Makaye InfoSec

2020

Top 10 Tactics To Strengthen Your Cybersecurity Posture

For Small and Midsize Businesses

Take command and control of your cybersecurity risk with commonsense cyber-hygiene strategies that every small and midsize business can – and should – implement to keep cybercriminals at bay.

"We're not a target, right?" *Wrong*. Small business vulnerabilities are attracting more cyber-attacks than ever.

If you're a small or midsize business (SMB) owner, you may think your organization is too little or unattractive for the most dangerous and sophisticated cyber-criminals to notice.

You are mistaken.

At one time, yes, most online attackers focused their attention on larger enterprises; but today, over half of malware attack victims are categorized as small businesses, according to the Verizon Data Breach Investigations Report (DBIR).[i] The emergence of easy-to-deploy attacks like ransomware have changed the calculus for cyber-criminals, making it low-cost and high-reward to specifically target SMBs over larger businesses.

"It's a real epidemic," says cybersecurity expert Daniel Tobok. "Twenty years ago, the big criminals were really only interested in government and bankers and banking associations, because they held a lot of meaty things that they could monetize quickly. But as those enterprises grew more educated and more secure, [SMBs] are one of the biggest attack vectors for cybercriminals and state-sponsored attacks, because smaller enterprises are not as mature when it comes to their security."[ii]

That's right: the situation has completely reversed, with small businesses now the *preferred* target. Instead of following the money, cybercriminals are targeting the low hanging fruit.

That means businesses like yours.

This may come as some surprise: data breaches and other cyber-attacks have been writ large in news headlines for years now, but the media tends to focus on the most spectacular security failures, like the now-infamous attacks on giants like Target, Home Depot, Yahoo!, Equifax, and more.

But despite their absence from the news, attacks on SMBs are indeed "epidemic" and can be devastating. Consider:

- Cyber-fraud set off a chain reaction of disaster, as one small business first lost $150,000, then lost a large investor, then suffered PR issues, and were forced to spend $$$ in recovery.
- Malware took another small firm's network down for a week, leading to huge revenue and productivity losses.
- Ransomware encrypted all systems at another SMB, which went down for two weeks – suffering major revenue losses – only to end up paying a $10,000 ransom.
- One SMB's CEO's Office 365 email account was hacked, with personal and business contacts compromised, leading to PR issues and potential legal action from affected clients/vendors.
- A virus attack took down another whole network, with $250,000 in outage fees to the state.
- Ransomware took a small healthcare provider down for two weeks, leading to fees and fines.
- Hackers broke into a firm and wired over a million dollars to accounts in Russia and China; unable to recover the lost funds, regulators shut the firm down just days after they reported the loss.
- Hackers added fake employees to one company's payroll, which ended up paying out tens of thousands of dollars before discovering the fraud.
- And the list goes on and on.

Now for the good news: SMBs can do *a lot* to significantly reduce their risk and exposure to potential cyber-attacks.

Even better, many of the most effective tactics are simple and straightforward. This paper will identify the 10 most important steps any SMB can take to protect itself against the kinds of attacks described above. Don't delay; after an attack is too late.

1 Maintain A Detailed Inventory of All Your Authorized IT Assets

This step is foundational to good security hygiene because organizations must have access to this information to understand their risk.

"To measure risk, you have to go beyond looking at what can go wrong and determine both the likelihood of something going wrong and how severe the consequences would be," writes Network Intelligence Analyst Angela Horneman for the Software Engineering Institute at Carnegie Mellon University. "This analysis requires knowing how [assets are] used to support enterprise operations."[iii]

With an always up-to-date inventory of IT assets, organizations can understand where and how all assets are being used and thus gain visibility into potential points of vulnerability.

Hardware Assets

The hardware inventory should include every IT device, regardless of whether it's connected to the organization's network or not. This includes computers, laptops, servers, peripherals, mobile devices, printers, copiers, etc. Implement a process that addresses unauthorized IT assets to ensure that they are blocked, quarantined, removed from the network, moved to a guest network, or added to the network (with the inventory updated immediately).

Software Assets

Maintain an up-to-date list of all authorized software on your firm's systems that is required for any business purpose. Ensure that only software currently supported and receiving vendor updates are added to the authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system. As with hardware assets, ensure that unauthorized software is either removed or added to the inventory system immediately.

Data Assets

Not all data is equal, and certain forms of data – private, privileged, or proprietary – must be protected to a degree beyond other forms. Federal and state regulations, for example, may mandate extensive protections for Personal Identifying Information. But how do you know which data needs which protections? Maintain an inventory of all sensitive information stored, processed, or transmitted by your organization's systems, including data stored both on-site and remotely via Cloud host.

2

Change Default Passwords on All IT Systems

The vast majority of cyberattacks are linked to compromised passwords; according to the 2019 Verizon Data Breach Investigations Report, 80% of hacking-related data breaches involve weak, compromised passwords.[iv] That should come as no surprise, as nearly half of companies (47%) never change the default passwords on their computing and IoT devices.[v]

That's extremely poor cybersecurity hygiene because default passwords tend to be simple – even as basic as *admin, user, 00000,* or *12345*. Even more intricate default passwords are still often just combinations of numbers that are easy to crack. Device makers tend to assume that owners will change the password immediately.

Before deploying any new IT asset, make sure your IT group changes all default passwords and provides evidence of the changes to management.

3

Encrypt All Laptops and Mobile Devices

The New York Times describes this step as "the one thing that protects a laptop after it's been stolen." Specifically, encryption prevents your data from being accessed by a criminal.[vi] It's important to understand that a password alone does not protect data because criminals can use other methods to extract the data from a stolen device.

Instead, the data itself must be protected directly.

"Encryption is a mathematical process used to jumble up data. If important files or whole devices are encrypted, there is no way to make sense of them without the key," Dennis Stewart, a security engineer at CipherTechs, told the *Times.*[vii]

Protect sensitive data and enforce privileges such that only authorized users have access to the data based on their need to use the data as part of their job responsibilities.

4

Use Dedicated Administrative Accounts

Most devices differentiate between "administrators" and "users," with administrative accounts having elevated privileges like the ability to install new software, change registry settings, alter configuration files, and more. In fact, many malware exploits *rely* on access to admin accounts and cannot successfully execute under restricted, regular user accounts.

Computer World even reports that as many as 94% of critical vulnerabilities reported by Microsoft can be mitigated by removing admin rights.[viii] Neil MacDonald, Vice President, Distinguished Analyst and Gartner Fellow Emeritus in Gartner Research, calls this "the single most important way to improve endpoint security."[ix]

Organizations can thus improve their security posture by removing administrator rights from users who do not need it and by giving admins dedicated administrative account access used *only* to perform administrative activities. Administrators themselves should use limited rights accounts for everyday activities like email, web browsing, and the like.

It's important to remember that this is not a cure-all – standard accounts can still be compromised in some cases, and many forms of attack do not rely on administrative rights – but it will significantly improve overall cybersecurity hygiene.

Turn On Audit Logging: Ensure that local logging has been enabled on all systems and networking devices.

5

Educate Your Team on Cybersecurity

Most sophisticated attacks target *people* rather than technology. Phishing schemes, for example, trick human users into executing programs or relaying sensitive information, thinking they're doing so for a legitimate purpose. That means that an unprepared workforce is the weakest link in your security. "You can have the most secure system in the world, but hackers will always seek out the path of least resistance. When your defenses are good, the weak link is often your employees," writes *CSO Online*, a publication of advisory firm IDG.[x]

Cybercriminals know this, and that's why phishing and similar social engineering attacks are on the rise and becoming more sophisticated. Thankfully, organizations can strengthen the "Human Firewall" with on-going training of their employees and by regularly testing them.

Train the workforce to:

1. Identify different forms of social engineering attacks, such as phishing, phone scams, and impersonation calls.
2. Identify and properly store, transfer, archive, and destroy sensitive information.
3. Be aware of causes for unintentional data exposures, such as losing their mobile devices or emailing the wrong person due to autocomplete in email.
4. Identify the most common indicators of an incident and be able to report incidents.

6 Implement Wireless Network Security Fundamentals

Your business should host two separate networks for connecting to the Internet: a Guest Network and a Private Network. Why? If clients and visitors, staff members' personal devices, Internet of Things (IoT) devices, and other smart devices (like smart TVs) connect to your Private Internet, they can potentially access private data, devices, and applications. With a Guest Network, you can isolate unknown, untrusted, or high-risk devices from your private Wi-Fi network. IoT devices in particular are notoriously insecure; and as long as they are accessing your Guest Network, even if they are compromised, they will not be able to offer hackers access to your primary network and its connected devices.

If appropriate, set up a new Guest Wi-Fi Network. Be sure to use strong wireless encryption standards (e.g., AES-256) to encrypt wireless data.

7 Lock Workstations After Inactivity

When we think of cybersecurity today, we mostly think of online attacks executed remotely by criminals far removed from our physical location. However, physically securing devices remains a mainstay of good security hygiene, and it's critical to remember that visitors or insiders with malicious intent can use insecure workstations to wreak havoc on an organization. In fact, Verizon's 2019 DBIR says insiders caused over a third (34%) of data breaches in 2018.[xi] One easy way to help mitigate this risk: set workstations to automatically lock after a standard period of inactivity.

Implement a Group policy to automate this feature.

8 Obtain Cyber Liability Insurance

Cyber-attacks are a risk against which no perfect protection exists. Activities like those outlined in this paper will dramatically reduce the risk, but nothing will set your cybersecurity risk to zero. But risk is why insurance exists, and most major insurers now offer Cyber Liability Insurance to their business customers. SMBs can cover their liability from a data breach in which customer data, such as Social Security or credit card numbers, are exposed or stolen by a hacker or other criminal who has gained access to the firm's electronic network. Such insurance can offset the costs involved with recovery after a breach or cyber-attack and make it more likely the firm will survive the incident.

Ask your insurer if they offer Cyber Liability Insurance.

9 Create and Test Weapons-Grade Backups

Good backups are an essential part of any recovery plan, but it's not necessarily enough just to have a second copy of data. That's why the cybersecurity world uses the term "weapons-grade backups." A weapons-grade backup equips the SMB with everything it needs to survive the incident. They're particularly critical in ransomware-type situations, where your data files may be locked or even destroyed by the cyber-criminal extorting your organization for money.

That means maintaining *both* onsite and offsite backups. Further, your IT team needs to verify that backups are actually happening (there's nothing worse than reaching for a backup to discover it's not there), *and* test them for accuracy and completeness.

Don't take IT's word; inspect what you expect! Backups are your last line of defense.

Create a well-defined backup policy, implement it, and add your backups strategy to your larger Business Disaster Plan.

10 Create and Test an Incident Response Plan

Because cyber incidents can prove fatal to SMBs – 60% of small businesses hit by a cyberattack go out of business within six months, likely due to the associated costs and reputational impacts – smaller organizations should treat security incidents as a matter of *when*, not *if*.[xii] That means developing a written Incident Response Plan that identifies key decision-makers and outlines procedures to follow during a security incident. It's also critical to assemble and maintain third-party contact information to be used to report a security incident. In other words, after an incident is detected, your organization will need to inform a variety of groups, including your IT vendor, any offsite data backup vendors, law enforcement, your bank (if financial transactions may be affected), and the U.S. Department of Justice Internet Crime Complaint Center (IC3). The Incident Response Plan should also be included in routine employee awareness activities.

TEST your Incident Response Plan! The worst time to test is during a disaster!!

Get Help

Comprehensive cybersecurity is a bigger job than most SMBs can handle on their own. Don't rely exclusively on your IT company, either: IT Managed Service Providers often face competing priorities that can detract from security effectiveness and may rely too much on piecemeal tools and apps. As a result, they can be excellent at IT and still falter at security. It's important for SMBs that don't have a cybersecurity company to engage one, even if on an ad hoc basis.

Strong security is only a few steps away.

If you take away only two key ideas from this paper, let it be these twin facts: First, your SMB is not as safe from cybercriminals as you would like to believe, and the consequences of an attack can be devastating – even fatal – to an SMB. Second, even a few simple and straightforward changes can *dramatically* reduce your risk of an incident. Perfect security may not exist, but you can get a lot closer than you might think. Following the steps outlined in this paper will go far in strengthening your cybersecurity posture. For more information, answers to questions, or help with more advanced strategies, please visit www.minfosec.com or email sales@minfosec.com.

About Makaye Infosec

We are a team of cybersecurity professionals with a passion for making the world a safer place by protecting SMBs from cybercriminals and helping them achieve security compliance. We serve the SMB market by helping businesses drastically reduce cybersecurity risk and stay compliant in the face of today's online threats. We work to implement necessary security controls, policies and develop ongoing security programs that are based on the NIST cybersecurity framework. We take the seemingly overwhelming cybersecurity and compliance requirements breaking them down into manageable and commonsense processes. We assist with implementation of these controls and provide ongoing management of the cybersecurity program.

Address
269 Renner Pkwy
Suite 150
Richardson, TX 75080

Phone
(469) 330-7001

Sales
sales@minfosec.com

Web
www.minfosec.com

References

[i] https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
[ii] https://www.theglobeandmail.com/featured-reports/article-small-businesses-caught-in-an-epidemic-of-cyber-attacks/
[iii] https://insights.sei.cmu.edu/sei_blog/2019/10/situational-awareness-for-cybersecurity-assets-and-risk.html
[iv] https://enterprise.verizon.com/resources/reports/dbir/
[v] https://internetofbusiness.com/password-iot/
[vi] https://www.nytimes.com/2018/03/13/smarter-living/how-to-encrypt-your-computers-data.html
[vii] https://www.nytimes.com/2018/03/13/smarter-living/how-to-encrypt-your-computers-data.html
[viii] https://www.computerworld.com/article/3173246/94-of-microsoft-vulnerabilities-can-be-easily-mitigated.html
[ix] https://blogs.gartner.com/neil_macdonald/2011/08/23/the-single-most-important-way-to-improve-endpoint-security/
[x] https://www.csoonline.com/article/3095486/cybersecurity-is-only-as-strong-as-your-weakest-linkyour-employees.html
[xi] https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
[xii] https://www.inc.com/joe-galvin/60-percent-of-small-businesses-fold-within-6-months-of-a-cyber-attack-heres-how-to-protect-yourself.html