e-Management
Your Success. We Deliver IT.

Prepared Testimony and
Statement for the Record of

Ola Sage
Founder and CEO, e-Management
Co-Founder and CEO, CyberRx

Hearing on

"Federal Government and Small Businesses: Promoting Greater Information Sharing for Stronger Cybersecurity"

Before the

Committee on Small Business, U.S. House of Representatives

November 15, 2017

2360 Rayburn House Office Building

Federal Government and Small Business: Promoting Greater Information Sharing for Stronger Cybersecurity

Opening Remarks

Good morning Chairman Chabot, Ranking Member Velazquez, and distinguished members of the Committee. Thank you for the opportunity to testify today.

My name is Ola Sage and I am the founder and chief executive officer (CEO) of two small businesses in technology. My first company, e-Management, is an Information Technology (IT) professional services firm that provides a range of cybersecurity services and enterprise IT solutions for federal government clients. Headquartered in Silver Spring, MD, we employ approximately 70 professionals who actively serve our government clients. In our 18th year in businesses, I am proud of the many contributions our small business has been recognized for including a Cybersecurity Achievement Award from the Department of Energy (DOE) for Innovative Technical Achievement highlighting our technical excellence and best practices in cybersecurity detection and risk management. Last year, the U.S. Chamber of Commerce selected e-Management as one of the top 100 small businesses in America and earlier this year, we were delighted to be recognized as a *Best Places to Work* honoree.

Two years ago, I set out with bold plan to create a cybersecurity company, CyberRx, specifically focused on helping small and medium-sized companies (SMBs) improve their cybersecurity readiness. Our CyberRx software platform allows SMBs to assess their capabilities using a unique application of the *Cybersecurity Framework's (CSF)* five key functions: Identify, Protect, Detect, Respond, and Recover to better understand their cybersecurity posture, assess their risks and financial exposure; and provides them with a customized and detailed plan of action to improve their cyber readiness. CyberRx is both accessible and affordable, as we believe the best cybersecurity solutions should be available to all organizations, particularly the most vulnerable—SMBs.

It is also a privilege for me to serve as the first small business chair of the *IT Sector Coordinating Council* (IT SCC) since its establishment over a decade ago. The IT SCC, comprised of the nation's top IT companies, professional services firms, and trade associations, represents private sector interests in cybersecurity and critical infrastructure protection to the U.S. government. The IT Sector, represented by industry via the IT SCC and by Government via the IT Government Coordinating Council (GCC), work together in a public private partnership led by the IT Sector-Specific Agency (SSA), Department of Homeland Security (DHS), to address a wide range of critical infrastructure security and resilience policies and efforts affecting organizations of all sizes.

As a champion and advocate for cybersecurity readiness, I regularly meet with and speak to small business groups and CEOs about cybersecurity. I have also been involved in several efforts to promote cybersecurity information sharing in the SMB community, including the creation of the American Small Business Cybersecurity Xchange last year, a forum designed specifically to bring together SMBs, technical experts, and policy makers to address small business cybersecurity concerns. Last summer, I had the opportunity to testify to the Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies, of the Committee on Homeland Security on the Cybersecurity Information Sharing Act ("CISA") program and its impact on SMBs.

I am grateful for the opportunity today to testify as a small business owner. As you know, the definition of small business varies by industry. Depending on the industry, a company with 500, 1,000, or even 1,500 employees can still be considered a "small business" based on size standards defined by the Small Business Administration (SBA). The focus of my testimony today is for SMBs that have operational responsibilities to protect data for their employees, customers, vendors, or partners, regardless of size.

The perspectives and recommendations I share are informed by my own experiences running a small business, interactions with other small business owners, as well as my involvement with the IT SCC. Please note however that my observations do not necessarily reflect the views or positions of the IT SCC.

In my testimony, I will discuss:

- Cybersecurity information sharing in the SMB community,
- How the Cybersecurity Information Sharing Act (CISA) can be helpful to SMBs,
- Incentives to improve SMB information sharing and cyber threat reporting with the government, and
- Concluding thoughts.

Small Businesses Are Reluctant to Share Cybersecurity Information

Cyber-attacks are hurting small businesses. In the last 12 months, 61 percent of SMBs report that their companies have experienced a cyber-attack. More than half involved exposure of customer and employee information, with an average cost of $1,027,053 due to damage or theft of IT assets and infrastructure[1]. Recent ransomware attacks have been devastating with 1 in 5 companies forced to immediately shutdown operations for three days and in some cases, more than two weeks.[2] And while many believe their organizations are susceptible to external cybersecurity threats, a stunning 71% are not prepared to address them.[3]

Solving this problem requires greater information sharing between the government and the SMB community to help companies better identify threats, protect their infrastructure, detect anomalies, respond to, and recover from significant cyber events. However, there is a reluctance among many SMBs to voluntarily share information with government entities. Some of the frequently cited concerns include:

- Information gets lost or goes into a "black hole" causing companies to worry about what is happening with their data and whether it is being secured
- Requests for similar data from different agencies consumes scarce resources, distracts from business focus, and is costly
- Slow response time to requests/inquiries
- Information is misunderstood or misused
- For SMBs that do business with the government, fear that any negative information that is shared may be used against them in future procurements

For any sharing information initiative to deliver real value and have substantive impact, it must be based on mutual trust, which cannot be mandated or demanded. As the government looks to encourage greater cybersecurity information sharing with small businesses, understanding some of the concerns SMBs have about sharing information, in general, with the government may be useful in developing strategies to overcome potential hurdles to sharing reporting cybersecurity specific information.

[1] 2017 State of Cybersecurity in Small and Medium-Sized Businesses, Ponemon Institute, September 2017

[2] Second Annual State of Ransomware Report: US Survey Results, Malwarebytes, July 2017

[3] Cyber Threats to Small and Medium-Sized Businesses in 2017, Webroot, 2017

CISA Applies to Small Businesses, But They Don't Know

In my testimony last year to the House Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies, of the Committee on Homeland Security, I provided some observations on the new law and suggestions for how CISA could be made more relevant to the SMB community. While significant progress has been made in implementing the law in general, several challenges raised last year still persist for SMBs.

1. ***Small businesses are still unaware of CISA or how it helps them.***

   In its Biennial Report on DHS' Implementation of the Cybersecurity Act of 2015, the Inspector General noted that since the law passed, DHS has taken some important steps to: 1) develop adequate policies and procedures and a supporting capability to share cyber threat indicators and defensive measures; 2) properly classify cyber threat indicators and defensive measures and account for the security clearances of private sector users; and 3) use the cyber threat indicator and defensive measure information received to mitigate potential security risks.

   The report, however, did not mention anything about raising SMB awareness of information sharing initiatives and CISA. While there are minimal references to small business in the law itself, arguably CISA does apply to SMBs and addresses some of the barriers to information sharing identified above, particularly in the area of liability protections. To encourage greater cybersecurity information sharing, CISA provides: 1) protection of properly designated proprietary information; 2) exemption from Federal and State FOIA Laws for information shared under CISA ; 3) protections against regulatory or enforcement actions taken as a result of information shared under CISA; 4) non-waiver of privileges and other legal protections, including trade secret protection; 5) anti-trust exemption for sharing cyber threat information or defensive measures with other companies; and 6) protections for sharing and receiving information when done in accordance with CISA's requirements.

   There is still an opportunity for DHS and the government in general to increase the visibility of the law through its existing outreach and awareness programs to the SMB community through, for example, DHS' Stakeholder Engagement and Cyber Infrastructure Resilience (SECIR) initiatives, Small Business Administration (SBA) programs, or by working with Chambers of Commerce, small business associations, and trade groups.

2. ***Small businesses are still confused by the myriad of information sharing initiatives.***

   The number and variety of information sharing initiatives continue to expand. It is still unclear to many small businesses whether they need them, and if so, which to use and when. Government options include agency resources for specific industries (e.g. Energy, Financial Services), DHS' Enhanced Cybersecurity Services, the Cooperative Research and Development Agreement, the National Cybersecurity and Communications Integration Center, the Automated Indicator Sharing program, among others. On the industry side, Information Sharing and Analysis Centers (ISACS), Information Sharing and Analysis Organizations (ISAOs), and private for-profit and non-profit organizations also offer a range of services. An SMB Guide for Cybersecurity Information Sharing would help SMBs better understand the value various information sharing options provide.

3. ***Cybersecurity information can be costly for small businesses.***

   When it comes to information sharing, one size does not fit all for SMBs who must decide what services are most critical weighed against their risk tolerance, capabilities, and budget. One of the distinct advantages the government has in sharing cybersecurity information with SMBs is that the information is "free." However, while the data may be free, many small businesses do not have adequate resources to stand up the necessary infrastructure to exchange data or the technical expertise to manipulate and analyze the data in a useful way. Depending on the type of business, it may make more sense for a particular SMB to sign up with a commercial information sharing organization. Unfortunately, many of the options available today cost thousands of dollars per year, putting them out of reach for many SMBs.

Incentives to Improve SMB Information Sharing And Cyber Threat Reporting With The Government

Many studies have been conducted and papers written over the years on incentives and whether or not they have a determinative impact on behavior. While the data may not be conclusive, incentives have been shown to work better when designed with specific outcomes in mind. Below are a few for consideration. Several of these proposals have been offered over the years in various forms, but with the increasing risk facing SMBs, the time is right to take action.

1. **Expand CISA liability protections to protect SMBs from potential liability in the event of a data breach or cyber-attack**

   CISA currently protects companies when sharing cyber threat indicators and defensive measure with other companies, but it does not currently shield companies from potential liability in the event of a data breach or cyber-attack. To provide a positive incentive for SMBs to share information with the government, Congress might consider a solution that extends liability protection up to a maximum threshold in the event of a data breach or cyber-attack to SMBs that exhibit a measureable commitment to information sharing through demonstrated use of the Cybersecurity Framework developed by NIST to increase their maturity above and beyond the partial level, voluntarily participate in one or more public or private information sharing forums, and maintain active cybersecurity insurance.

2. **Tax Incentives**

   Tax incentives are often used by governments to promote specific behavior, in this case improving cybersecurity information sharing. To further encourage voluntary sharing of cyber threat information with the government, an ISAC or an ISAO, Congress might consider introducing tax incentives that could include deductions and credits for cybersecurity and information sharing related capital investments and personnel, incentives for accelerated depreciation of cyber-related equipment, deductions for cybersecurity related expenses, etc.

3. **Include use of the CSF and participation in a public or private information sharing program as a selection criteria for government procurements**

   The government has and continues to use preferential consideration in the procurement process to promote participation or influence desired behavior. Examples include procurement considerations for minority groups, quality and process improvement standards such as ISO, CMMI, and research priorities, among others. To encourage greater cybersecurity information sharing and reporting, Congress might consider use of the CSF and participation in a public or private information sharing program as selection criteria in government procurements. GSA offers recent examples of preferential consideration for quality standards in procurements such as its GSA Alliant 2 Small Business GWAC.

4. **Recognize SMBs that commit to cybersecurity information sharing**

   Public recognition offered by voluntary programs can be important instruments to promote desired behavior while serving as a signal of commitment or quality to the market. Programs such as EPA's Energy Star, a joint program of the Environmental Protection Agency **(**EPA**)** and the Department of Energy (DOE), has produced impressive results over the past 20 years, by recognizing and highlighting consumers, businesses, and industry committed to the adoption of energy efficient products and practices. Voluntary programs like this could serve as a blueprint to design a public recognition program for SMBs participating in public or private cybersecurity information sharing programs.

5. Simplify the entry point for cyber threat reporting for SMBs

When it comes to reporting cybersecurity incidents, most SMBs either don't know who to call or are overwhelmed by the choices, and therefore, won't bother. For example, on one government website, the following guidance is provided.

> **If Your Business Has Been The Victim of a Cyberattack**
>
> - Inform local law enforcement or the state attorney general as appropriate.
> - Report stolen finances or identities and other cybercrimes to the Internet Crime Complaint Center.
> - Report fraud to the Federal Trade Commission.
> - Report computer or network vulnerabilities to US-CERT via the hotline: 1-888-282-0870 or the US-CERT website

While such guidance is intended to be helpful, most SMBs don't know how or where to get the contact information for several of the resources cited in order to report.
Perhaps the "911" system provides a model. Since 1968, "911" has been designated as the nationwide emergency number for the public to request emergency assistance and provides fast and easy access to a Public Safety Answering Point (PSAP). Last year, the Critical Infrastructure Partnership Advisory Council (CIPAC) formed a working group with DHS' Office of Infrastructure Protection to investigate how to get a National Tip Line started that would serve as the single POC for reporting emergency cybersecurity information. Using the example above, one could envision a scenario where an SMB calls the national emergency response number and based on information provided would immediately be connected to the appropriate resource(s). Initiatives like this are an important step in simplifying the process for cyber reporting and encouraging more SMBs to engage.

Conclusion

CISA is still early in its life cycle but holds tremendous promise for the value it can bring, in particular, to the SMB community as more companies become aware of the law and how it can help them. We at e-Management and CyberRx look forward to continuing to work with Congress to promote greater information sharing and to make the application of CISA more relevant to the SMB community. Thank you again for the opportunity to testify. I am ready to answer any questions you may have.