STATEMENT OF DR. PHYLLIS SCHNECK, VICE PRESIDENT AND CHIEF TECHNOLOGY OFFICER, GLOBAL PUBLIC SECTOR

McAFEE, INC.

BEFORE:

UNITED STATES HOUSE OF REPRESENTATIVES

COMMITTEE ON SMALL BUSINESS

SUBCOMMITTEE ON HEALTH AND TECHNOLOGY

"PROTECTING SMALL BUSINESSES AGAINST COMPLEX AND EMERGING CYBER-THREATS"

MARCH 21, 2013

Good morning Chairman Collins, Ranking Member Hahn, and other members of the Subcommittee. I am Phyllis Schneck, Vice President and Chief Technology Officer, Global Public Sector for McAfee, Inc. We appreciate the Subcommittee's interest in cyber security as it affects small business, and I'm pleased to be addressing the Subcommittee once again.

My testimony will focus on the following areas:

- The threat landscape and its implications for small business
- Recommended best practices for small businesses to protect themselves
- What the private sector can do to help small business
- What government can do to help small business

First I would like to provide some background on my experience and on McAfee.

I have dedicated my entire professional career to the security and infrastructure protection community. My technical background is in high performance computing and cryptography. In addition to my role with McAfee, I serve as Chairman of the Board of Directors of the National Cyber Forensics and Training Alliance (NCFTA), a partnership between government, law enforcement, and the private sector for information analytics that has been used to prosecute over 400 cyber criminals worldwide. Earlier, I worked as Vice President of Threat Intelligence at McAfee and was responsible for the design and application of McAfee's™ Internet reputation intelligence. I am the Vice Chair of the Information Security and Privacy Advisory Board (ISPAB) and have also served as a commissioner and working group co-chair on the public-private partnership for the Center for Strategic and International Studies (CSIS) Commission to Advise the 44th President on Cyber Security.

Additionally, I served for eight years as chairman of the National Board of Directors of the FBI's InfraGard™ program and as founding president of InfraGard Atlanta, growing the InfraGard program from 2000 to over 33,000 members nationwide. Prior to joining McAfee, I was Vice President of Research Integration at Secure Computing. I hold a Ph.D. in Computer Science from Georgia Tech, where I pioneered the field of information security and security-based high-performance computing.

McAfee's Role in Cyber Security

McAfee, Inc. protects businesses, consumers and the public sector from cyber-attacks, viruses, and a wide range of online security threats. Headquartered in Santa Clara, California, and Plano, Texas, McAfee is the world's largest dedicated security technology company and is a proven force in combating the world's toughest security challenges. McAfee is a wholly owned subsidiary of Intel Corporation.

McAfee delivers proactive and proven solutions, services, and global threat intelligence that help secure systems and networks around the world, allowing users to safely connect to the Internet and browse and shop the web more securely. Fueled by an award-winning research team, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security.

To help organizations take full advantage of their security infrastructure, McAfee launched the Security Innovation Alliance, which allows organizations to benefit from the most innovative security technologies from thousands of developers, who can now snap into our extensible management platform. Today, more than 160 technology partners—large and small businesses all committed to continuous innovation in security—have joined the alliance, with more to be announced soon.

The Threat Landscape and its Implications for Small Business

Since I last testified before the Subcommittee the cyber threat has only intensified. I want to focus on two areas where information technology is helping small business be more efficient but where caution is also necessary. These are the areas of mobile communications and the cloud.

Mobile Threats

It should come as no surprise that cyber criminals follow the latest technology trends because that's where the targets are the most promising. The growth in mobile communications is staggering, and the U.S. leads the world in mobility. Globally, mobile data traffic grew 70% in 2012, and by the end of this year the number of mobile-connected devices is expected to exceed the world's population, according to the Cisco Visual Networking Index.

Small businesses, as others, are relying more on mobile devices not only for communication but also for business processes, and there's every reason to believe this trend will continue. When I last appeared before the subcommittee, in December of 2011, mobile threats had begun to appear on the radar screen. Now they are front and center.

According to McAfee Labs, the growth in mobile malware almost doubled in each of the last two quarters of 2012. At the beginning of this year, the total number of samples in our mobile malware "zoo" reached almost 37,000 – with 95% of those having arrived in 2012. To put this in perspective, in all of 2011 we gathered only 792 samples. The Android platform is the lead target of mobile malware, with 97% of last quarter's (4th Q 2012) being directed there.

One of the most volatile and worrisome areas of threats today is some new functionality in malware. A scam known as Android/MarketPay is a Trojan horse program that buys apps from an app store without a user's permission. We're likely to see crooks take this malware's app-buying payload and add it to a mobile worm. With such a mobile worm, attackers will no longer need victims to install a piece of malware. And if user interaction isn't needed, there will be nothing to prevent a mobile worm from going on a shopping spree.

Another developing area for mobile threats is in phones or other devices with near-field communications (NFC), which are becoming more common. As users are able to make "tap and pay" purchases in more locations, they'll carry their digital wallets everywhere. That flexibility will, unfortunately, also be a boon to thieves. Attackers will create mobile worms with NFC capabilities to propagate (via the "bump and infect" method) and to steal money. Malware writers will thrive in areas with dense populations (airports, malls, theme parks, etc.). An NFC-enabled worm could run rampant through a large crowd, infecting victims and potentially stealing from their wallet accounts.

Attackers love it when users install malicious apps that let the bad guys gain complete control of victims' phones; it's no wonder that mobile backdoors remain popular with attackers. Android/FakeLookout.A is a mobile backdoor that pretends to be an update to antivirus software. In reality it hands control of a phone to an attacker. It's designed to steal and upload text messages and other files to the attacker's server. Another one of these is Android/GinMaster.A, a mobile backdoor that uses a root exploit to gain further access to a user's phone. It posts a number of pieces of identifying information to the attacker's server and accepts commands from the attacker.

As you can see, innovation is thriving in mobile malware development and needs to thrive even more strongly in our small businesses. Faced with the challenges of "Bring your own device," sometimes known as "BYOD," many small businesses will struggle with maintaining security and management control over a wide spectrum of devices that consumers increasingly want to use for their work.

Migration to the Cloud

Another IT trend that serves small business particularly well is migration to the cloud. Small businesses, in particular, can find real efficiencies in outsourcing their IT and communications systems to the cloud. They can reduce costs, improve offerings, eliminate complexity and have less need for onsite IT staff. These are great objectives – as long as security is not sacrificed.

I won't go into detail here, but not surprisingly, we are seeing bad actors target cloud providers. Most cloud providers do not offer a forensics capability as part of their base offering. This means that if a company's data stored in the cloud is breached, it will cost the company extra to provide forensic data to either law enforcement or a security firm so that the breach can be traced and remediated. Small business owners should address this need up front with cloud providers so they are not surprised if a breach occurs.

This is especially important at this time, when companies of all sizes are being encouraged to report breaches or suspected events to 1) protect victims, and 2) use the behavior intelligence and forensics around the event to help protect others. There has never been a more important time for a security provider – cloud or otherwise – to enable easy, sound, connected intelligence and behavioral analysis at a price point that is a worthy investment. This helps small businesses individually and collectively.

What Can Small Businesses Do to Protect Themselves?

Mobility and the cloud are here to stay, and it makes sense for small business to embrace these trends. They shouldn't do so without protections, however; this, too, makes good business sense.

Here are some recommendations for small businesses to protect themselves:

In General

At McAfee, we believe in "Security Connected," from the chip to the cloud. As a part of the Intel Corporation, we explore behaviors from hardware to software and specialize in recognizing malicious intent before it can cause irrevocable harm. The keys are ensuring that cyber security is a boardroom issue of risk – even in the smallest of companies – and enabling companies to implement a connected, holistic approach that considers their networks an ecosystem of traditional, mobile and cloud devices and services.

This ecosystem concept is well described in the white paper from the National Protection and Programs Directorate within the Department of Homeland Security. Done correctly, networks can detect behaviors over time and begin to recognize, almost biologically, threats before those threats can overtake network functionality. Maturity models have shown that for any size organization, a wise design up-front leads to increasing security and decreasing cost over time. A connected, behavior-based approach enables network components such as phones, laptops and servers to communicate observed behavior amongst each other. Security can thus be managed in real-time based on policy that adapts to current threats and provides resilience: the ability to run while under attack.

These intelligent systems are the result of innovation, and we need to help small business make wise – not expensive – choices to create a connected security foundation. As I mentioned in my prior testimony to this Committee, small business comprises over 95% of the U.S. business fabric. Small businesses have personal information stored, operational requirements and valuable intellectual property, and they need strong cyber security as much as large enterprises. Budget constraints in smaller businesses accentuate the need for a connected, ecosystem-based strategy in planning in security investment.

For Mobility

Like laptop and desktop PCs, today's mobile devices are complex platforms with multiple modes of communication, significant processing power and large storage capabilities. This by itself would make today's mobile devices subject to the same risks as business laptops; however, mobile devices have certain characteristics that make them even more vulnerable than PCs. Thus we recommend contracting with reputable service providers who take security seriously.

There are also precautions that small business owners can take to make sure their employees' devices are secure. Here's a partial list:

- Track and adaptively manage the devices that access your corporate network
- Educate employees on their role in protecting the organization, its data, and brand against theft, loss or malicious use
- Use passwords
- Encrypt on-device data and email, and ensure mobile device data and email remote "wipe" capabilities
- Have policy controls over memory card usage and encrypt that data.

- Implement Bluetooth controls, such as installing firewalls and pairing with only known, trusted devices
- Protect against Trojans with blacklisting and whitelisting applications
- Have policy controls over web browser use and website access
- Install a firewall on the mobile device to restrict inbound connections and prevent use of the mobile device as a bridge

The best security providers offer both targeted and comprehensive protections for the leading mobile device platforms. As mentioned earlier, Android devices are attacked much more than others. As an example of emerging mobile security software, McAfee last week announced an embedded control solution that is the industry's first to reside in the Android kernel. The control is embedded in the operating system rather than sitting at the user level, which is what makes it unique. As businesses depend more on mobile devices, security vendors will continue to innovate in the mobile space.

For the Cloud

Nine out of 10 businesses cite security as the top obstacle to cloud adoption, according to International Data Corporation (IDC). Yet small businesses can take advantage of cloud computing safely with some precautions upfront. These include making sure they are outsourcing to a cloud provider that can ensure robust security. We recommend that cloud providers contract with a third-party security vendor, offering the most up-do-date protections for the most recent – and emerging – threats.

But there are steps small business owners can take before even getting data to the cloud provider. You can think of these practices as building a secure bridge to the cloud. Here are a few recommendations:

Discover and classify data in the organization before it even leaves to go to the cloud

Before even beginning to consider what type of data should or should not be moved to the cloud, a business must first understand what data it has, where it resides – and more importantly – the value or sensitivity of the data. Only when there is a complete inventory of the data can an organization begin to classify the data to build the appropriate policies to protect it and then enforce policies while data travels both within and outside the organization.

These policies can be kept simple, but they should be in place to enable cyber security to be managed as a risk mitigation tool and business enabler for small business.

Secure the primary channels of traffic that move data to and from the cloud

These channels include email traffic, web traffic (including mobile), and authentication traffic (making sure users are who they say they are, and that they are authorized to access the data).

McAfee and other comprehensive security vendors offer cloud security platforms that are very effective at managing these tasks.

It's also possible for small businesses to get their security virtually – whether or not they are outsourcing their IT. Again, we and other security vendors offer security via a third party, or "the cloud," and this can be a cost-effective way for small businesses to get optimum security without having to manage everything themselves.

What the Private Sector Can Do to Help Small Businesses

In addition to providing security for mobility and the cloud, the security and IT industries need to keep their focus on innovation in order to help small business and other organizations. At McAfee we feel strongly that the path forward is for security to be integrated into products at the beginning, for disparate islands of security to be connected, and for security vendors to offer real-time situational awareness of threats.

Security features are not as effective when they are glued onto systems as an afterthought. Rather, cyber security must be integrated into equipment, systems and networks at the very start of the design process. Security must be embedded in a product or network element so that it becomes an integral part of the product's or element's functioning. Products must also be built to communicate with each other -- exchanging information in real-time about what each product is seeing on the network to create the behavioural knowledge throughout the network ecosystem. This design-level approach is not only more effective; it is less cumbersome and less expensive than trying to lock down systems that are inherently insecure. This approach also provides tremendous cost savings for small businesses, because the products and services that enable the business have more native security and lead to a safer infrastructure with less need for additional expenditures.

McAfee and Intel create and support these Security by Design and Security Connected approaches. Today's attackers now can be stopped below the machine's applications layer – and even below the operating system. McAfee and Intel are working together to change the security paradigm to dynamically and adaptively protect systems against attacks at the core of computing, and to provide proactive defenses in real-time, making networks intelligent enough to prevent malicious instructions from reaching their targets – instead of requiring those targets to be vaccinated using signatures.

We also believe that as a security industry we must unify, simplify, and strengthen the way we provide security. We need to provide a framework for integrating potentially disparate technologies – building bridges between security islands to close coverage and technology gaps. This is the rationale for McAfee's Security Connected platform. With cyber security integration, security companies and their small business customers will be able to quickly and comprehensively detect and deter threats.

And having real-time visibility into emerging threats and a comprehensive view across the threat landscape is a powerful means of defeating cyber incursions. One robust technology that enables this real-time global visibility is called Global Threat Intelligence. With Global Threat Intelligence, millions of sensors scan the Internet across the globe and feed back real-time data on threats. This data is instantaneously correlated and fed back into security products, delivering real-time protection to customers, as we identify and block malicious files, Internet protocols and web addresses. With even more threat data from more security organizations fed into this network, customers would get even more comprehensive visibility into the quickly changing patterns of infestations and could take immediate steps to counter them.

What Government Can Do to Help Small Business: Enable Information Sharing

It's hard to overstate the importance of being able to share threat information between the private sector and the government. There are several initiatives that can facilitate this process, and I'll discuss two of them: an information sharing bill and an information sharing mechanism available to large business known as ISACs, or Information Sharing and Analysis Centers.

An Information Sharing Bill - Rogers/Ruppersberger

During the last Congress and again this year, House Intelligence Chairman Mike Rogers (R-Michigan) and Ranking Member Dutch Ruppersberger (D-Maryland) introduced the *Cyber Intelligence Sharing and Protection Act*, also known as CISPA. The bill would facilitate the sharing of cyber intelligence between the government and the private sector. Significantly, the bill would offer liability protections for private entities sharing cyber threat information in good faith. Ensuring that sufficient privacy protections are baked into this bill will help cement the broad consensus necessary to make this proposal a legal reality.

An Information Sharing Construct – ISACs

While we definitely need legislation for robust information sharing, the government has endorsed and the private sector has put in place several Information Sharing and Analysis Centers, or ISACS. These ISACS, which are organized by sector, provide a specific mechanism for sharing cyber threat data.

Small businesses have neither the budgets nor the cyber experts to participate in a traditional ISAC. Indeed this Committee might consider the merits of conducting a study or holding a hearing on this matter to develop policy proposals to enable deeper small business community participation in the ISAC community. As we know, small businesses represent 99.7 % of all employer firms and employ about half of all private sector employees, according to the Small Business Administration. We need to find a way to include small business in our nation's security paradigm – and that includes information sharing.

The National Cyber Forensics and Training Alliance (NCFTA) is one example of successful information sharing. Small businesses need the intelligence that such collaborations provide, and perhaps the small business community could leverage the information sharing agreements in the NCFTA so that collectively they could better protect the U.S. small business fabric, and thus our economy.

Thank you for the opportunity to address the subcommittee. I will be happy to answer any questions.