"Protecting Small Businesses Against Emerging and Complex Cyber-Attacks" House Small Business Subcommittee on Health and Technology

March 21, 2013

Submitted by:

The Computing Technology Industry Association (CompTIA)
515 2nd Street, NE
Washington, DC 20001

Computing Technology Industry Association (CompTIA)
Public Advocacy
515 2nd St NE
Washington, DC 20002
202-503-3624

Introduction

Good afternoon, Chairman Collins, Ranking Member Hahn, and distinguished members of the House Subcommittee on Health and Technology. This testimony is submitted on behalf of the Computing Technology Industry Association (CompTIA).

My name is Dan Shapero, I am a CompTIA member and the Founder of ClikCloud, a company I launched in 2010 focused on offering a variety of IT services, such as Digital Marketing, Website hosting, SEO (Search Engine Optimization) blogging, email newsletters, and other business advisory services.

I am a California native and graduated from the University of California, San Diego. Prior to ClikCloud I spent 20 years working as a technology executive, including at Ernst and Young, a professional services organization, and at Kaseya, an IT automation and cloud services based business. I have launched or helped other entrepreneurs launch several IT startup companies. For instance, my past clients include Vincinity which is now Microsoft Maps, and Avamar which is now EMC2.

In short, I have 25 years of experience in the IT sector as an executive and entrepreneur. I have worked on cybersecurity issues for 8 years and have looked at the issue as a user and a service provider.

I want to thank Chairman Collins, Ranking Member Hahn, and Members of this Subcommittee for holding this important hearing to "examine the increased volume and complexity of cyber-attacks as it affects emerging technologies utilized by small businesses, such as cloud computing and mobile technology."

From the perspective of a small tech business, cybersecurity is among the most important issues facing small and medium size companies. We will highlight this point shortly, but first some background on CompTIA.

About CompTIA

The Computing Technology Industry Association (CompTIA) is the voice of the world's $3 trillion information technology industry. CompTIA membership extends to more than 100 countries. Membership includes companies at the forefront of innovation along with the channel partners and solution providers they rely on to bring their products to market and the professionals responsible for maximizing the benefits that organizations receive from their technology investments. The promotion of policies that enhance growth and competition within the computing world is central to CompTIA's core functions. Further, CompTIA's mission is to facilitate the development of vendor-neutral standards in e-commerce, customer service, workforce development, and ICT (Information and Communications Technology) workforce certification. CompTIA is also the leading global provider of IT workforce vendor-neutral certifications. Currently there are over 1.4

million CompTIA IT vendor-neutral certification holders worldwide, and many of those are for IT security.

CompTIA's members include thousands of small computer services businesses called Value Added Resellers (VARs), as well as nearly every major computer hardware manufacturer, software publisher and services provider. Our membership also includes thousands of individuals who are members of our "IT Pro" and our "TechVoice" groups. Further, we are proud to represent a wide array of entities including those that are highly innovative and entrepreneurial, develop software, and hold patents. Likewise, we are proud to represent the American IT worker who relies on this technology to enhance the lives and productivity of our nation.

Overview of the IT SMB Sector

As a baseline, the IT security infrastructure for SMB's is as vulnerable to cyber attacks and threats as large companies and firms. Unfortunately, SMB's are less resilient than larger companies because they have fewer IT resources in terms of personnel, hardware and software to combat the onslaught of daily cyber threats and attacks that many SMB's encounter on a daily basis.

Some SMB's are comprised of 5 to 20 employees, so resources come at a premium. As a small business owner I have to rely on my own expertise to implement adequate measures to ensure that the IT infrastructure that supports my business is secure. I also have to make sure that my clients understand the cybersecurity risks and threats to their businesses, and I advise them on the type of cybersecurity compliance measures that they must implement to keep their IT systems secure.

Opportunities for SMB's from Emerging Technologies

In the last five years, we have seen a steady transition from a server environment to a cloud-based one. This has created a tremendous opportunity and boost to the SMB sector. For SMB's, cloud computing services have been a huge equalizer in the marketplace. In the 1990's and early 2000's a new company had to invest considerable resources in IT infrastructure, including mainframes, servers, routers and other IT products and services to satisfy their computing needs. Today, with the advent of the cloud, SMB's can economically subscribe to cloud and virtual computing services from a third party for (literally) pennies on the dollar compared to the cost of building out the infrastructure that would offer comparable services. The emergence of cloud technologies is now allowing SMB firms affordable access to IT infrastructure, including software, that was financially beyond reach only a few years ago. This is an exciting time in the IT SMB sector, and it is even more critical now that we ensure there are adequate measures and controls in place to protect SMB's from cybersecurity threats and attacks.

As an IT professional, entrepreneur, and CompTIA member I would like to highlight two policy issues that have a significant ongoing impact on the IT SMB sector.

Data Breach Notification Reform

First, the majority of cyber attacks create exposure across state lines. For this reason data breaches are an area of serious concern. There are currently 47 state data breach notification (DBN) laws in place. These laws establish the circumstances under which a consumer must be notified when a breach of their personally identifying information (PII) has occurred. We think that consumer notice is a fundamental consumer right and we fully support it.

The issue for the SMB sector is that ongoing compliance with the patchwork of 47 different data breach laws across the country are an unnecessary burden, and in some instances, an insurmountable regulatory hurdle for an SMB to overcome. For example, state DBN laws vary as to when a consumer notice should be provided. Some state DBN laws require consumer notice when a company is made aware of a breach. Other state laws require consumer notice only if the breached data has the likelihood of resulting in consumer harm to the consumer. Moreover, all state DBN's differ on the type of penalties and fines that can be imposed and whether a consumer can file a private right of action against a company that has suffered a breach of consumer PII. These issues are compounded in the context of the cloud due to the mobility of data. In a cloud environment data travels across multiple jurisdictions adding more uncertainty for SMB's who may not have the resources to understand their DBN compliance obligations.

As mentioned earlier, SMB's tend to be very small with only a few employees. An annual report by the Ponemon Institute found that the average cost to a business for one incident of data breach to be $6.75M and $214.00 per customer record compromised.[1] A contributor to these costs arises from legal compliance and related expenses. For many SMB's an exposure of $6M is enough to send an SMB into bankruptcy.

To be clear, CompTIA supports data breach notification laws, but again, the issue is that the current patchwork of state data breach laws imposes duplicative costs and undue burden on SMB's. SMB's must hire lawyers and expend other resources simply to track down the various compliance obligations. With our increasingly mobile economy these laws are getting even more complicated to understand since it is not always clear what state a data breach may have actually occurred in which can be different from where a consumer may reside.

Therefore, CompTIA believes that the creation of a national framework for data breach notification can go along ways towards reducing costs and eliminating barriers to entry

[1] http://www.ponemon.org/news-2/23

for SMB firms. A national framework for data breach notification will serve as an incentive toward the expansion of IT services across state lines.

Workforce Development

Another issue that we face as small and medium size businesses is the ability to recruit and retain in-house talent to help protect ourselves from cyber attacks. As Advanced Persistent Threats (APT) become more advanced and more persistent, all of our employees have a responsibility in keeping us secure; especially those in IT related roles. However, there is a skills-gap issue that is affecting the IT community as a whole. There are approximately 250,000 open IT jobs in the U.S. at any given time. As the SMB community, not only are we competing with the rest of the world for this talent, we are competing against other larger U.S. companies with big names. If the ecosystem were better saturated with the necessary skills, it would be significantly easier for us to attract candidates to our open positions. There are a lot of great opportunities that come with working for small and medium size companies that you cannot get in a larger institution, but we simply cannot compete with the recruitment dollars that are spent by the bigger names.

Certifications play an important role in this conversation. It is not the magic bullet, but it is a critical part of the solution. It is a way for us as employers to know that an applicant knows what they say they do and to have a professionalized IT workforce. The government should lead by example by hiring individuals who have earned industry-recognized certifications and by encouraging their existing IT employees to earn certifications. This will encourage others looking to enter the cyber workforce to focus on certifications as an entry point and help close the skills gap. Having access to a plentiful and skilled workforce will help companies like mine protect themselves from cyber attacks.

Finally, we believe that education about the steps SMB's should take to protect their IT infrastructure goes a long way toward making the overall US IT ecosystem more secure. Many of the IT vulnerabilities come from human error and negligence. For example, failure to implement security passwords or failure to keep the passwords secure with certainly reduce the overall threat of cybsecurity. Also, sharing information about how to safely share and exchange, information on the Internet can also help the overall ecosystem.

In closing, I would like to share for the record with this Subcommittee CompTIA's Information Security Trends report (https://comptia.box.com/s/f2pob0gz7rl6hj5tdg9e), and a link to a recent blog which I have highlighted below: (http://clikcloud.com/blog/2013/03/07/cyber-security-threat-to-small-business/).

Beef up your Network Security to Avoid Cyber Security Threats

Your network is only as strong as the weakest point. To avoid threats from Cybersecurity make sure you have a Firewall in place and keep all connected devices have up to date firmware, operating system patches and keep the latest anti-virus and anti-malware definitions current.

Cyber Security Education and Training

Educate your employees and staff on the threats of cybersecurity. Make sure they are aware of the threats of Phishing schemes and are able to identify and avoid these dubious attacks. Train all employees on the risk of sharing privacy data such as name, email, birthdays and financial information on social media networks.

CyberSecurity Policies and Procedures

Establish clear procedures on notification and escalation of a data leak or data breach. Ensure your team knows how to escalate a concern within your company. It is more important to raise the issues quickly rather than cover up a Cyber Security breach. Ensure you have clear policies on how to coordinate notifications outside of your company, should an attack occur.

CyberSecurity Insurance

Cybersecurity insurance is designed to help mitigate the loss of data leaks, network damage and other financial exposure of a Cyber Security attack. Your business may be eligible for affordable insurance to cover costs associated with CyberSecurity attacks.

There is no way to totally eliminate the risk of a Cyber Security attack, however, there are steps you may take to prevent attacks and be prepared on what to do in case your business is victimized. Contact your IT Support organization for a complete IT Security Assessment.

Closing

Thank you again for the opportunity to share our perspective on the issue of cybersecurity, and I would be happy to answer any questions.