Five Things You May Not Know About Cybersecurity in the (Truly) Small Business

Some considerations for small businesses and those who work with them

William Yurek, President, Inspired Hacking Solutions, LLC

The cyber threat to small businesses is well known and well documented, at least within cybersecurity circles. The National Cyber Security Alliance found that almost 50 percent of small businesses have experienced a cyber attack, and more than 70 percent of attacks target small businesses. I could go on and on with the stats, but they're easy enough to find, and frankly you likely wouldn't still be reading this if you didn't already have at least some idea of the threat to **small businesses.**

Small businesses account for 58% of cyber compromises

Verizon DBIR Report, 2018

But What is a Small Business, Really?

When it comes to this question, most people turn to the US Small Business Administration (SBA). After all, if anyone would know it's them, right? But it's not that simple. The SBA definition can vary based on industry, average annual revenues and number of employees. In short, a business must make between or below $750,000 and $35.5 million, and have between or below 100 and 1,500 employees, depending on the industry, to be a "small business." Not exactly a discrete reference point.

What I'm focusing on in this article is not the SB (small business), but the TSB (truly small business). Call them what you will: family business, mom and pop, startup, microbusiness, whatever. The Census Bureau's 2016 Survey of Entrepreneurs found that companies with less than 20 workers made up 98% of the 5.6 million employers in the United States. These TSBs are the companies with which I've most often consulted, and they make up a tremendously underserved segment in terms of cybersecurity support.[1]

[1] In my experience, it's not economically viable for cybersecurity companies to identify, pitch, and service TSBs due to the relatively small return on investment.

What follows are some observations I’ve made after consultations with about 35 companies.[2] Please understand that this article is not meant as some sort of “dig” at small businesses. It’s merely observations. My goal is twofold: 1) encourage the TSBs that may be reading to think about cybersecurity now, rather than when it’s too late, and 2) help larger, more established and (hopefully) more secure businesses make knowledgeable decisions when considering partnering with, acquiring, or otherwise doing business with, TSBs.

Cybersecurity Starts out Low on the Priorities List, if It’s There at All

The average TSB starts out just trying to get that elusive first contract on the books or the first customer through the door. This comes before any thoughts of IT infrastructure, security, or anything else.[3] The usual start is two people with two laptops and two cell phones. Once they get that first contract that keeps the lights on, they are after the next one, the one that will feed their families. Then on to the one that might actually let them draw a salary. For those businesses that succeed, growth kind of sneaks up on them. One day they look up and they’ve got a slate of clients and bunch of data spread between several laptops, phones, iCloud, DropBox, etc. They may start thinking about cybersecurity now, but usually they don’t act on it because….

They Don’t Think it Will Happen to Them (or they Don’t Care if it Does)

When and if cybersecurity does cross the mind of a TSB, few of them think they are really at risk. The reasons I’ve heard for this include:

- They don’t think anyone would want their data. Most TSBs don’t handle what would be considered sensitive information. Think of businesses such as jewelry-makers, auto mechanics, beauty salons, yard services, etc. These companies don’t see it as too big a deal if they get hacked. The auto mechanic figures nobody is going to want to know when Mr. Jones had his brakes replaced. The jewelry maker figures nobody will care if Ms. Wilkins bought a garnet broach. For those companies, explaining things such as resource theft, ransomware, and botnets gets their attention. I then go into topics such as hacker use or sale of data, use

[2] These companies ranged from 1 to 35 employees. Most had under 10 employees.

[3] Notable exceptions are the regulated services companies, such as accountants and nurses, where laws such as HIPAA demand a certain level of security and licenses may depend on compliance.

of data for phishing, risk to upstream and downstream clients, partners or customers and, finally, the risk all of those things pose to corporate reputation.

> ***“Many business leaders assume that if they have a firewall, they have a padlock on the door and no one can get in.”***
>
> Chad Paalman, CEO of NuWave Technology Partners

- They Trust in Antivirus, Firewalls and ISPs. The devices TSBs buy usually come with a free trial of one of the well-known antivirus / antimalware programs. Unfortunately, most don’t keep the programs updated, and those who do don’t actually configure the software to maximize protection. These companies also become more vulnerable to fake malware “updates” precisely because they don’t understand how updating works. Almost all TSBs I spoke to said firewalls were important, and put substantial faith in them.[4] A few TSBs believed that their ISP monitored traffic for malware, so they were protected already.

- They Figure It’s Probably Going to Happen No Matter What. We’ve all heard, and many of us have repeated, a mantra that goes along the lines of “there’s two kinds of companies, those who have been hacked and those who will be hacked.” Meant to encourage companies to protect themselves, that mantra can have a perverse / inverse effect. A TSB, naïve in the world of cybersecurity, will often view this as an excuse to just press on and get as much done as they can before they are hacked. Why put energy and money into security when they will get hacked anyway? When coupled with the common belief that they’re not worth hacking or have nothing valuable to lose, this position is a recipe for disaster.

They save EVERYTHING

In general, data storage is cheaper now than it’s been in ages, driven mostly by easy access to online storage services. Most TSBs start out relying on the free storage they are given by Apple, Google, DropBox, or a host of other providers. As a result, it’s possible for even small companies to store tremendous quantities of information. TSBs

[4] The firewalls relied upon were almost always those that were included with operating system or software packages, not firewall devices or software purchased separately. Ironically, many small business employees turn off the built-in firewall on their devices, mostly because they felt it made other programs harder to use. Usually this belief was unfounded, or came from the TSB not taking the time to configure their firewall to avoid software conflicts and other common firewall issues.

tend to save every bit of information they've ever received or generated. Aside from the relatively low expense, several other reasons come into play:

- They don't have a document archival or destruction plan
- They are afraid a client will one day ask for something and they want to have it on hand
- They think it may one day be valuable for something use down the road
- Statutory, contractual, or regulatory requirements may require extended storage and availability
- If the company has backups (many don't), they effectively double their storage need

This collection of data leads to several issues of concern for the cybersecurity professional. First, seemingly diverse databases can, when combined by a hacker, become sensitive information. Second, the more data that is stored, the more data that can be compromised. Would you rather have your 10 current clients compromised, or the current 10 plus those you've had over the last 5 years? Third, the use of cloud storage necessarily creates a need for encryption protection during data transmission, which most TSBs have never even thought about. On a related note, one of the simplest steps that can be taken to protect the mass amounts of data that can be stored on a device is at-rest encryption, and you would be surprised how few businesses, whether small, medium, or large, actually use that feature, even when it's a built in part of the operating system and is free to use.

The Wake-Up Call Causes Frenzy

The one thing that usually shakes a TSB out of complacency is the first compromise, even if it's as simple as a virus infection that doesn't cause much damage because that free antivirus program they downloaded actually found and cleaned it. The initial response is one of frenzy. The CEO calls his "cousin who used to build computers," the sales guy's wife is a programmer so he calls her. And so on. The most common ending to this frenzy is 1) the purchase of some pretty blinking device that a vendor told them will solve their problems, and 2) the hiring of the cheapest security "expert" they can find to fix things. The former usually is a waste of money, because the TSB doesn't really know how to make the device work for them, and it's really not a solution, anyway. The latter may help, if they get lucky in who they find.

It's Difficult to Fix the Plane When It's In the Air

If I'm advising a TSB at this point, I usually have an attentive audience, but I'm now trying to fix things while the business is recovering and also still trying to generate revenue. Like many businesses, TSBs don't want to step back and create policies, plans and procedures to guide their next steps. They don't want to do assessments. They want to dive into buying whatever it takes to make them feel safe. Like many businesses of every size and shape, believe that cybersecurity is about networks, firewalls, and passwords, when it is really about people. Because they've been stung already, I usually have little issue convincing them of the need for an Incident Response Plan (IRP). But they almost never want to start with overall cybersecurity policies or plans, so the IRP isn't nearly as useful as it could or should be. It usually ends up being an adaptation of lessons learned from the compromise that prompted them to action, which is fine if the exact same compromise happens in the same way the next time. Better than nothing, but not by much.

I've found that it takes a TSB several months or more after their compromise[5] to be willing to listen to the need for policies and plans about backups, encryption, authentication, social media, email, remote computing, and a host of other necessary "formalities." Even then, the human factor is a complication. Most TSBs begin with a family team, a group of close friends, or a combination thereof as their employees. There's often no clear boss, and even if there is getting him/her to lay down the law in terms of policies governing employee behavior is difficult. Tom doesn't want to tell his college buddy Jeff that Jeff can't go to gambling sites on the work computer. Jill doesn't want to tell her father that he can't use his personal laptop for work, even though it's insecure and obsolete.

When I talk to TSBs about policies, I tell them that if they aren't going to enforce a policy, they should change it to one they will enforce, or just don't have it at all. A policy not enforced is, in my opinion, worse than one that doesn't exist. Policies are the primary way of binding employees to the company. If a company can't, or won't, train and guide its employees, nothing anyone outside the company does is going to make them secure.

Conclusion: It's not a Slam

[5] Assuming their business survived the compromise.

Again, it’s not my goal here to portray TSBs in a negative light. Heck, I am a TSB. It’s a tough route to create and build a business, and cybersecurity can be a daunting task even for an established business.

If you’re a small business and are reading this, do you see yourself anywhere? If so, take some steps now to get your cyber house in order. The key is to get started. Even a few small, simple steps up front can dramatically improve your security posture.

If you’re a more established and/or larger business, are you looking to work with, or acquire a small business? If so, take a minute to assess their cybersecurity posture. If it doesn’t meet your needs, maybe you can help them do so, or just don’t work with them. But Mr. Pot, be careful before you call Mr. Kettle black. There are plenty of large businesses out there with poor cybersecurity. Even if you’re not a small business, does anything you’ve read here ring a bell with you? If so, maybe it’s time for you to act.

98% of companies in this country fall into the category that is known to be the most vulnerable to computer attacks and compromise. Yet it is also the most underserved segment of the corporate community. Companies that want to do business in this environment need to go into it with their eyes open as to its inherent risks.