Testimony of Robert Luft

Owner

SureFire Innovations

On behalf of the National Small Business Association

House Small Business Committee

"Protecting Small Businesses from Cyber Attacks: the Cybersecurity Insurance Option"

July 26, 2017

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

Good morning. Thank you, Chairman Chabot, Ranking Member Velazquez 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 cyber insurance can help small businesses mitigate risks.

My name is Robert Luft and I am the owner of SureFire Innovations located in Cincinnati, Ohio. The company is a certified Service Disabled Veteran Owned Small Business (SDVOSB) and Minority Business Enterprise (MBE). SureFire Innovations is a network design, security, and installation company that specializes in developing robust network management systems. Our clientele base is largely comprised of medium-and-large-size companies on a national scale.

SureFire Innovations originated shortly after my return from the Army, where I served 16 years as a Combat Engineer. I had the privilege to serve the nation on multiple combat deployments to Iraq. It was during my time in service where I developed the necessary leadership skills to transfer over to the civilian sector as a successful entrepreneur.

I am pleased to be here representing the National Small Business Association (NSBA), where I currently serve on the Leadership Council and the Small Business Technology Council. 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 to representing the interest of the small business which provide almost half of private sector jobs to the economy.

State of Cybersecurity

Cybercrime is growing rapidly with annual costs to the global economy estimated to reach over $2 trillion by 2019. Organizations of all sizes are at risk for cyber-attacks. Small businesses represent more than 97 percent of total businesses in the U.S. and make up an essential part of the supply chain to some of the largest companies, many of which are in critical infrastructure sectors, from financial and transportation organizations to power, water and healthcare suppliers.[1]

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. Due to this current landscape that our networks are operating within, we all must accept that cybersecurity attacks are now an inherent risk for businesses of all sizes—including small entities. In 2015, 43 percent of all attacks were directed at small businesses.[2] Despite the growing awareness of cyber-related crimes, and the increase of small businesses being a target for these attacks, 77 percent of small-business owners believe their company is not at risk for cyber-threats such as viruses, malware, hackers or a cybersecurity breach. This figure is quite alarming.

[1] Fanelli, B. The State Of Cybersecurity among Small Businesses in North America. https://www.bbb.org/globalassets/shared/media/state-of-cybersecurity/cybersecurity-research-report.pdf.
[2] https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf
[3] https://www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize- businesses.html

Small Business – Understanding Cyber Risk

Every successful small business owes their success to their ability to understand the risks inherent in their perspective industries. Cybersecurity starts with understanding and managing potential dangers. The unfortunate reality is that many small businesses do not identify these threats until they experience some level of disruption.

The level of risk for being a target of cyber-crime is high, 42 percent of small businesses surveyed by the National Small Business Association (NSBA) reported being a victim of a cyber- attack, with cyber-attacks cost an average $32,021 for companies whose business banking accounts were hacked, and $7,115 on average for small businesses overall.[4] NSBA members who were victims of credit card theft, 13 percent of the attacks the company's entire network was compromised and in 10 percent there banking accounts were breached. 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.

Since total elimination of threats is impossible, protecting against them without disrupting business innovation and growth should be a top management priority. Unfortunately, many small businesses are still not placing cyber-threats within their top priorities for business survival. Growing revenue, increasing profit, managing cash flow and attracting and retaining qualified employees are the top challenges identified by the respondents overall. The Better Business Bureau conducted a survey where only 20 percent of respondents identified cyber-threats, including lack of data security, as a top challenge for growth and survival.[5]

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%

Small Business Operational Perspective

The NSBA 2015 Year-End Economic Report demonstrates that in a technologically advanced economy, network vulnerabilities and the lack of a comprehensive cybersecurity policy can completely disrupt business. Due to the cyber-attacks, almost half of the affected businesses experienced an interruption of service.

[4] 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.
[5] Id. The State of Cybersecurity at 17

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%

The above graph shows the difficulty that small business confronts when resolving a cyber-attack, 34 percent of attacks persisted for up to three days, with 41 percent taking three days are more to resolve. This is an incredible burden on an organization of any size, but when factoring in that these our small businesses with limited financial and technological resources, the problem becomes compounded. Only 14 percent of small business rate their ability to mitigate cyber risk and vulnerabilities as effective. That is an unfortunate reality when factoring that 60 percent of small companies go out of business within six months of a cyber-attack.[6]

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 must 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 with 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.

As a result, small businesses must become more efficient in their utilization of cybersecurity methods that are designed to help mitigate the potential risk of cyberattacks. The statistics show that there is a sufficient amount of work to be done on part of small companies and their operational strategies. Sixty-five percent of small businesses reported that they do not strictly enforce their password policy, this is the largest gateway for potential breaches. It is imperative that we, as small-business owners, fully enforce the most intrusive method of sabotaging our networks, and therefore our business.

[6] Cyber Security Statistics – Numbers Small Businesses Need to Know
Matt Mansfield - https://smallbiztrends.com/2017/01/cyber-security-statistics-small-business.html

One of the most popular responses on why small businesses do not allocate financial resources to threat mitigation is that they feel they do not store any valuable data. This is a misconception on what constitutes valuable data – email, phone numbers, billing addresses may be viewed as not valuable information to the small business, but to a cyber-criminal, these are very valuable and effective data points that can be used for malicious purposes. Although, small-business owners are becoming increasingly tech savvy, limited resources and knowledge still leave many vulnerable to cyber-threats.

Transfer of Risk - Cyber Insurance

There are several reasons why small businesses should consider cyber insurance. First, insurance provides the small business to place a value on their current level of cyber risk. This allows business owners who may not be technically versed in cyber-attacks and the threats they pose, to quantify the potential cyber incidents.

Before purchasing SureFire Innovations cyber-liability insurance policy, I was like the vast majority of small-business owners, I felt as though, my company was too small to be targeted, the cost of another insurance policy was not within my operating budget, and did not know the actual value of having a policy. This was my thought process before a fellow business owner was the victim of a cyber-attack.

As with most cyber-attacks, his company was a victim of a phishing email attack, in which the hacker targeted an employee with a seemingly innocent password reset email. This allowed the hacker to gain access to their Amazon Web Services account and steal all the data and then delete everything from their account. This had a severe impact on their company, as within one year's time, they were out of business.

In 2016, I made the decision to evaluate my entire network and cybersecurity methods and make an honest assessment of what our vulnerabilities were and how to effectively mitigate them. The first step was to see what the daily cost and earnings that would be lost if my company was to be a target and shut down for several days. This was a simple formula: daily payroll, daily sales, and the cost to notify any individuals whose sensitive information is stored on my network. The formula I used was an annual sales divided by the amount of business days, which gave me $3,200 in effective lost daily earnings due to a potential cyber-attack. Taking this initial step allowed me to start building dollar amounts associated with any potential cyber-related incident and help me understand the need for a cyber insurance policy.

Second, the process of applying for a cyber liability policy forces you to acknowledge and address the potential vulnerabilities on your company, this is an assessment most small businesses have never taken. The application process made me account for several items that were not in existence for my company's operations. For example, we did not have a cybersecurity policy, this was a sober awakening, as the sheer amount of resources to assist small businesses in building this critical document could not be more plentiful. My company utilized the Federal Communication Commission's (FCC) Cyberplanner to help with the initial building of our cybersecurity policy. I came across the FCC resource, by conducting a simple web search seeking assistance in drafting a cybersecurity policy. This helped me to understand where there were weaknesses and areas that needed to be reinforced in my daily operations. Simple

measures, such as encrypting data, complex passwords, and having a firewall was explained in detail on their necessity. The Cyberplanner serves merely as a guide for companies—such as mine—that currently do not have a policy in place and may be uncertain as to what action steps to implement. This document helped provide a path for me to begin addressing sound cybersecurity protocols needed for my company.

Third, if the small business does experience a cyber-attack, certain policies include incident response assistance. This can be of great value for companies that are uncertain on how to appropriately respond in these dire circumstances. Smaller companies may not have the experience or the manpower to respond to the type of issues that may arise out of a security breach: reputational damage or any type of regulatory concerns. This adds immense value to the policy overall, as it allows the small-business owner to have guidance through an immensely complex and difficult situation.

Policy Selection

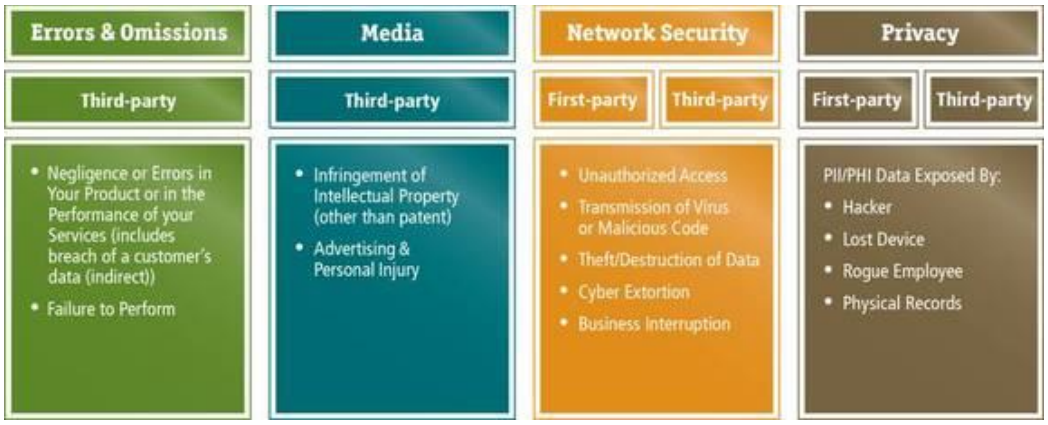
When I reached the decision to purchase a cyber liability policy to help transfer risk, it was an incredibly challenging situation. I was uncertain as to what constituted a good policy and the levels of protection that were needed. It was my assumption that my current insurance agent would have the intimate details of potential polices thoroughly digested, this was not the case. In fact, from the time he introduced the policy to me, it was clear that he was unfamiliar with the underwriting process of cyber policies. As I was completely unfamiliar with the process, my solution was to work with the current agent and wait for him to gather the information and address my questions and concerns. In the end, this process took more than a month, when an experienced agent could have better advised me on the nuances of the plans, in a shorter amount of time.

There were two policies proposals offered: one with an annual premium of $1,800 and another with an annual premium of $3,200. After reviewing the two different policies, it was my interpretation that there was one main feature difference: the $3,200 policy included Technology Errors and Omissions. This was justification enough for me to move forward, as this provides coverage for claims that arise from the failure to perform your business activities for a client to the required standard. Being in the technology industry, standards can change rapidly and having this line of coverage felt necessary and appropriate for SureFire Innovations.

When I look back at my decision-making process, there are several areas that I would have reconsidered had I been more informed and knowledgeable, at the time. Starting with finding a well-informed agent that had experience and expertise in the field of cyber liability policies. I made the mistake assuming that my agent, who issues my other insurance coverages, would also understand cyber liability. This was not an accurate judgement, and it would have been a smoother process if I would identified an experienced cyber insurance agent to help address my coverage needs.

In my opinion and from my experience, it is highly important that a small-business owner, when selecting an agent for their cybersecurity policies, stay within the sphere of knowledgeable cybersecurity agents, as they will be able to better assist with identifying the appropriate policy for the level of coverage required per the business.

Garnering my cyber liability policy was not the smoothest process, but at the end of the day, I did acquire a policy that does suit my company's requirements. There is a variance of policies to choose, but small businesses can expect their cyber coverage in some combination of four components: Errors and omissions, media liability, network security and privacy.[7]



An important coverage element that should always be considered, which was not considered during my initial purchase, is retroactivity coverage. Many cyber policies limit coverage to breaches that occur after a specified "retroactive date." In some, this date is the same as the policy's inception date. This means there may be no coverage provided for claims made due to breaches that occurred before the policy period, even if the insured did not know about the breach when it bought the policy. Because breaches may go undiscovered for some time before claims are made, insured should always ask for a retroactive date that is earlier than the inception date. This will ensure that the coverage includes unknown breaches that first occur prior to the policy's inception, but do not manifest themselves until after that date. Insurers do not always offer retroactive coverage unless asked, but it is commonly available for periods of one, two, five or ten years. Some offer unlimited retroactive coverage.[8] Before finalizing my policy, I attended a small business cybersecurity symposium where it was suggested that before purchasing a cyber policy, request that retroactivity be included. That simple request allowed my policy to include one year retroactivity at no additional premium increase.

Conclusion

When I started my company, I was unsure of many of the challenges that would happen to a small-business owner and the need for sound, quick, and effective decision making. SureFire Innovations has had the opportunity to build a strong reputation in the technological space and work with large commercial enterprises as our customer base.

[7] Cyber Insurance 101: The Basics of Cyber Coverage I Wooodruff-Sawyer
https://wsandco.com/cyber-liability/cyber-basics/
[8] Top 10 Recommendations for Negotiating Your Cyber Insurance Policy
https://www.pillsburylaw.com/en/news-and-insights/don-t-wait-until-it-s-too-late-top-10-recommendations-for.html

Our customers have afforded us the opportunity to provide network services across the country and provides us a platform for growth. This has been incredibly difficult, but the rewards of building and managing a young company that is growing far outweigh the challenges. Which is why the area of cybersecurity and small business effectively mitigating and transferring risk is so important to me.

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. I have personally witnessed a company taken out of business at no fault of their business operations, employees, or completion, but rather an individual lurking on the internet with the intent to destroy an entire company and the opportunities it provides to its employees.

In fact, according to NSBA data, ninety-four percent of small-business owners are concerned about being targeted by cyber-attacks. The potential for loss from a singular cyber incident to a small business can completely neutralize its ability to compete in the marketplace. Additionally, 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. Not to mention that a highly public breach could also damage the business's brand and lead to long-term loss of income. The ripple effect that this issue can have on the overall economy is staggering.

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 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.

Robert Luft
SureFire Innovations
President

Robert Luft is the Owner, President of SureFire Innovations, a Service Disabled Veteran Owned Small Business (SDVOSB) and Minority Business Enterprise (MBE) based in Cincinnati, Ohio that designs and installs wired and wireless, security, and smart city networks.

Robert started SureFire Innovations after serving in the Army for sixteen years, which included multiple combat deployments to Iraq as a combat engineer conducting route clearance operations to defeat the Improvised Explosive Device (IED) threats. Robert has a Bachelors in Marketing with a minor in Public Relations. These experiences provide the requisite leadership skills that would transfer over to the civilian sector as an entrepreneur.

After his military service, Robert devoted himself to entrepreneurship and founded SureFire Innovations. The company's focus is in the technology sector, specifically network infrastructure. SureFire Innovations has been able to service large-scale enterprises on their infrastructure requirements through an emphasis on employee development, training, and immersion in the latest technological advancements in the industry.

Robert serves on the National Small Business Association (NSBA) Leadership, Economic, and Technology councils. He also serves on the Board of TechDefenders, an organization whose mission is to offer technology training to underprivileged students in the Cincinnati area.

As a proud veteran, Robert's passion for the veteran community is evident by his involvement with the Disabled Americans Veterans (DAV) and United Service Organization (USO).