Testimony of Rick Snow

Owner

Maine Indoor Karting

On behalf of the National Small Business Association

House Small Business Committee

"Small Business and the Federal Government: How Cyber-Attacks Threaten Both"

April 20, 2016

1156 15th Street, N.W., Suite 502
Washington, DC 20005
202-293-8830
www.nsba.biz

Good Morning. Thank you Chairman Chabot, Ranking Member Velázquez and members of the House Small Business Committee for inviting me to testify today on the current state of cybersecurity for small companies and how credit card fraud and phishing scams have impacted my own small business.

My name is Rick Snow and I am the owner of Maine Indoor Karting located in Scarborough, Maine. My wife, Lori, and I started our business in 2003 after being downsized from the financial services industry. We are an indoor entertainment venue with a ¼ mile go-kart track, mini-golf, arcade, and café. We have had as many as 40 employees but since the recession of 2008 we have dropped to less than 20 full and part time employees after losing 35 percent of our gross revenues. We hope to get back to our 2007 gross revenue this year or next.

I am pleased to be here representing the National Small Business Association (NSBA), where I currently serve as a Board of Trustees Member and chair of the Environmental and Regulatory Affairs Committee. NSBA is the nation's oldest small-business advocacy organization, with over 65,000 members representing every sector and industry of the U.S. economy. NSBA is a staunchly nonpartisan organization devoted solely to representing the interests of the small businesses which provide almost half of private sector jobs to the economy.

Cybersecurity Landscape

In the last few years, cybersecurity has emerged as one of the most pressing concerns facing both the private and public sectors. Cyber criminals are becoming increasingly sophisticated in their attacks on networks and their attempts to steal personal information that can ultimately lead to severe financial distress. These attacks happen every day and are often completely undetected until well after the damage is done. Some particularly insidious attacks take weeks to slowly infiltrate systems and fully develop. While still other attacks target a third party network, with the hope that the real target will access the infected network.

The terms "data breach" and "identity theft" have truly entered the everyday vernacular of the American public. The enormous breaches at the Office of Personnel Management (OPM) in 2013 and the Internal Revenue Service (IRS) in 2015 in addition to breaches at large nation-wide retailers, grocers and other high-profile incidents have heighted awareness and concerns about these threats. However, heightened public awareness has not stemmed the tide of these threats. There is certainly more to be done to protect all American interests, particularly America's smallest employers, from the dangers these attacks pose.

Private Sector

The threat posed by these attacks to the private sector is enormous, in terms of both the interruption of normal business operations and the direct financial cost of the attack. In a recent report compiling information from 70 different organizations there were almost 80,000 security incidents from 2014-2015 resulting in over 2,122 confirmed data breaches.[1] That is an average of more than 1,000 security incidents a year per organization and more than 300 confirmed data breaches. What is even more alarming is that in almost half of those data breaches, it is not even clear how much data was taken[2], making assessing the damage and repairing it incredibly difficult.

One thing to keep in mind about the private sector is that it is very diverse, whereas the public sector is much more homogenous. In the private sector entities can be differentiated by function structure, industry, and perhaps most importantly, size. This means that there are many more dynamics at play when looking at solutions in the private sector than you may see on the public side. As I will highlight later in my testimony, small businesses like mine have different security challenges and needs than a larger corporation may have when dealing with cybercriminals.

Public Sector

While government agencies are generally structured fairly similarly, it is alarming to me that there have been several high-profile cybersecurity incidents in the past several years spanning multiple agencies. Incidents at both OPM and the IRS have highlighted how much sensitive information the government is entrusted with by the American public. The most recent cybersecurity report published by the Office of Management and Budget (OMB) illustrated the scale of attacks being levied against government agencies. From Oct. 1, 2014 to Sep. 31, 2015, the government reported 77,000 cybersecurity incidents, up 10 percent from the previous year.[3]

Of particular concern to the small-business community is the performance of the U.S. Small Business Administration (SBA) in this report. Although, there has been a marked decline in policy violations at the agency in the past three fiscal years, this report indicated that in FY 2015, there were three times more incidents involving suspicious network activity than in FY 2014.[4] It is further concerning that SBA continues to lag behind other agencies in certain email screening

[1] Verizon, *2015 Data Breach Investigations Report* 1 [hereinafter *DBIR*], *available at* http://www.verizonenterprise.com/DBIR/2015/.
[2] *Id.* at 3.
[3] Office of Management and Budget, *Annual Report to Congress: Federal Information Security Modernization Act* 5 (2016) [hereinafter OMB Report], *available at* https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy_2015_fisma_report_to_congress_03_18_2016.pdf.
[4] *Id* at 59.

and phishing prevention programs.[5] The report indicates the SBA email systems simply do not check sender verification when receiving messages from outside the network[6] and use of content filtering programs to prevent access to websites posing cyber threats is nonexistent.[7] SBA has and handles sensitive information concerning millions of small businesses, and the results of a large-scale breach within the agency could be catastrophic for the small-business community. It is quite worrisome to me that the very federal agency tasked with supporting small businesses lacks the essential resources to defend us against cybercriminals.

Breaches at the government level, particularly at the IRS, are troubling for small-business owners because the financial stability of the owner is inextricably tied to the stability of the small business and vice versa. A financial loss on the personal front can seriously impair the functioning of the business while a loss for the business can potentially be detrimental to the owner and their family. These are the dangers that small-business owners face and they are very different than those faced by larger companies. If the federal government cannot protect its networks and data from cyberattacks with almost unlimited resources at its disposal, how can we expect America's small businesses to do so?

NSBA and its members are mindful of the work of Congress in recently passing cybersecurity legislation and applaud their efforts. Facilitating dialogue between the public and private sector about threats is terribly important. There needs to be continued thought given as to how to make this dialogue truly beneficial for small businesses. Any federal discussion on cybersecurity or development of a private-public partnership or advisory board must include representatives of small business. NSBA has long urged Congress to move forward on establishing streamlined guidelines and protocols to ensure the protection and security of online data and financials, but caution against a knee-jerk reaction that would unfairly place a disproportionate burden on America's small firms.

Congress also needs to realize that most of these attacks move alarmingly fast. Approximately 75 percent of attacks spread from the victim 0 to victim 1 in less than a day, while almost 40 percent of them do so within 1 hour.[8] Keeping in mind the infrastructural limitations of small businesses, it is crucial Congress finds ways to keep them abreast of these threats by providing clear, simple steps companies can follow when their data is breached and balancing the need for greater information sharing with privacy rights.

[5] *Id* at 69, 72, 75.
[6] *Id.* 69.
[7] *Id.* at 75.
[8] *DBIR*, at 11.

Small-Business Perspective

Given the increasingly commonplace occurrence of hacking and cyber-crimes, coupled with the fact that, over the past few years in a difficult economy, small-business owners are handling more of their firm's IT operations, cybersecurity is a growing concern for small business. Even a simple cyber attack can effectively destroy a small business.

Has your business been the victim of a cyber-attack (i.e. computer virus, malware/spyware, website hack, credit card or banking hack or trojan, etc.)?

	DEC. 2015	DEC. 2014
Never	58%	50%
Only once	17%	16%
2 to 5 times	21%	28%
More than 5 times	4%	6%

What was the nature of the cyber-attack? (check all that apply)

My computers were hacked	34%
My credit card information was stolen	31%
My website was hacked	17%
Our entire network was hacked	13%
My bank account was hacked	10%
My company information was hacked from a third-party (i.e.: insurance company, accounting company, etc...)	7%
Our cloud data was hacked	2%
Other	16%

These attacks are startlingly becoming more common among small businesses. In a recent NSBA survey, 42 percent of members indicated that they had been the victim of cyber attack.[9] In almost a third of those attacks on NSBA members, credit card information was stolen. In 13 percent of the attacks the entire network was compromised and in 10 percent a bank account was hacked.

The NSBA Year-End Economic Report emphasizes the fact that in an increasingly technology-reliant global marketplace, cybersecurity issues and vulnerabilities can bring commerce to a screeching halt. In almost half of the attacks, there was an interruption in service.[10]

[9] National Small Business Association, *2015 Year-End Economic Report* 12 *available at,* http://www.nsba.biz/wp-content/uploads/2016/02/Year-End-Economic-Report-2015.pdf.
[10] *Id.* at 13.

On average, how long did it take to resolve cyber attacks?

	DEC. 2015	DEC. 2014	AUG. 2013
Less than 1 day	24%	30%	38%
Between 1 – 3 days	34%	34%	40%
Between 3 – 7 days	15%	14%	11%
More than a week	10%	9%	7%
More than two weeks	16%	13%	5%

In 75 percent of the cases, it took more than a day for the issue to be resolved, and 26 percent of the time it took more than a week to resolve.[11] This is in stark contrast to larger companies where an attack may not even slow down operations while sophisticated IT departments repair the damages. But many small businesses are not able to have dedicated IT departments and still others have to outsource IT functions or assign these duties to an employee as a secondary function. In fact, in 2013, 40 percent of business owners were handling IT personally and only 24 percent were outsourcing the function.

For those owners handling it themselves, it is certainly expected that resolving incidents will require research, training, trial and error, and a great deal of time away from the core functions of the business—acting as accountant, benefits coordinator, attorney, and personnel administrator. Simply outsourcing the function is not necessarily a silver bullet either. It can be cost prohibitive for some businesses and there are also issues in expected service delays. Simply put, a small business might not be high on the IT service provider's list of priorities if there is a systemic problem, even though such a firm is more likely to have the experience and technical expertise to resolve the issue quickly. The economies of scale which make retaining in-house IT professionals efficient for larger companies simply do not exist for small businesses and thus creates serious unique challenges to the smallest ones.

Although, small-business owners are becoming increasingly tech savvy, limited resources and knowledge still leave many vulnerable to cyber-threats. However, on average NSBA members indicated that each attack costs them over $7,000. Additionally, when money was stolen from bank accounts as a result of these attacks, the average amount stolen was $32,000. Small businesses often operate on very tight profit margins and seldom carry a lot of excess cash. These losses can be devastating to businesses in those circumstances.

[11] *Id.*

It is unfortunate that the resource limitations illustrated above make small businesses a greater target for attacks than larger companies. Fewer IT resources and dedicated staff mean that cyberattacks may require less sophistication and perhaps even more importantly, garner slower reaction time. In many cases, small businesses without sophisticated monitoring equipment or contractors may not even know they have been the victim until days after an attack. The reality is that those cybercriminals are aware of these limitations and at times specifically target small businesses because of them.

Phishing

Although cyber attacks through "hacking" and viruses are common, phishing continues to be one of the most damaging forms of attacks against small businesses. Phishing is generally when a fraudster sends messages impersonating a business or organization to solicit sensitive information from the receiver—often citing an urgent need to login to an account or provide other vital information. In prior years many of these attempts where rudimentary and conspicuous. However, recently they have become increasingly sophisticated, many containing carefully crafted emails mimicking those of the impersonated bank or other trusted institution or even directing the user to a clone of the impersonated businesses website. Attacks of this nature have increased from about 2 percent of cyber attacks in 2010 to 20 percent in 2014.[12]

Success rates of these phishing campaigns have varied, but in some situations 23 percent of recipients are opening the phishing messages and 11 percent actually click on attachments.[13] These campaigns operate incredibly quickly, often those who open a phishing email do so within an hour of it being received, in many cases because the scams purport to require emergency action. In some tests, the first response to a phishing campaign came in under two minutes.[14] With the ability of employees to work remotely at all hours with constant access to email and other vital company information, this means that a network or sensitive information could be compromised almost instantaneously, at any time. A sobering and terrifying thought for small-business owners. Phishing attempts also continue to be the primary method of cybercriminals who attempt to exploit government systems as well, so small-business owners certainly are not alone in their concerns.[15]

Because the human element and the fear of inaction that these emails are intended to illicit will always compromise some, it is generally accepted that the best way to prevent these attacks from succeeding is to totally prevent phishing messages from arriving at an employee's inbox. This

[12] *DBIR,* at 5.
[13] *Id* at 13.
[14] *Id.*
[15] *OMB Report*, at 22.

cuts against small businesses again because of the limitation on resources. Sophisticated software necessary to filter these messages and detect when the messages succeed is not available to all businesses—making the attack on a small business more likely. In a larger company, very few people would even have access to sensitive information. However, in a small business, proportionally more people with less training would have access to the information, making the number of potential targets more tempting to cybercriminals.

Phishing is also particularly dangerous to small businesses because business accounts do not have the same level of protections and guarantees against loss and theft as those provided to consumers. Business accounts are governed by the Uniform Commercial Code, which does not hold banks liable for unauthorized payments as long as the bank employs a commercially reasonable method of providing security. This means that a small business whose funds are stolen from its account is not guaranteed to have the losses covered. Many small-business owners do not know this until it is too late and never recover stolen funds.

Bearing all this in mind, my experiences with cyber threats should not come as much of a surprised.

Maine Indoor Karting

When I started my business I had the naïve expectation that I would be able to follow my passion and race go-karts with the help of my wife and a few close friends. I had no idea of the demands that are placed on a small-business owner. When you own your own business, everything is your responsibility. I had to become an expert in human resources, insurance, banking, theft, employee psychology, plumbing, electrical work, restaurant management, regulations and advocacy.

My first introduction to the dark side of small business-ownership came three months after opening and we discovered that someone was removing cash from our drawer, after two months and losing an estimated $50,000 we discovered the culprit and let that individual go. I then went through the expense of installing an expensive camera system to work with the installed burglar alarm system. It is unfortunate that I had to take such extreme measures to simply protect my business and to think that it would not be the only or last time I had to take measures to protect my small business from theft.

Phishing can happen to anyone, phishing attacks are meant to scare you and make you act without thinking, given the right circumstances, anyone can be lured by them. I am certainly no exception. I was busy working at my desk one day, when I received an alert email from my bank that there had been a suspicious online attempt to gain access. The email urged me to

immediately log into my account to confirm that it was an unauthorized attempt. The link provided in the email looked identical to the log on page for my bank. Frantic that my business could be loosing all of its funds, I stupidly did just that. As soon as I typed my password I realized that I had been phished. I had to drop my work and race to the local branch of my bank and explain what happened. The bank required that I then set up a new account, which took several hours.

Additionally, I had to order new checks and debit cards for myself, wife, and three staff members authorized to use company cards. It took about a week to rush the new checks and debit cards to us. Since we use the cards and checks for all our bills and local purchases for the events we put on for our customers, I had to either use our company credit card (with a line of credit of 24 percent interest) or my own credit card which I would then have to reimburse myself when the new checks arrived. Situations like this blur the lines between personal finance and that of my small business. The cost was roughly $250 for the new checks and rush order and overnight shipping not to mention the delays and disruptions to my business. It took my wife an additional day to update our entire auto bill paying with the new account numbers and another day on the phone to update the payroll company. Since she runs the day- to-day operations of the business, she had a very stressful week trying to keep up with the regular routine and update all our vendors. However, I know that it could have been much worse, and soon thereafter, I experienced how much worse it could really be.

Two weeks later I was working late, like most evenings, and I decided to check on our business for that day. I logged into our bank accounts, and to my utter horror, I found that my balance was zero. This was a pay day, and I was terrified that the paychecks that were issued that day would not clear. We were supporting a number of families, many of which live paycheck-to-paycheck and could not have made it without the paycheck we issued them that day. I was also very worried about our business' reputation since a restaurant nearby had just bounced their paychecks and the company never recovered from the bad publicity they received from not making their payroll. I quickly discovered that three wire transfers were made that night to three different banks around the country totaling $15,000. Fortunately the payroll company had debited the new account the night before so I knew our employees would be paid.

I then spent the rest of the night trying to get a hold of someone in my bank to stop the wire transfers and recover the money. Because it was so late, none of the banks in my region were open. I was luckily able to get in touch with one bank still open in Washington State. I had to be at the bank first thing the next morning, but I was able to stop the wire transfers. However, I had to than spend another day away from work opening a new account and going through the process—that I had just done—of getting all new cards and ordering new checks. Again, there were disruptions in my ability to make purchases for business. My poor wife had to spend

another week going through the same process she did just two weeks earlier. My wife, who is also our business' book keeper, spent the better part of two weeks away from her normal duties because of this phishing incident. She also told me that if this happened again, I would no longer have a wife or a book keeper. To this day no one knows for sure how the cybercriminal was able to gain access to the new accounts.

My bank told me that this was a standard phishing loss and that I was lucky that I discovered it before 48 hours had lapsed so no money was actually stolen. My business accounts are not protected against theft the way that my personal accounts would be. Other than being out the cost of the two new check books and the man hours and a lost night of sleep I was lucky. I also discovered that there was going to be no one at the receiving banks to arrest the person claiming the stolen funds.

Since then, my wife and I have had our personal credit cards stolen three different times. Like most small businesses the line between our personal finances and that of our business is often blurred, we sometimes have to use our personal credit to support slow times in the business cycle.

The first time my card information was stolen, I received a call from MasterCard security asking me if I was in Japan, I was at home and most certainly not in Japan. After confirming both my wife and I had our credit cards, they informed us that someone had used our card the night before in Japan to make $14,000 worth of purchases and that our cards would be frozen until new ones arrived. Fortunately, the money was frozen on our account and we had to fill out a notarized statement to state that we were not the individuals making the purchases. We were told that we should have the money back in our account in 30 days. This was our Cash Management account so we had to use the margin of our stocks and bonds to support us for the rest of that month. I was later told that someone had cloned our card and used it overseas.

The next time our card was stolen was during the Hannaford loss where it is estimated that seven million card numbers were stolen. As a precaution we were told by our issuing bank that we should replace any cards that we use at Hannaford. We use that company card for both our personal food supply and also use them for our catering needs at the track. Our bank was able to reissue the debit cards for our business that day at the local branch, but our personal cards would need to be overnighted from Morgan Stanley. That was the most frustrating for us because the new card was going to be overnighted to us while we were out-of-town. Because of horrible logistics we had no use of our card for the week we traveled and had to go to a Fed Ex office in Florida to finally pick up our cards.

The most recent was just a couple of weeks ago when my brand new chip card was used in Long Island to purchase $300 worth of products at a Bed Bath and Beyond. Again, I was out of credit card use for a week waiting for my new card.

In all of my cases, I have been lucky that I was not out the money that was stolen. It cost me a lot of my time and frustration to deal with all these attempts and the merchandise purchased with my fraudulent cards was never recovered and someone had to absorb those costs. Now that the laws have changed if I do not use the chips for processing my sales at my business, I will be responsible for those losses. For me, I have now implemented a policy that I hope prevents another phishing expedition using server based software for spam and a second computer based security system to identify junk mail. I pay $500 per year for the software system and the server based system is part of my IT company's package.

Any of these attempts could have ended my business if I was not able to recover the money. Most small businesses do not have a significant cushion to absorb these types of losses, and we are no different. Losing thousands of dollars at bad time could make a significant difference for both me and my business and for my employees.

Conclusion

As small businesses become increasingly dependent on services and applications that connect to the internet, they also become a larger target for cybercriminals looking to exploit vulnerabilities to steal money and credit card credentials, intellectual property, personally identifiable information as well possibly destroy data and disrupt operations. These threats are very real and immediate. In fact, ninety four percent of small-business owners indicate that they are concerned about being targeted by cyber attacks. For many small firms, a cybersecurity incident could lead to an entire network being down for many days until the full extent of the problem is known and then fixed. No to mention that a highly public breach could also damage the business's brand and lead to long-term loss of income.

This is the ongoing threat of the internet age, as more and more small businesses rely on web-based products and services, and it will only persist and evolve as long as the internet continues to facilitate commerce in the global economy. It is unlikely that there will be one solution to stop all of the attacks. In fact, slowing and preventing these attacks will most likely require an ongoing process to identify new threats, vulnerabilities and ultimately solutions. NSBA urges Congress and this committee to always bear in mind the unique challenges that small businesses face and continue to include the small-business community in that process.

Thank you for allowing me to testify before the committee today. I would be happy to answer any questions you might have for me.