Testimony

of

C. E. “Tee” Rowe

President/CEO

America’s SBDC

March 8, 2017

Committee on Small Business

Hearing on

Cybersecurity: Federal Resources and Coordination

Chairman Chabot, Ranking Member Velazquez, members of the committee. Thank you for inviting me to testify on behalf of America's SBDC, the Association of Small Business Development Centers.

SBDCs operate over 1,000 centers in all fifty states as well as the District of Columbia, Puerto Rico, the Virgin Islands, American Samoa and Guam. SBDCs provide management and technical assistance to over 200,000 small businesses every year and training to over 300,000 business owners and their employees. All of these small business owners have the same basic question, "How do I succeed?". That's not always a simple answer but, for almost every business that means maximizing sales, and we've been able to aid those clients to the tune of nearly 7 billion of new sales every year.

This is a great statistic, but it contains a not too hidden peril, cyber-crime. More and more of our clients do business online. Every single one of them is vulnerable, and they may not even know it. They may not even have a website but they are potential victims. Every time they run a credit card transaction, or answer their email they expose themselves and their customers to the risk of hacking, phishing and ransomware.
And the dangers go beyond e-commerce. Any business, whether a vendor or a contractor, is at risk if they are connected and have personally identifiable information or the potential to be an access point to others who do.

By now I assume everyone is aware of the alarming statistics about cyber-crime. Cybercrime costs the global economy about $445 billion every year, with the damage to business from theft of intellectual property exceeding the $160 billion loss to individuals. Fifty percent of small businesses have been the victims of a cyber-attack and over 60 percent of those attacked will go out of business.

Despite these facts many small businesses continue to ignore or avoid the risk. Many of our clients believe, “I don’t do business online or I don’t have any valuable information.” Of course, the truth is exactly the opposite. Every time they take an order, swipe a credit card or send an email they put themselves and their customers at risk. Too often the concern is for customer privacy but corporate clients and vendors are at risk too.

Small business present cybercriminals with an easy way to gain access to customer credit card records and bank accounts, supplier networks and employee financial and personal data.

They want to do more and more business online but they have weaker online security. Or they use cloud services that don’t have strong encryption. As a result, the small business can be a gateway to gain access to clients, business partners, and contractors and a backdoor into many large organizations. To a hacker, that translates into reams of sensitive data behind a door with an easy lock to pick. If a small business has any Fortune 500 companies as customers, they are an even more enticing target. These secondary attacks are now a regular problem for small business.

Small businesses are particularly vulnerable to email attacks mimicking their banks or other trusted institutions and citing an urgent need for account or some other vital information, and often multiple employees have access to that information. Further, business accounts do not enjoy the same protection against loss as consumer accounts—something many small-business owners do not discover until it’s too late. Consumers are protected by regulations which limit their liability. Commercial accounts, however, are covered by the Uniform Commercial Code (UCC) and enjoy no such protections. Under the UCC banks aren’t liable for unauthorized payments if their security is considered “commercially reasonable”. As a result, few small businesses that are the victims of cyber theft ever recover their funds.

More than ever, sensitive data, intellectual property and personal information of small and medium sized firms are targeted by an ever increasing and sophisticated community of cybercriminals. Symantec has found that over the last several years there has been a steady increase in cyber-attacks targeting businesses with less than 250 employees.

And not all hacking is for financial gain. Two years ago, several businesses were simultaneously hacked and their websites were taken over by what appeared to be ISIS. Islamic State logos and Arabic script was plastered all over the sites for Montauk Manor in the Hamptons; Eldora Speedway in New Weston, Ohio; Dogwoods Lodge dog kennel in Des Moines, Iowa; Sequoia Park Zoo in Eureka, CA; Montgomery Inn in Montgomery, Ohio; the Moerlein Lager House in Cincinnati; and Elasticity, a vocational charity St. Louis, MO. No financial information was stolen but imagine the time, effort and lost business for each of these firms. They had to rebuild their sites and try to rebuild client confidence. After all, if you knew a hotel had been hacked would you give them a credit card to hold a reservation?

At the SBDCs we have been working to spread awareness of all these threats to our clients. We offer training programs to our clients at most SBDCs and we are working to expand the coverage to the entire network. In our centers in New York, Delaware, Florida, Texas and others we are developing programs to not only advise and inform our clients but spread the information and training capacity throughout our networks. In Florida, our network is collaborating with Ridge Global, the firm founded by former DHS Secretary Tom Ridge, to develop a series of training videos on cybersecurity. The New York SBDC has developed a cybersecurity planning guide which we are working to disseminate to other states to help them build their capacity. In Michigan, besides training, our network is launching a media campaign day to spread awareness. SBDCs began developing these resources on our own over the last few years. My members recognized that, while they are advising and training their clients on the value of the web as a marketing and sales engine, they also needed to educate them on the dangers and pitfalls of the web.

On top of the organic efforts within the SBDC networks we are now working at the national level to help develop a national small business cyber strategy. Pursuant to section 1841 of the National Defense Authorization Act for 2017 America's SBDCs is working with the Department of Homeland Security (DHS) and the Small Business Administration (SBA) to develop a strategy to leverage the collective resources of DHS, SBA and the national network of SBDCs to provide the resources, training and assistance small businesses will need.

We will be working share and improve cyber programs, enhance services and raise awareness of the threats. In particular, we want to help develop cost-effective, high-quality tools for small business and a network to share information and analysis on threats.

On behalf of our clients I want to thank the members of this committee for their efforts in getting that language included in the NDAA. The timing could not be more critical, the threats and the awareness of the threats has grown but at the same time so has the confusion. What steps do small businesses need to take? Do they need security software, a cyber specialist, certifications? What tools are effective, what certifications are valid?

SBDCs are developing and training small businesses on that first line of their cyber security needs, the internal focus of basic security practices. Teaching employees about the threats and weaknesses, helping them protect client and customer information. They are also working with small businesses to help them recognize and develop their own strategies and assessments of their needs. My members have developed some excellent education and it will grow stronger but the harder effort is going to be assisting small businesses in dealing with the external demands of cybersecurity.

Commercial customers and big business will have growing demands on the cyber infrastructure of their small business suppliers. What certifications will they demand, what hardware? Who will supply these certifications, and at what cost? If we add federal procurement issues (already a complicated area) how will small businesses cope? I want to divide this area of concern into two sides – commercial business and government business.

On the commercial side, small business faces a real problem. Who is in charge and to whom are they responsible? Last year, the Federal Communications Commission (FCC) stepped into the world of e-commerce and declared Internet Service Providers (ISPs) to be "common carriers". Now the FCC has decided to hold off on the privacy rule in favor of "harmonization". Small businesses are left to wonder, "Who is responsible, anyone?

At America's SBDC we will be working hard to ensure that our clients have the best possible, most cost-effective tools. At the same time, it would nice to know if anyone further up the "food chain" is to be held accountable. There is a real concern about the trickle down nature of the regulatory framework. While titans like Verizon and Comcast battle Google and Facebook, what level of regulation will be placed on small business?

We know there is a potential for small business to be a back door. Does that mean, in a regulatory framework controlled by internet giants, that the rules will be set by the giants at the expense of the pygmies? We have already seen Google declare that websites without what they consider "adequate security" will be labeled "unsafe". I do not doubt that http vs. https is serious, but how many small businesses are either aware of this distinction or aware of what they need to do to be Google compliant?

I expect Google aficionados and techies will call me a Luddite. They would be wrong. I use Chrome and love it. I know what an SSL certificate is. How many small business owners do, or know where they can get the help they need? How much business will a small business lose because they are on eBay and, as of the end of January, eBay wasn't https compliant?

These are the types of trickle-down, large firm favoring regulatory schema about which we should be concerned.

Now I'd like to comment on the government side. The previous administration was proud of their efforts and successes at meeting small business contracting and subcontracting goals. I'm concerned about how whether that success can last. Unfortunately, a lot of the uncertainty we face now is because the previous administration also put out cybersecurity regulations at the very end of their term before anything could really be discussed and tried out. The result is the uncertainty and confusion we see now.

There should be significant concern that federal and state agencies will begin to develop conflicting and potentially contradictory procurement regulations, derived from the best intentions regarding security and privacy, but having a negative effect on small business participation. The Department of Defense has issued cybersecurity amendments to the Defense Acquisition Regulations (DFAR) and the FAR Council issued amendments to the Federal Acquisition Regulations (FAR). Just recently the Department of Homeland Security released three proposed regulations on cybersecurity though they are, I believe being held by the current administration. Those regulations weren't even for classified information; they were for Controlled Unclassified Information (CUI). To date, I have seen only two comments in the Federal Register. I doubt any small business that contracts with DHS is aware of these proposed regulations, and many of our SBDC clients are those affected businesses.

How will all these regulations operate? Can they co-exist? Agencies issue the proposed rules and state they will "harmonize" them with FTC and other efforts, how? Who will "harmonize" them? These regulations have the best and most laudable goals, protecting government data integrity and protecting citizens' privacy. However, the potential costs of compliance for any small business involved in, or wishing to be involved in government contracting could be crippling. Will the standards be set at the convenience of the largest contractors with small businesses left to wonder how they'll be able to comply?

In addition, what will happen to subcontractors? Imagine a one-size fits all cybersecurity protocol that flows down to subcontractors. The potential for small businesses becoming frozen out is very real.

That is why America's SBDCs is glad to be working on this strategy with DHS and SBA now. We want to help head off the confusion and provide training to ensure opportunity is not sacrificed for cybersecurity. At America's SBDC we believe it important to be at the front of this effort, to develop a set of resources to enable small business participation through assistance and training, rather than having to play "catch up" with small businesses confused by a new regulatory framework.

Thank you again for the opportunity to testify. I look forward to your questions.