. In too many organizations, "risk" is an outdate concept. Because of adversary actions, "risk" has evolved from a "possibility" to a certainty, but executives continue to act in terms of possibility.

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?

Companies are adopting frameworks in order to be compliant with regulations and to withstand third party scrutiny. Most companies talk about applying "risk-based approaches," and they use the flawed definition I described earlier.

ii. Does this vary by industry or size of company?

I have no data on this topic.

1. If so, what are the driving factors?

No comment.

8. In Dr. Lin's written testimony he stated that "complexity is the enemy of cybersecurity."

a. Do you agree with this assessment?

Yes. "Cyber security" is a "wicked problem." (Please see my later answers for an explanation of this term.)

b. Is it possible to reduce this complexity?

i. If yes, what are the consequences?

I can offer one example from the industrial control system world. Complexity can be reduced by replacing, where possible, general purpose hardware and flexibly programmed operating systems and applications with purpose-built hardware and deterministic, limited programs. For example, there are few, if any, technically sound reasons to introduce general purpose hardware and flexibly programmed operating systems and applications into certain industrial control systems. Customers buy these systems because they are cheaper. Unfortunately, they expose a greater surface area due to their complexity, and import vulnerabilities that were previously not present.

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?

Moxie Marlinspike (www.thoughtcrime.org/) is the authority on the problems with digital certificates. I recommend asking him to obtain definitive answers.

i. How significant are these weaknesses?

No comment.

ii. Can these weaknesses be eliminated or adequately mitigated?

No comment.

b. Are Certificate Authorities subject to any form of oversight?

i. If so, by whom and how does this function?

No comment.

ii. If not, would enhanced oversight help address the weaknesses examined in Question 1? Why or why not?

No comment.

c. Are there alternatives to the digital certificate model?

i. If so, what are they?

No comment.

ii. If not, how can the current digital certificate ecosystem be improved?

No comment.

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?

I strongly recommend reading "Attributing Cyber Attacks" (bit.ly/attributing-cyber-attacks) by Dr Thomas Rid and Ben Buchanan for the definitive scholarly article on attribution. In brief, from their paper:

"[A]ttribution is what states make of it. Matching an offender to an offence is an exercise in minimising uncertainty on several levels. On a technical level, attribution is an art as much as a science. There is no one recipe for correct attribution, no one methodology or flow-chart or check-list. Finding the right clues requires a disciplined focus on a set of detailed questions — but also the intuition of technically experienced operators. It requires coup d'œil, to use a well-established military term of art.

On an operational level, attribution is a nuanced process, not a simple problem. That process of attribution is not binary, but measured in uneven degrees, it is not black-and-white, yes-or-no, but appears in shades. As a result, it is also a team sport — successful attribution requires more skills and resources than any single mind can offer. Optimising outcomes requires careful management and organisational process.

On a strategic level, attribution is a function of what is at stake politically. The political stakes are determined by a range of factors, most importantly by the incurred damage. That damage can be financial, physical, or reputational. Viewed from the top, attribution is part resourcing and guiding the internal process; part participating in final assessments and decisions; and part communicating the outcome to third parties and the public."

b. How does attribution of the threat help a company or organization recover from a breach?

I will explain how attribution can assist responsible actors, from defenders through policymakers, using the diagram at left.

Starting from the bottom, at the Tools level, attribution matters because identifying an adversary may tell defenders what software they can expect to encounter during an intrusion or campaign. It's helpful to know if the adversary uses simple tools that traditional defenses can counter, or if they can write custom code and exploits to evade most any programmatic countermeasures.

Vendors and software engineers tend to focus on this level because they may need to code different defenses based on attacker tools.

The benefits of attribution are similar at the Tactics level. Tactics describes how an adversary acts within an engagement or "battle." It describes how the foe might use tools or techniques to accomplish a goal within an individual encounter.

For example, some intruders may abandon a system as soon as they detect the presence of an administrator or the pushback of a security team. Others might react differently by proliferating elsewhere, or fighting for control of a compromised asset.

Security and incident response teams tend to focus on this level because they have direct contact with the adversary on a daily basis. They must make defensive choices and prioritize security personnel attention in order to win engagements.

The level of Operations or Campaigns describes activities over long periods of time, from days to months, and perhaps years, over a wider theater of operations, from a department or network segment to an entire organization's environment.

Defenders who can perform attribution will better know their foe's longer-term patterns of behavior. Does the adversary prefer to conduct operations around holidays, or certain hours of the day or days of the week? Do they pause between tactical engagements, and for how long? Do they vary intrusion methods? Attribution helps defenders answer these and related questions, perhaps avoiding intrusion fatigue.

CISOs should focus on this level, and some advanced IR teams incorporate this tier into their work. This is also the level where outside law enforcement and intelligence teams organize their thinking, using terms like "intrusion sets." All of these groups are trying to cope with long-term engagement with the adversary, and must balance hiring, organization, training, and other factors over budget and business cycles.

At the level of Strategy, attribution matters to an organization's management and leadership, as well as policymakers. These individuals must decide if they should adjust how they conduct business, based on who is attacking and damaging them. Although they might direct technical responses, they are more likely to utilize other business methods to deal with problems. For example, strategic decisions could involve legal maneuvering, acquiring or invoking insurance, starting or stopping business lines, public relations, hiring and firing, partnerships and alliances, lobbying, and other moves.

Strategy is different from planning, because strategy is a dynamic discipline derived from recognizing the interplay with intelligent, adaptive foes. One cannot think strategically without recognizing and understanding the adversary.

Finally, the level of Policy, or "program goals" in the diagram, is the supreme goal of government officials and top organizational management, such as CEOs and their corporate boards. These individuals generally do not fixate on technical solutions. Policymakers can apply many government tools to problems, such as law enforcement, legislation, diplomacy, sanctions, and so forth. All of these require attribution. Policymakers may choose to fund programs to reduce vulnerabilities, which in some sense is an "attribution free" approach. However, addressing the threat in a comprehensive manner demands knowing the threat. Attribution is key to any policy decision where one expects other parties to act or react to one's own moves.

c. What makes attribution so difficult?

It is difficult because the amount of time and effort required to perform attribution is disproportionate to the amount of time and effort required to frustrate attribution.

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?

I defer to the Commission on the Theft of American Intellectual Property (The IP Commission, www.ipcommission.org).

b. How does the economic impact of Intellectual Property theft compare to something like the theft of consumer data?

I defer to the Commission on the Theft of American Intellectual Property (The IP Commission, www.ipcommission.org).

c. Is it possible to quantify the economic effect of stolen Intellectual Property?

I defer to the Commission on the Theft of American Intellectual Property (The IP Commission, www.ipcommission.org).

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.

I defer to the Commission on the Theft of American Intellectual Property (The IP Commission, www.ipcommission.org).

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?

The majority of organizations do not conduct a security program with a goal of minimizing loss due to intrusion, with a strategy of rapid detection, response, and containment. Because they are not looking for intruders already present in the network, they end up learning about breaches when third parties notify them.

i. Are certain sectors better at identifying vulnerabilities than others?

In general, defense and finance companies operate the most mature private sector incident detection and response programs.

ii. Is there variation based on the size of the company? If so, why?

The larger the company, the more likely they will have a mature program. It is expensive to sustain security programs capable of frustrating a range of threat actors. Only the largest companies can afford to distribute the cost of the team across a large information technology or security budget.

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?

It can be exceptionally difficult to dislodge an intruder, or groups of intruders, once they have been resident for weeks, months, or years. Depending on the nature of the threat and their dedication to retaining access, it may take weeks to remove them. However, if the threat actors receive tasking to return to the victim network, the organization will likely confront a long-term campaign.

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?

The only strategy I have seen work during the 18 years of my career has relied on detecting and responding to intrusions before the adversary accomplishes his mission.

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?

I believe, and many others concur, that cyber security is a "wicked problem" (en.wikipedia.org/wiki/Wicked_problem). Simson Garfinkel described it in these terms:

"There is no clear definition of the wicked problem. (You don't understand the problem until you have a solution.)

There is no "stopping rule." (The problem can never be solved.)

Solutions are not right or wrong. (Benefits to one player hurt another.)

Solutions are "one-shot." (No learning by trial and error. No two systems are the same. The game keeps changing.)

Every wicked problem is a symptom of another problem."

This description is derived from Garfinkel's 2012 presentation (www.afcea.org/events/tnlf/east12/documents/2012-04-25_Cybersecurity.pdf), which summarized an October 2011 Chatham House article by Dave Clemente, "Cyber Security as a Wicked Problem" (www.chathamhouse.org/publications/twt/archive/view/178579).

b. How can executives and security professionals reconcile their different priorities and views?

In my five levels of strategic thought -- goal, strategy, operations/campaigns, tactics and tools -- I see chief security officers (CSOs) as a bridge, usually working at the operational level, between the CXOs and board members and the security teams and vendors. I prefer to see CSOs speak policy and strategy to the CXOs and board members, and tactics and tools to the security teams and vendors, while running operations from the CSO office. This is a shift in mindset and approach, but I am seeing signs that it is welcome and effective.

<u>The Honorable Markwayne Mullin</u>

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?**

Depending on the nature of the company, a SMB might face all of the challenges of a large business, but lack the resources to meet those challenges. The SMB will likely lack the resources because it cannot scale its expenses across a larger revenue base.

2. **What advice would you give to an entrepreneur opening up, say, a retail shop or restaurant?**

1. Identify and minimize information assets. Do you really need that data? This question prompts the user to consider whether the data they collect, store or transmit is truly necessary for business operations. Sometimes, outside regulators seek to control data, as is the case with the Payment Card Industry Data Security Standard (PCI DSS). Even when not regulated, everyone, from corporate employees to home users, should think about the sorts of data they manipulate. The best way to keep sensitive data out of the hands of criminals might be to never let it exist in digital form.

2. Keep sensitive data off the network as much as possible. Everyone has sensitive data, but not all that data needs to be connected to a network. For example, a company processing tax returns could keep that information on systems not connected to the Internet. Alternatively, sensitive data might reside on external hard drives that are attached to a PC or laptop when needed, and detached when not needed. If a criminal can't reach sensitive data because it is off the network, he can't read, steal, or delete it.

3. Provision a separate PC for sensitive business functions, like banking. SMBs should identify one or more computers to be used only for sensitive functions, like electronic commerce. The PC used to transfer money from one account to another should only serve that function. Users should not check their email, browse random Web sites, connect USB thumb drives, or take any other actions on the "e-banking PC." Criminals want to steal the usernames and passwords associated with bank accounts, but their job is a lot harder if users never check email or Web sites on the computer they use for doing banking. If possible, only connect this PC to the network when doing electronic commerce.

4. Enable two-factor authentication (2FA) wherever possible. 2FA refers to practices that require users to log into accounts using something more than a username and password. Some readers may be familiar with tokens that flash a new six-digit code every minute or so. Free solutions, like Google Authenticator are another option. Some sites provide users with the option of adding a code sent via Short Message Service (SMS) texts, sent to mobile phones. No solution is hack-proof, but whatever option a service provides above and beyond simple usernames and passwords, users should test and adopt.

5. Leverage trustworthy cloud solutions. Most computer users aren't interested in being information technology experts. Many SMBs can't afford in-house IT departments, or don't consider IT as a core

business function. In these cases, companies should evaluate cloud providers. Theoretically, a cloud provider can hire the necessary expertise to keep data secure, and scale that expertise across the customer base. The trick is identifying trustworthy cloud providers. Ask or research the following questions: 1) what government agencies subscribe to the cloud solution, and 2) what documentation can the cloud provider provide concerning its security practices? Cloud providers who fail these two tests may not yet be ready for conscientious SMB customers.

6. Join Infragard. Infragard is a non-profit organization run by the US Federal Bureau of Investigation. The FBI created Infragard in 1996 to assist the private sector with cyber defense. Infragard maintains chapters in virtually every major city across the country. These chapters hold regular meetings with content designed to educate attendees on cyber threats and mitigations. Such events allow attendees to learn from each other, and also meet their local FBI agents. Organizations should become acquainted with their respective law enforcement agents prior to any serious security incident. The worst time to first meet an FBI agent is when you need that agent's help with a computer intrusion.

7. Treat cyber security as a business problem, not a technical problem. Business leaders have traditionally considered cyber security to be a problem for the IT staff. Executives thought that if they just bought the right software, they could "solve" the "hacker problem." However, the pervasiveness and consequences of digital breaches have encouraged those leaders to properly consider digital defense as a business problem. No one buys a software package to manage human resources, believing that the new application has "solved" hiring, retention, and other personnel challenges. No one subscribes to a cloud-based sales solution, thinking that they have "solved" their customer acquisition and satisfaction problems. In a similar way, executives will find security software to be necessary, but not sufficient, to address hacking woes. It is important for leaders to devise a security strategy appropriate for their business, then execute on that strategy on a daily basis.

3. How can businesses be sure that their vendors understand their specific cybersecurity issues and will develop a system that will provide protection?

Choose vendors with a reputation for caring about security. For example, is the vendor a member of the Forum of Incident Response and Security Teams (www.first.org/about/organization/teams)? Does the vendor operate a product security incident response team (PSIRT) or at least have a “/security page” on their Web site (e.g., www.fireeye.com/security), offering ways to contact the vendor about security issues? These are useful starting points.

4. Would you say that security breaches we see in small businesses are an IT problem or a business problem?

All security problems are first and foremost business problems.