WHITE PAPER

Cybersecurity Best Practices

for Small and Medium Businesses (SMB) in the Health & Human Services Industry

medisked

The Problem with SMB Cybersecurity

The most common question Small and Medium Businesses (SMBs) ask about Information Security / Cybersecurity is "Why?" Why would a hacker want to attack my organization? What would a hacker want from my network? How bad could it really be? Why should we spend our time or money on cybersecurity? The answer may surprise you.

Here are some of the ways the 'hackers' (more appropriately called 'threat actors') exploit small businesses:

DATA THEFT

Not just data about your company or your bank accounts, but also about you, your employees, and the individuals your organization supports (names, email addresses, social security numbers, and other Personally Identifiable Information [PII]).

RANSOMWARE

Threat actors could encrypt your systems and only give you the decryption key if you pay them. Even if you do not, many times they will then force you to pay to keep your company's information from being released to the public.

INDIVIDUALS YOU SUPPORT

Many threat actors realize that while a larger or more protected hospitals or healthcare organization may be difficult to attack, their smaller providers may be easier targets. By using this variant of a "supply chain" attack, threat actors may be able to more easily access the information they seek.

Besides these kinds of exploits, there is another major technical evolution that has further endangered SMBs: **Machine Learning (ML)**. ML, a subset of Artificial Intelligence, "is a field of inquiry devoted to understanding and building methods that 'learn', that is, methods that leverage data to improve performance on some set of tasks."[1] Before the advent of ML, attackers would have to manually reconnoiter and slowly test the defenses of any business one at a time. However, modern cyber criminals have readily embraced these technologies and have used them to scour the internet with automation, 'improving their performance' such that they are enabled to attack scores of weakly defended SMBs almost continuously and with impunity. In fact, according to some reports, **55% of SMBs have experienced cyber-attacks.**[2]

[1] https://en.wikipedia.org/wiki/Machine_learning

[2] https://www.connectwise.com/blog/cybersecurity/why-smbs-are-high-risk-for-cybersecurity-threats-in-2021

What is the average cost of a SMB data breach?

Attacks against SMBs are not only increasing in frequency but they are also becoming more expensive. IBM commissioned the Ponemon Institute to conduct research and subsequently publish the 2021 Cost of a Data Breach report in which they concluded that organizations with less than 500 employees spent an average of $2.98 million per data breach.[3]

Unfortunately, cybercrime is a profitable business and many SMBs are quite blissfully ignorant of the enormous risk that these threat actors and constituent criminal organizations represent. A 2018 EUROPOL report stated that the "total global impact of cybercrime [has risen to] US $3 trillion, making it more profitable than the global trade in marijuana, cocaine and heroin combined."[4] As astounding as that sounds, it has gotten far worse since the drafting of that EUROPOL report. According to a 2021 report from the US Federal Bureau of Investigation (FBI), cybercrime cost over $3.46 trillion in damages within the United States alone (see Table 2).[5] While it is staggering to realize that the cost of cybercrime in the US is more than what it was worldwide just four years ago, it is even worse when you realize that business may only be reporting 28% of all attacks to law enforcement.[6] Suffice to say, cybercrime is big business indeed.

2021 By Victim Loss

Crime Type	Loss ($)
BEC/EAC	2,395,953,296
Personal Data Breach	517,021,289
Identity Theft	278,267,918
Corporate Data Breach	151,568,225
Ransomware	49,207,908
Phishing/Vishing/ Smishing/Pharming	44,213,707
Computer Intrusion	19,603,037
Malware/Scareware/ Virus	5,596,889
TOTAL: $3,461,432,269	

Table 1. *Data from the Federal Bureau of Investigation Internet Crime Report 2021[5]*

[3] https://www.ibm.com/security/data-breach
[4] https://www.europol.europa.eu/iocta/2018
[5] https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
[6] https://www.csoonline.com/article/3398700/why-businesses-don-t-report-cybercrimes-to-law-enforcement.html

SMB Cyber Threats

The next issue to deal with in regards these cyber threats is to consider how threat actors are gaining access to SMB networks. In Verizon's 2022 Data Breach Investigations Report (DIBR) (see Figure 1), the top three threat vectors cyber adversaries are using against SMBs are Ransomware, Stolen Credentials, and Phishing.[7]

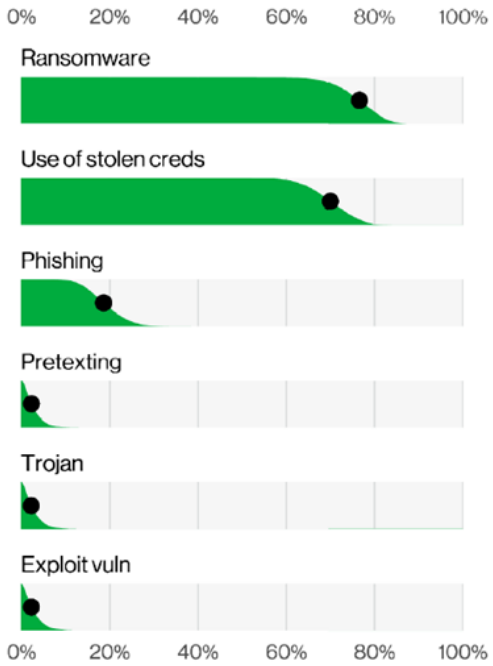

Figure 1. *From Verizon's 2022 Data Breach Investigations Report (DIBR)*[7]

Ransomware is very straightforward; they get into your network, encrypt all or most of your data, and you must make a substantial payment to get the encryption keys to get your data back. Until you do – or unless you have backups – your company's network and data are unavailable.

The second most common threat is **Stolen Credentials**, which involves the theft of valid usernames and their corresponding passwords. This can happen through a variety of means including phishing, man-in-the-middle attacks, mass breaches of customer databases which get posted online, and lack of security training or requirements. These credentials are the classic way to get into many networks, and the bad guys realize that finding a valid user's credentials is much safer, simpler to use to avoid detection, and easier to get.

Finally, the third top vector is **Phishing**. If you are not already familiar with phishing, this is the practice of sending emails that appear to come from a trustworthy source which entices the recipient to give information, click on a link, or open an attachment that they would not otherwise do. Phishing has been at the top of the threat vector list for several years now and it continues to be a threat to all businesses as this type of attack accounts for more than 90% of data breaches.[8] Phishing is also one of the most 'visible' types of attacks in terms of the end user's perspective.

[7] https://www.verizon.com/business/resources/reports/dbir/

[8] https://umbrella.cisco.com/info/2021-cyber-security-threat-trends-phishing-crypto-top-the-list

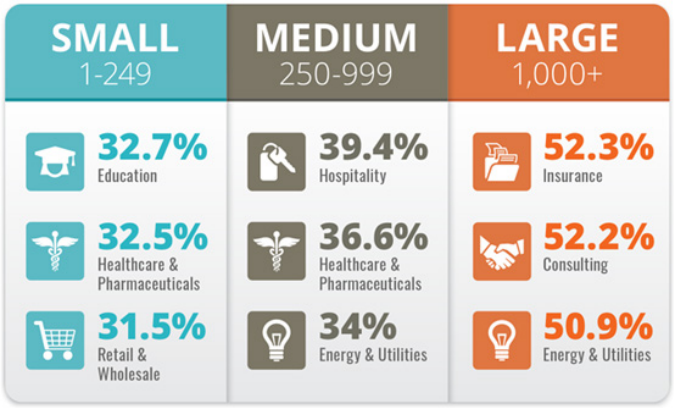

Figure 2. *From KnowBe4*[9]

According to phishing awareness and training company KnowBe4 (see Figure 2), some industries are more at risk based on their size.[9] However, the statistics show that as many as 3 billion phishing emails are sent every day, and around 19.8% of people click on phishing email links.[10] This means that statistically every SMB will have to deal with phishing attacks one way or the other. The only choice they have is in whether they choose to protect their users and data or

Unfortunately, one of the most dangerous risks to SMBs is not external, but rather the mindset for how smaller businesses see the risk they face from the many varieties of attacks. Many smaller organizations fail to see the legitimacy of cyber-attacks as they see themselves as too small to be a target. However, 43% of attacks in 2021 involved SMBs; the same percentage of SMBs that said they do not have any cybersecurity plan in place to defend themselves.[11] Another fallacy is to believe that a SMB could not really be materially harmed by cyber-attacks even though 40% of the SMBs that faced a severe attack experienced at least eight hours of downtime.[11]

SMB Cybersecurity Best Practices

Despite the enormity of the threat to SMBs, the situation is not hopeless. There are a vast number of resources available freely to even the smallest organizations with expert tips on how to protect your business from these constant external threats. For example, the United States' Cybersecurity & Infrastructure Security Agency (CISA) has a page with resources for SMBs including their "Cyber Essentials" guide.[12] Similarly, the National Cybersecurity Alliance and the U.S. Small Business Administration (SBA) both provide helpful guidance and links to provide SMBs with cyber tips.[13] You can also find assistance from commercial organizations like Verizon, whose 2022 Data Breach Investigations Report has a section on what to do to avoid becoming a target for cyber criminals, as well as how to tell if you have been victimized,

[9] https://www.knowbe4.com/phishing

[10] https://www.zdnet.com/article/three-billion-phishing-emails-are-sent-every-day-but-one-change-could-make-life-much-harder-for-scammers/ and https://terranovasecurity.com/gone-phishing-tournament

[11] https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/

[12] https://www.cisa.gov/uscert/resources/smb

[13] https://staysafeonline.org/cybersecurity-for-business/ and https://www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threats

and whom you should contact if it happens.[14] Each has a somewhat unique perspective on what constitutes effective security for SMBs and all can provide value if their advice is effectively implemented.

The truth is that the information security controls a SMB should implement depends greatly on what type of business it is and how they conduct their operations. With that all being said, there are some universal best practices that most organizations can implement regardless of their size that can have a significant impact on the company's cyber resilience.

1. Train Your People

Most organizations think about cybersecurity in terms of technology and blinking lights, but it starts with your employees. Training your staff about cybersecurity not only helps them understand why information security is important, but it is also critical to helping them understand the scope of the threat and their responsibilities to help protect your systems and data. For example, if users do not understand what a phishing attack is, what red flags they should be looking for daily, or what to do to report a suspected phishing attack, your organization is understandably at risk. This training should be repeated annually, reenforced throughout the year (e.g., testing with simulated and unannounced phishing tests), and highlighted during Cyber Security Awareness Month (CSAM) in October.[15]

2. Patch Your Devices and Software

While we have gotten much better about patching operating systems (installing the latest vendor updates) and software over the last few years, unpatched machines represent a significant risk to any network. For Microsoft-based machines, the developer releases monthly software updates on "Patch Tuesday" as well as out-of-phase updates for some critical patches.[16] These patches should be applied as quickly as possible, as each patch notification is also a roadmap for threat actors to exploit the vulnerabilities the patches remediate.

Organizations should also patch their networking equipment (e.g., routers, switches, etc.) in addition to any smart devices (e.g., smart TVs) that may be on the network. These devices are often overlooked but can represent a significant threat if left unmanaged.

[14] https://www.verizon.com/business/resources/reports/dbir/
[15] https://www.cisa.gov/cybersecurity-awareness-month
[16] https://msrc.microsoft.com/update-guide

3. Backup Your Data

Backing up your data has always been a common-sense control so that you can restore your systems and data following the failure of a server or some catastrophic incident. However, the rise of ransomware has made this an even more critical component of a secure system architecture. The use of off-line backups which are only connected to a computer or network when actually backing up or restoring systems is a further control to counteract the reach and impact of ransomware on your SMB's data.

4. Password Security

Many organizations consider the mere existence of a password to be sufficient, but this is certainly not the case. According to security.org (see Table 2), short and non-complex passwords can be 'cracked' (broken) almost immediately.

Fortunately, there are a number of relatively simple controls that SMBs can implement to address this risk. They include:

ENFORCE STRONG PASSWORDS

Require users to select passwords at least 12 characters long, including at least one uppercase letter, number, and symbol which are changed every 90 days. Even better, encourage the use of long pass phrases that are easier to remember but more difficult to crack; these may only have to be changed annually.

# of Characters	Lowercase letters only	≥1 uppercase letter	≥1 uppercase letter + number	≥1 uppercase letter + number + symbol
Up to 6	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 min	6 min
8	Instantly	22 min	1 hrs	8 hrs
9	1 min	19 hrs	3 days	3 wks
10	1 hrs	1 mths	7 mths	5 yrs
11	1 day	5 yrs	41 yrs	400 yrs
12	3 wks	300 yrs	2,000 yrs	34,000 yrs

Table 2. *Data from security.org on how long it takes for passwords to be cracked.*

AVOID OLD PASSWORDS

Do not allow users to reuse old passwords as old passwords may be compromised and available to threat actors online. You can check some of these yourself using the website https://haveibeenpwned.com.

DO NOT REUSE PASSWORDS

This is different from using a password you once used—it is the practice of using unique passwords for every account you may use. Statistics show that during a Microsoft study over just three months from January to March 2020, 44 million users used the same password on more than one account.[17] Similarly, a 2019 Google study found that 52% of users reused the same password on more than one site while 13% used the same password for all of their accounts.[18] This makes your corporate password as unsecure as the weakest security of another site using the password, so this is a practice to avoid.

USE A PASSWORD MANAGER

The easiest way to ensure good password security is to use a password manager, also referred to as a password vault. These types of software can generate complex unique passwords for your accounts and save those for you so that all you have to do is remember one master password to get into your manager.

5. Multi-Factor Authentication (MFA)

Given the susceptibility of a password, MFA (often also called two-factor authentication) can greatly reduce your risk from hackers.

There are three general types of authentication:

Something you **know**
(like a password or PIN)

Something you **have**
(like a physical key)

Something you **are**
(like a fingerprint)

Having at least two different types of authentication constitutes MFA and according to a Microsoft report, MFA can block 99.9% of automated attacks.[19]

[17] https://www.comparitech.com/blog/information-security/password-statistics/
[18] https://services.google.com/fh/files/blogs/google_security_infographic.pdf
[19] https://www.zdnet.com/article/better-than-the-best-password-how-to-use-2fa-to-improve-your-security/

6. Protect Email

There are numerous vendors who can implement outgoing mail encryption and real-time defense automation like phishing detection, spam quarantining, image & link sandboxing, and other protections.

However, there are three relatively simple and inexpensive controls that you can put in today that provide significant protection against many email-based attacks, based around DKIM (Domain Keys Identified Message), DMARC (Domain-based Message Authentication, Reporting & Conformance), and SPF (Sender Policy Framework).[20] Making sure your DKIM, DMARC, and SPF records are properly configured will not stop everything, but it will authenticate your outbound emails and help to ensure the reputation of any sender domains – on the cheap.

7. Anti-Virus Software

While this is almost a given in the current day, many organizations fail to implement this very fundamental security control. However, even those companies that do install Anti-Virus (AV) software on endpoints sometimes fail to ensure that they are constantly updated with the most current virus signatures (how viruses are detected for pattern-based AV products). If you want to go to the next level, all devices should also have a heuristic (learning) based AV solution that scans for non-file (memory) based viruses for layered protection.

8. Remove Local Administrator Access

Many small organizations allow all users to have local administrative access to their computer or laptop. Unfortunately, this means that each user is a potential fast track into the heart of your network if they or their credentials are compromised. Restricting administrative access to only your IT team is a best practice that will save many SMBs hundreds of hours of grief.

[20] https://dmarc.org/2016/03/best-practices-for-email-senders/

9. Close Unused Ports & Services

By default, most operating systems (e.g., Windows 11) turn on a myriad of services to make the host computer even more functional. Any of these services that connect or interoperate with other network or web-based devices listen on 'ports' (similar to channels on a TV) which usually have discrete and defined functions (e.g., port 80 is for web browsing [http] and 443 is for secure web [https]). However, many of these ports and services may not only be unused by most users but could also represent opportunities for threat actors to gain access to your company's network. Disabling these unused ports & services reduces the attack surface for external threats.

10. Monitor Your Network

While it would be nice to say we could completely protect your SMB's network, this is simply not realistic in our complex, internet connected world full of program bugs and zero-day attacks. As Dr. Eric Cole said,

"Prevention is great, but detection is a must."

The only way to really secure your network is to assume the bad guys have gotten inside and you have to detect them as soon as possible.

While there are open-source (i.e., free) Security Information and Event Monitoring (SIEM) solutions (like OSSIM, the ELK stack, OSSEC, and Wazuh to name a few), these can be overwhelming if you do not have cybersecurity expertise and experience on-staff. In these situations, you can contract with a Managed Security Services Provider (MSSP) who can provide your organization with 24/7/365 network monitoring and only alert you when something truly suspicious is happening on your network.

Beyond the Basics

Finally, health and human services organizations should take an even more thorough approach to their network security than other SMBs, as they deal with Protected Health Information (PHI). Your organization may want to consider implementing a security control framework like the Cyber Security Framework (CSF) which was developed by the National Institute of Standards and Technology (NIST) pursuant to Executive Order 13636 which was signed by President Obama in 2013.[21] This is a straightforward framework, and it can give your organization the standards, guidelines, and best practices to further its maturity and manage cybersecurity risk.

Whatever strategy your organization takes, rest assured that your SMB is anything but powerless. The key is to implement these fundamental controls and make sure that you are not the weakest member of the herd—let the hackers find someone easier to mess with. With a little time and attention, you can make your environment resilient to many of the most common attacks and ensure that your systems and data will be there when your business needs it most.

About the Author

Shayne Champion is the Chief Information Security Officer (CISO) at MediSked, LLC. With almost 30 years in Information Technology (IT) and Cyber Security industries, Shayne has experience spanning a wide range of technical domains. He has built, worked in, lead, and/or managed a wide variety of IT organizations prior to joining MediSked in 2020.

[21] https://www.nist.gov/cyberframework and https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

MediSked is the leading brand in holistic solutions that improves lives, drives efficiencies, and generates innovations for health and human service organizations that support our community. MediSked solutions combine to provide innovative, person-centered technology that improves outcomes and quality, while reducing costs for individuals receiving home and community-based services and long-term services and supports through government & oversight, care coordination/payer and provider agencies. MediSked has supported clients across the United States since 2003.

Want to learn more? Check out medisked.com!