Cybersecurity for Small Business: It Doesn't Keep You Up at Night? It Should!

If you want a pleasant Sunday morning read, check out this list of data breaches of major companies, organizations and government agencies. These are entities with IT departments, security professionals monitoring their networks, cybersecurity policies, and a budget to support their cybersecurity efforts. At least one of these data breaches included data about you. And, these cyberattacks were not even the primary targets of most attacks in the world. Hackers today find it lucrative to target businesses and, more specifically, North America-based small businesses.

Hackers have breached about 14 million small businesses in the last year, and most don't know it. Cybersecurity for Small Business might sound obscure if you're in business on "Main Street" and don't sell online. However, it's one of the most important management areas of your business to focus on today. Cybersecurity itself means protecting your digital world from attacks in a variety of forms so you can focus on running and growing your business.

Unfortunately, gone are the days when you can buy antivirus software for your desktop computer and all your digital worries can go away; it's part of the solution but it's not the whole solution. There are many ways in which hackers can penetrate your personal, your business, your employees, and your customers' machines and access data with intent to steal or get access to that equipment for nefarious reasons. Frequently, the reasoning doesn't make sense on the surface so you aren't suspicious, and this can be the most dangerous cybersecurity breaches because you are unaware for so long.

I'll use the colloquial term "cybercrime" throughout this discussion to cover the wide variety of crimes, unethical tactics, and downright immoral practices of individuals and companies against personal and business systems and their data. These cybercrimes include, but are not limited to,

- hacking your digital devices (which could be your smartphone, computers and laptops, Point of Sale terminals, credit card machines, and similar devices),
- hacking your digital services (think about your website, email, cloud storage, and online services),
- blatant physical theft (ergo, larceny) of digital equipment to get the underlying data,
- data theft,
- phishing,
- stalking,
- identity theft,
- wire tapping,
- denial of service (DoS) and distributed denial of service (DDoS) attacks against your servers to shut down your websites,
- email bombing (the equivalent of a DoS/DDoS attack, but with a volume of email messages sent to you instead of HTTP requests to the server), and
- injection of malware (malicious software), ransomware (taking data to make you pay to gain get it back), and other types of software that do dubious actions to your digital environment.

Now isn't this a Charlie Foxtrot, eh? I know it's daunting and it might scare and overwhelm you. It's understandable that you may feel this way. But, as a business owner in the Internet Age, you must head cybercrime off at the pass, or risk losing time, money, and clients. Thankfully, there are some common sense ways to deal with cybercrime, so you can rest at ease knowing your digital world is safe and get back to running your business.

Physical security of hardware

Every Small Business should have physical security protocols for all digital devices (phones, external hard drives, computers should be secured in place so they cannot be easily picked up and run away with, laptops / tablets / credit card readers should be secured in locked storage when not in use.

Your next best defense since people are fallible, is to have an offsite backup. This can include making a full copy of your encrypted data on an external hard drive and taking it someplace away from the business location, and/or using a cloud storage backup service such as Carbonite, Crashplan, or even Google Backup and Sync.

Something that some businesses are starting to do as well, when all else fails, is to make sure their business liability insurance cover physical theft. And, you should know that there are cyber security risk / liability insurance policies available for damages and losses from digital means.

Physical access to systems (users)

When it comes to physical access to systems, your users should be guided by an effective Digital Device Policy and include protocols for:

- How to create employee user accounts and assign only the administrative/user privileges needed for them to perform in their role.
- Give users physical access to systems only at the times needed to satisfy their assignments, and not give access to unnecessary systems at all. If employees don't need access to your server room, don't give it to them.
- For how to allow Bring Your Own Device (BYOD) employees at your business. You should have in place a policy for managing BYOD's. Employees must use and abide by these security protocols on their mobile devices, if they use personal devices at work.

Separation of personal and business devices

You separate your business and personal finances, because you need to track what is yours and what is your business', even if only for tax purposes. The same goes with cybersecurity. You need separate personal and business logins for online accounts. This may also include hardware, like the phone you use to make and receive personal or work calls. Will your ISP or telecommunications provider have protections in place if you're using your consumer service for business purposes? Probably not. The fine print matters here.

Software protections

Since the late 1990s there has been antivirus and anti-spyware software. And, yet, business owners resist installing reputable antivirus software on their business machines. While some have costs associated with them, many are free and built into your operating system, such as Windows Defender. You simply need to activate them. But, if you have purchased a license for one not built into your operating system, please make sure that your license is still valid and the

software are kept up-to-date (including your mobile phones and devices). Also, firewalls keep your computer, and any devices or routers connected to the Internet safer, especially your Web browsers (all of them, even if you don't use them all, all of the time), must have firewall protection. Again, on Microsoft Windows, there's Windows Firewall that simply needs to be enabled.

VPN when on WiFi on anyone else's network

If you spend much of your time on other people's WiFi, then you need to use a Virtual Private Network (VPN) to secure your business data trafficking across the network. This includes any open WiFi network at your local cafe and if you're working at a coworking space or even at your client's site. No network outside your firewall can be trusted to be secure. A VPN product you can try for 500MB per month for free is TunnelBear and if you use more data than that per month across your business, then you can upgrade.

Web browsing and email protections

As a business owner (and advising your staff similarly), don't open suspect emails and don't transact any personal or private information about yourself via email. Period.
At the core of most Web and email protection is antivirus and spam-filtering software, so it's definitely recommended that your ESP (email service provider) and/or ISP (Internet service provider) give you options for protecting and securing your Web and email traffic. However, that's simply not enough for a business today.

In addition to such protective software, you should also seek out information on implementing SPF, DKIM, and/or DMARC as available through your ESP.

It also doesn't hurt to enable two-factor authentication (a/k/a 2FA or TFA) on all online services that have the capability. Where possible, use a password manager, such as LastPass, 1Password, or Dashlane, to not only use unique passwords for every online account you have for the business, but also long passwords with unique passwords to increase its resilience to attacks.

Mobile security

As more and more computing happens on mobile devices, security on them will become the dominant concern for small business owners. But, mobile doesn't simply stop there. With the advent of Internet of Things (embedded "smart" technology in everyday things), wearable technologies, smart vehicle systems (Android Auto, anyone?), and voice assistants (like Amazon Echo devices, Google Home, and, the newcomer, Apple HomePod), cybersecurity needs expand to have to meet those new frontiers.

It’s so important for Small Business to have their representatives’ support when it comes to combatting cybercrime against them and their customers. In April, a bipartisan small business cybersecurity bill was introduced by nine senators—the MAIN STREET Cybersecurity Act of 2017. Sadly, this bill, according to Skopos Labs as detailed on GovTrack.us, has a 3% chance of becoming law. This is a commonsense piece of legislation to get the National Institute for Standards and Technology (NIST), “to disseminate resources to help reduce small business cybersecurity risks, and for other purposes.” Call your congressional representatives and tell them that you support S. 770 and they should support their small business voters by supporting this bill.

Also, if you’re scared senseless and you need help, never fear. Contact the Alexandria Small Business Development Center and we can refer you to professional security consultants who can help you.

Next Roundtable - August 15, 2017 - Sizing Up the Competition: How to Create a Competitive Advantage

Alexandria Small Business Development Center hosts a monthly Business Development Roundtable from January to November. We meet in our main conference at noon on the third Tuesday of the month, and you can bring a beverage or your lunch, for a different business marketing or management topic that’s pertinent to Alexandria Small Business. Join us on August 15, 2017 at noon, when we gather to discuss “Sizing Up the Competition: How to Create a Competitive Advantage.”

Comments/Notes

Educate yourself (NIST PDF,