U.S. Senate Committee for Small Business & Entrepreneurship

"Cybersecurity" Hearing April 25th, 2018

Testimony:
Ben Toews
President
Bullet Tools - Hayden, ID

Thank you Chairman Risch, Ranking Member Cardin and distinguished Senators for the opportunity to share this testimony with you.

I'd like to start by explaining what specifically qualifies a small business owner/operator like myself to speak on this subject. My degree is in International Business, not Information Technology. Managing the techy side of my business was a necessary evil during the early days of my company but I learned a lot. I created our business network, figured out how to get everyone connected and did my share of troubleshooting and training people to use and protect their computers. As soon as I found people who were capable, experienced and undoubtedly more passionate about IT then I was, I handed over the reins and never looked back.

Not that I don't recognize the importance and benefit of the amazing organization, information processing, communication and collaboration that technology allows, I really do appreciate it and leverage it. My business spends roughly the same amount on IT related purchases as we do on R&D which is the lifeblood of our business. That doesn't mean that I love the nitty gritty details of how it all works. I'm guessing a lot of you are like me.

So, what qualifies me now that you know that I am not a computer genius, a hacker or a cyber security specialist? In short -- having my business hacked with ransom ware and surviving it on June 4th of last year. Let's look at our company as a sort of case study by analyzing our security measures before and after the attack along with how we recovered with relatively little damage.

Security plan BEFORE the attack:

Our first line of defense was a hardware firewall which is very secure but, to make our VOIP phones work we had to open numerous ports which acted as open doors. Our second line of defense was a domain controller with centrally administrated user names and passwords. The third line of defense was Microsoft Security Essentials on each desktop although it was not updated regularly. This is known to be ~90% secure if up-to-date. Our fourth line of defense was informal training of users of good internet and e-mail practices (don't respond to Nigerian princes who request bank account information no matter how much money they are offering you, or send wire transfers overseas without a verbal okay). Our fifth and final line of defense was to back-up our Financial/Inventory data offsite on a daily basis.

Friday before the attack:

We set-up a new computer without any antivirus software (no security guard), Set-up new user with no password (unlocked door), a brand new non-updated version of windows 7 pro (blinking arrow pointing to entrance) and plugged it into our network (an illuminated path to the unlocked safe).

What happened (as near as we can tell)

The non-updated version of Windows was viewable as a potential vulnerability. Once they had our IP address they could tell we had a remote desktop activated. They likely used a brute force user name attack to find out if any users had no password protection then used the user without a password to execute a piece of ransom ware on our server which encrypted every file that the user had access to and placed a ransom note in every folder the user had access to. We discovered this on Monday morning.

Recovery

We discovered we had been attacked and 1st had everyone turn off computers and unplug from network We had to analyze what had happened to determine how widespread and ongoing the issue was. After seeing the ransom note we used our cell phone browsers to find reputable online security companies with utilities that could identify and possibly help us restore our system. We cautiously booted one system at a time and searched for encrypted files and found that only our shared network folders and the files on the remote desktop account of one user were encrypted.

As each system was booted we installed Malwarebytes and ran a full scan where we discovered that the new computer had over 300 malware/virus files. Everything else was mostly clean. Computers using outlook often had some slight issues. We deleted the user, backed up the infected files on a separate hard drive and deleted from networked folders, updated windows on the new computer and all others then restored financial/inventory back-ups to the network. The majority of our company was back running as usual in 3-4 hours. Without the off-site backup we would have been in a really tough position.

The data we lost on our shared network folders was 80% older files which was kind of like having your storage unit destroyed that had been accumulating junk for 10+ years. You lose some valuable items but also a lot of junk that made it hard to find what was important anyway!

In process security measures:

We are in the process of creating a dedicated network for our VOIP phones (outside the firewall) and have a policy change to NEVER create a user without immediately creating a password and have also set-up a VPN to connect offsite to remote desktops. We perform updates on systems and anti-virus regularly on all computers and we are formalizing our communication on IT issues with users. Finally, we now have offsite back-ups of all shared folders on a nightly basis.

Lessons Learned

I've found in my life that learning from others' mistakes is a lot less painful then making the mistakes yourself. That is why I'm here today, to encourage you to help small businesses learn from my, and others, experiences to avoid going through it with their company.

There's a saying that "what we learn most from history is that we learn very little from history," let's try anyway by looking at a WWII example that works quite well as an example of the psychology behind the relaxed approach many small businesses have taken in relation to cyber-security:

In the years running up to the beginning of the second world war the British government was extremely concerned that in the event of hostilities breaking out, the German Luftwaffe would launch significant

attacks against Britain and especially London. With an estimated 250,000 casualties in the first week alone, the consensus was that millions of Londoners would flee, leaving the industrial war engine to grind to a halt. Several psychiatric hospitals were even set up on the outskirts of London to handle the huge numbers of casualties psychologically affected by the bombing.
History shows us that the psychological results expected never materialized, despite horrific numbers of casualties and extensive damage to homes, property and businesses throughout London.

A Canadian psychiatrist, J. T. MacCurdy, in his book *The Structure of Morale* postulated this was because the effect of a bomb falling on a population splits them into three groups:

1. The people killed by the bomb. As MacCurdy puts it, “the morale of the community depends on the reaction of the survivors, so from that point of view, the killed do not matter.” Put this way the fact is obvious, corpses do not run about spreading panic.

Harsh, but true in this model.

2. The Near Misses. The ones that feel the blast, see the destruction but survive, deeply impressed. It may result in ‘shock’ and a preoccupation with the horrors witnessed.

3. The Remote Misses. These are the people who hear the sirens and the explosions, watch the aircraft overhead, but the bombs explode down the street. For them the experience of the bombing is that they survived easily, unlike the Near Miss group. The emotional result of the attack is a feeling of excitement with a flavor of invulnerability.

Near miss = trauma, remote miss = invulnerability.

Diaries and recollections of the period certainly support these theories. For instance, when a laborer was asked if he wanted to be evacuated to the countryside (after being bombed out of his house twice) he replied; “What, and miss all this? Not for all the tea in China!”

The reason for this attitude, the sense of invulnerability, is that they have been through the very worst of time - and survived. They had faced their fears, and realized they were not as bad as they thought they were going to be, and, in fact, the result of surviving had given them a sense of elation that made them feel even more alive than before.

On the subject at hand we can categorize all small business owners into these three categories: Those that have been hacked but didn't survive (direct hits). Those that have been hacked and survived (near misses), and those that have never been hacked (remote misses, - unhacked, by luck or precaution).

Now it probably goes without saying why the 1st category, those that get hacked and don't survive, aren't likely to be going around advertising it and probably have enough trauma from the event to produce a strong desire to forget it ever happened. They are also likely embarrassed by what happened and would prefer to keep it to themselves. This category of small business owner, we'll call them "Hacked to death," are probably busy starting a new business or working for someone else, leaving them with little free time to talk about what they are trying to forget anyway.

The second category is likely more prepared then many of those in the first and, unless it happened quite recently, have probably set up a very secure computer system at their companies that are safely backed up behind a hardware firewall….. or have abandoned using computers altogether in favor of pencil and paper along with their trusty fax machines, these business owners sporting their flip phones and calculators are willing to give up the productivity of computers for the safety of the tried and true - not likely a recipe for long term success.

The last category is the “remote miss” group. They've heard about companies being hacked on the news but nothing has hit anyone close enough to get their attention. They probably believe they are too small to be a target, have sufficient security in place or are just unlikely to be attacked. This group is who we are most likely trying to get information to, but like the Londoners of WWII there is a feeling of invulnerability that comes from hearing about what has happened to others that hasn't happened to them. Let's face it, if many of the largest companies on the planet along with some of the most sophisticated countries can get hacked so can they. Granted they are big targets and small business might not be but the cyber criminals are starting to realize that small, vulnerable, easy targets can be very lucrative.

For small businesses that are part of the lucky group that haven't yet been attacked or compromised this is a great time to realize the fact that they aren't immune to cybercrime, attacks are becoming more likely and frequent, not less, and the threat isn't going to go away so now is a great time to focus on understanding, analyzing and investing in the necessary precautions to keep themselves protected.

Recommendations:

Knowing the psychology of those that have not yet been directly impacted by cybercrime is useful in formulating a strategy to help them. They need to be informed that they are a target and that increasingly small businesses are being successfully attacked. Spreading the word about this reality is critical to getting their attention. Once they are convinced there is a significant threat they need to be educated on how to protect themselves. You already have great resources available to small businesses and I would recommend finding ways to actively spread the word and further leverage them.

The Idaho SBDC helped our business write its initial business plan, obtain its initial funding and weather the storms of growing a small business over the last 18 years numerous times through coaching and classes. I now sit on the advisory board of the Idaho SBDC. I see how the SBDC has started responding already. The SBDC already has good resources in place to help prevent or mitigate the devastating effects of cyberattacks including a vulnerability assessment and other tools. They also run a listserve that shares best practices with other SBDCs nationwide. However, SBDC need to be empowered to fully develop these resources and help actively promote them to small business.
These resources need to be not just further developed but actively promoted to the small business community. This could be done through public service type announcements that could be sent through various social media platforms targeting small businesses. Federal agencies also need to be encouraged to collaborate with SBDCs and promote them as a resource. There are nearly 1,000 SBDC locations, the SBDCs are the “boots on the ground” coaches across the country who can educate those at risk and help those dealing with a cyber-attack on their business.

I would also recommend encouraging cybersecurity training programs and developing common resources for SBDCs to use to aid and inform small business. The Department of Homeland Security and the other federal agencies have a lot of resources and knowledge but that knowledge is hard for small businesses to find and use. I am encouraged that SBDCs and those agencies are already working on this effort due to language this committee supported in the 2017 Defense bill.

There is also a need to establish standardized, reputable certifications for cybersecurity professionals along with a way for small businesses to confirm the credentials of cybersecurity providers. When dealing with I.T. issues many small business owners are wary since it is hard to know what exactly the people you hire are doing and it is difficult to know if they should be trusted with your information.

This results in businesses often choosing not to do anything since it is both costly and seemingly risky to hire someone. Thankfully, SBDCs are already involved with the IT community to identify qualified providers but more remains to be done.

I hope that my testimony will help make a difference in combatting cyberattacks and it has been an honor speaking with you today.