STATEMENT FOR THE RECORD OF

THOMAS GANN, CHIEF PUBLIC POLICY OFFICER, MCAFEE, LLC.

BEFORE THE U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON SMALL BUSINESS

ON "FEDERAL GOVERNMENT AND SMALL BUSINESSES: PROMOTING GREATER INFORMATION SHARING FOR STRONGER CYBERSECURITY"

November 15, 2017, 11:00 AM | RAYBURN HOUSE OFFICE BUILDING ROOM 2360

Good morning, Chairman Chabot, Ranking Member Valazquez, and distinguished members of the committee. Thank you for the opportunity to testify today. I am Tom Gann, Chief Public Policy Officer for McAfee, LLC. I have over 20 years of experience in the IT industry, having run government relations and public sector alliances functions for Digimarc, Siebel Systems and Sun Microsystems. During the last decade, I have focused on cybersecurity and identity management issues. I hold degrees in business and political science from the London Business School and Stanford University.

I am pleased to address the committee on this important matter. My testimony will address the cybersecurity challenges small businesses face, why sharing technical information is particularly difficult for small businesses, the types of information sharing that could be most useful to them, and general recommendations that can enhance the cybersecurity capabilities of small businesses.

MCAFEE'S COMMITMENT TO CYBERSECURITY

McAfee is one of the world's leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions that make the world a safer place. By building solutions that work with other industry products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, we secure their digital lifestyle at home and while on the go. By working with other security players, we are leading the effort to unite against state-sponsored actors, cybercriminals, hacktivists and other disruptors for the benefit of all. McAfee is focused on accelerating ubiquitous protection against security risks for people, businesses and governments worldwide.

Before beginning my comments, I want to express how extremely pleased McAfee is in seeing the focus on improving the cyber threat landscape for small businesses. Through the past several years, a great deal of time and effort has been focused on larger organizations with resources to invest, but attention on risks to small business – the backbone of our nation's economy – is long overdue. For too long, small businesses have been a target of malicious actors with little or no way to protect themselves due to education and resource constraints. Thank you for investigating ways to better protect this vital segment of our digital economy.

CYBERSECURITY RISKS FACED BY SMALL BUSINESS

There's no doubt that small businesses face many of the same cybersecurity risks as large ones. Some cyber-attack methods, such as ransomware and those that begin with spear-phishing, are particularly well-suited to small businesses, who might be an easy target because of their lack of cybersecurity resources. Small businesses store personal information, implement operational requirements and own valuable intellectual property just as large enterprises do, so they too need strong cybersecurity protections. In fact, more than 50 percent of cyber-attacks are launched on firms having fewer than 50 employees, according to cyber expert Steve Morgan. A 2016 report from Keeper and the Ponemon Institute found that only 14 percent of small and medium-sized businesses say they have the ability to effectively mitigate risks and vulnerabilities. Further, 50 percent say they had been breached in the past 12 months. This is not at all surprising, given that many small businesses might not even have IT staff, let alone cybersecurity staff.

Not addressing these risks have real consequences for the businesses themselves, larger businesses and local economies. For example, an August 2017 analysis by Tech Republic found that a single cybersecurity attack could cost a small business $256,000. And we've seen at least one instance of a small business breach affecting a larger one in the Target hack.

An October study by the Better Business Bureau, The State of Small Business Cybersecurity in North America, found that half of small businesses could remain profitable for only one month if they lost essential data. Further, while small businesses may be adopting solutions like antivirus software, one of the most cost-effective tools, employee education, is used by fewer than half the companies surveyed. The report also found that while awareness of cybersecurity risk among small business owners is growing, they are not at all certain what to do about it.

According to an August 2017 survey from BizBuySell, the Internet's largest business-for-sale marketplace, 90 percent of small businesses believe it's at least important to protect themselves from a cyber-attack. Yet moving from cyber protection being important to it being essential, practical and affordable is a big step. Investing in more than just very basic cybersecurity tools requires time, money and other resources – like an IT staff – that small businesses often don't have. We have to acknowledge the fact that for most small businesses, cybersecurity is an expense they don't want to incur when they're trying to simply make payroll and remain profitable.

"Profitability is the ultimate test of risk," one of the Better Business Bureau report's authors said, adding that small business owners have to do a cost-benefit analysis of cybersecurity. "It doesn't do any good for a small business to adopt a $10,000 solution if the potential risk reduction is worth $5,000," he added.

THE INFORMATION SHARING CHALLENGE FOR SMALL BUSINESS

So, what's the solution? Should small businesses participate in the Department of Homeland Security's (DHS) cyber threat information sharing program mandated by the Cybersecurity Information Sharing Act (CISA)? This is a question worth exploring. In talking with our customers, it is clear that many small businesses are unaware of CISA, often don't understand how the law can help them, and are confused by the many information sharing initiatives out there.

However, I also believe we should consider how information sharing efforts, such as those mandated by CISA, can directly benefit small businesses.

The DHS initiative known as Automated Indicator Sharing (AIS) is open to small businesses, but few have the resources or an educated IT staff to make direct use of or benefit from it. The kind of information shared via AIS is comprised of indicators of compromise (IOCs). While the overall program has been a strong step in the right direction, it still provides far too little real value. IOCs are just the breadcrumbs that network security staff look for to uncover clues as to what may be occurring inside their organizations. Typical IOCs include registry keys, MD5 hashes of potential malware, IP addresses, virus signatures, unusual DNS requests, and URLs. While these can be useful, they are not enough to provide the defensive information needed to protect an organization.

The information shared must be both useful and actionable to the receiving parties and, in the case of AIS, it also must be automated. As many small businesses outsource functions like their point of sale systems, or even their entire IT needs, they may not have access to the information contained there, let alone be able to ensure it is useful and actionable. Even if they had their own IT support infrastructure, small businesses would have to acquire and set up systems and software to collect, share and use the information. The reality is any information sharing capabilities require time, money and resources that many small businesses just do not have.

Additionally, it should be understood that we are not sharing information just for sharing's sake. There needs to be a valuable purpose for the sharing if a business is going to spend the money needed to set it up and maintain it going forward as a core business practice. If the information being shared is not useful, actionable and automated, then the entity sharing it doesn't bring much value to the table – nor would the small business get value from it. Today, the type of simple information via IOCs exchanged by AIS is hard for small businesses to get value out of.

A DIFFERENT KIND OF INFORMATION SHARING

This doesn't mean that small businesses don't need or can't benefit from cyber threat intelligence; they certainly can. But perhaps we should focus our discussion more on sharing a different kind of information – information that is more informative and educational right away.

The Better Business Bureau study found that when asked to judge 10 statements on cybersecurity as either true or false, the average score was below 60 percent, meaning that there are still opportunities to better educate small businesses and dispel some myths. And regarding what to do first in a data breach, only about 20 percent of respondents answered correctly. Granted, the laws vary from state to state and can be complicated, but this just points out the need for more education on the benefits of having a plan before a breach occurs.

Education and awareness efforts are essential. The Federal Trade Commission (FTC) just last month launched a new site for Protecting Small Business that offers advice on cybersecurity basics, protecting personal information and what to do in the event of a data breach. Likewise, the Small Business Administration (SBA) also provides resources on its website. We need even more initiatives like these that make it as easy as possible for small businesses to learn more about how to protect themselves.

The federal government can also help raise awareness among vendors and solutions providers of the role small businesses play in protecting the nation's critical infrastructure. Many important government contractors are small businesses and, as we learned in the retail attacks of 2014, small businesses are attractive attack conduits for breaching larger business or government targets rich in high-value data or other assets.

DEDICATED INFORMATION SHARING ORGANIZATION FOR SMALL BUSINESS

The federal government should also help develop and fund the standup of a non-profit Information Sharing and Analysis Organization (ISAO) focused on U.S. small businesses. Small businesses do not have the resources to address the problem of gathering and analyzing cyber threat intelligence on an ongoing basis, but a highly targeted ISAO with initial support from the federal government could help. A small business-focused ISAO could use the economies of scale to be able to supply appropriate information to those business that lack the resources but still need current cyber threat intelligence. Such an ISAO could provide education services to its members as a part of their services, such as basic cyber hygiene and more advanced topics like incorporating the NIST Cybersecurity Framework into their security program. Cyber education is critical to the success of small business being able to understand the problems in order to begin addressing them.

The ISAO could provide its members with best practices, lessons learned, templates and processes for addressing incidents, the ability to get help understanding the problems and act as a hub in case a breach occurs. In the event of an incident, small businesses need to know where to go and what to do. The ISAO could also act as the first point of contact in determining whether or not to reach out to law enforcement and to assist the business in addressing the incident. This would also allow the ISAO to communicate the situation to its other members so that they too could be informed.

An information sharing organization such as this would be also able to spread costs among its members. We encourage the government to consider providing the initial startup funding for a national small business ISAO.

ADDITIONAL RECOMMENDATIONS FOR PROTECTING SMALL BUSINESS

<u>Move to the Cloud</u>

Advances in technology can also serve to protect technology. For example, outsourcing infrastructure to a cloud provider is becoming more common. This practice could have real advantages for a small business, as the cloud provider would be responsible for security. Both infrastructure as a service and security as a service warrant attention from small business, as both can be economical ways to provide efficiencies and security without the business owner having to think about it. The growth of cloud applications has made these "as-a-service" technologies real possibilities. Leveraging them could enable a small business to focus on becoming a medium-sized business, for example, rather than having to be an IT and security expert.

At the same time, cloud providers have the opportunity to gain the insight from the threats they see on the endpoints of their small business customers, benefiting from the ever-growing network effects of more and more threat data, which in turn can enhance their ability to improve their

customers' security. Cloud providers should also be able to leverage their economies of scale to share threat information with their partners in the private and public sectors.

While the move to the cloud has real benefits, small business owners cannot contract out all of their cybersecurity obligations, particularly in the area of strong blocking and tackling – making sure that passwords are updated on a regular basis and backing up information on a regular basis.

Improve DHS's Automated Indicator Sharing (AIS) Program

While the AIS program is still in the startup phase and needs to broaden the type of information it receives and shares, we should not give up on its potential. Policymakers need to enable the administration to move beyond simple indicators supplied via AIS and provide a means to enrich the effectiveness of shared information. The administration should increase its efforts with the private sector to further evolve the way cyber threat information is represented, enriched and distributed in a timely fashion. Doing so will help create a high-functioning ecosystem of information sharing that will help all organizations, both large and small, to compete with global networks of sophisticated hackers.

Encourage Cyber Insurance for Small Businesses

Small businesses would also benefit from cyber insurance, which is specifically designed to protect an organization from risk. This is still a small but growing part of the insurance market. It deserves more attention, as does the idea of having the government act as a reinsurer for the cybersecurity insurance market during its early stages. Alternatively, the government could establish a program similar to the National Flood Insurance Program to help support the private market in the event of catastrophic, widespread attacks.

Invest in Fighting Cyber Crime

The government should also devote additional resources to fighting cybercrime. Too often, it is small businesses in sectors like health care and finance that are being hacked by cyber criminals. These criminals are perfecting the art of ransomware, and small businesses are all too often being forced to pay to protect their data. Law enforcement at all levels – federal, state and local – need to have the resources to identify and take down hackers who have been terrorizing the small business community.

CONCLUSION

It's important to recognize that technical information sharing is only one piece of the puzzle. Small businesses need, first of all, to get the basics of cybersecurity right. Information sharing efforts designed to educate and raise awareness are more important – at least at this point – than those intended to share automated, actionable indicators of threats. Small businesses can benefit greatly from moving their infrastructure and security to the cloud and the economies of scale of ISAOs dedicated to their unique requirements. Cyber insurance also holds promise, as does doubling down on investments to fight cybercrime. We also need to support efforts to boost the effectiveness of the Automated Indicator Sharing program to ensure that everyone wins over time.

Thank you for giving McAfee the opportunity to testify on this important topic. I'm be happy to answer any questions.