Cybersecurity guide for small business

Written by Steven Bowcut – Last updated: February 24, 2021

Small business owners face unique challenges in many areas of their profession. Cybersecurity is no exception. From understanding their risk to finding appropriate resources for mitigating that risk, many small business owners struggle to keep their small enterprise cyber-safe.

Their struggle to stay cyber-safe is attributable to the need for small business owners to work within a budget. Budget restraints often mean that they are responsible for making decisions in areas for which they may lack expertise. Being the best plumber, consultant, or dentist in the world does not necessarily include the knowledge needed to negotiate shark-infested cyber waters.

This guide provides strategies and suggestions for keeping small businesses safe from the ever-growing catalog of cyber threats. It includes ideas for calculating risk, understanding threats, plugging vulnerabilities, and implementing mitigation steps. A list of useful resources is also included.

Small businesses are attractive targets

Small business owners walk around with a metaphoric target on their backs. At least, that is how cyber threat actors may see it.

> According to the Small Business Administration (SBA), 99.7 percent of U.S. employer firms are small businesses. These independent businesses, each having less than 500 employees, account for 49.2 percent of private-sector employment

Small businesses are a critical part of the US economy, and cyber attacks are a growing threat against them. Small businesses are an attractive target because they have information that cybercriminals can leverage, and they often lack the security infrastructure of larger enterprises.

Sometimes the gains to be had from attacking a small business are smaller than what the results could be if a larger enterprise were the focus of a cyber-

attack. But, because of the corresponding lack of security controls, bad actors can see small businesses as “easy pickings.”

Other times, however, a small business is viewed as a critical component of the attack vector into a large enterprise. Large firms of every type use small business vendors. The SBA incentivizes large companies to use small business suppliers. Cybercriminals have found that attacking a large firm through their small business partners can be a successful strategy.

According to a recent SBA survey, 88 percent of small business owners felt their business was vulnerable to a cyber attack. Yet many companies can’t afford professional IT solutions, they have limited time to devote to cybersecurity, or they don’t know where to begin.

How to evaluate cyber risk

Before a small business owner can make any informed decisions about improving their cybersecurity posture, he or she must have a clear picture of their cyber risk.

An understanding of this risk will guide the implementation of security strategies, process changes, and justify security-related expenditures. Without understanding risk, any security decisions are nothing more than a shot in the dark, hoping to hit the mark.

While there are many definitions of risk, each requires an understanding of threats, vulnerabilities, and criticality or impact.

The basic equation is **Risk = Threat x Vulnerability x Impact**.

Each of the three factors are described in detail below. Deriving the product, risk, will enable the small business owner to make informed decisions rather than emotional or fear-based choices.

Although risk is represented here as a mathematical formula, it is not about numbers; it is a logical construct. For example, suppose a small business owner wants to assess the risk associated with the threat of hackers

attempting to plant ransomware (a likely threat) on a system containing essential data.

If the network is particularly vulnerable (perhaps because it has no firewall and no antivirus software), and this system is critical (a loss would constitute a negative impact on the company's ability to maintain its operation), then their risk is high. However, if the small business has good perimeter defenses, so their vulnerability is low, and even though the system is still critical, their risk will be medium.

Security vendors crowd the industry with often-competing claims of the best way to stay safe online or to protect sensitive data. To be generous, the credible vendors are not wrong in their claims, but their solutions are not always a good fit for small businesses.

Cyber threats to small businesses

The two most common types of threats for small businesses are social engineering and malware. While hackers often accomplish social engineering attacks without the use of malware, malware attacks almost always include a social engineering component.

About 97 percent of cyber threats include some element of social engineering. Social engineering is the use of deception to manipulate individuals causing them to divulge confidential information or to click a link and download a file or to visit a malicious web page.

This is often accomplished with email phishing techniques but can also be performed by telephone or text message deception. The most common objective for social engineering campaigns is to obtain a victim's account login credentials. Still, it could also include luring the victim to use a link or visit a website where the hacker can deploy ransomware or other malware.

This guide addresses mitigation strategies later, but this is an excellent time to pause and consider that the most effective cybersecurity mitigation strategies that small businesses can adopt are related to the knowledge and behavior of themselves and their employees.

Malware threats

Malware (malicious software) is an umbrella term that refers to software deliberately designed to cause damage to a computer, server, client, or computer network. Malware can include viruses and ransomware. The objective of a social engineering attack may be to convince someone within a small business to download malware unwittingly.

Viruses are malicious programs intended to spread from computer to computer (and other connected devices). Viruses are designed to give cybercriminals access to the victim's system. Their ability to spread from one computer to another makes them a favorite for bad actors that are targeting a small business because of their relationship with a larger target.

A hacker may be looking for a way to spread a virus to the larger firm through their computer connection with the smaller firm.

Ransomware is a specific type of malware that locks a victim out of their computer or encrypts targeted data until a ransom is paid. Ransomware is usually delivered through a malicious link in a phishing email and exploits unpatched vulnerabilities in software.

Often the data or system is not released even after the ransom is paid. Small businesses are often hyper-dependent on their critical data. The loss of this data could cripple a small firm. Hackers prey on this vulnerability using ransomware.

Email threats

Phishing is a type of social engineering attack that uses email or a malicious website to infect a machine with malware or collect sensitive information. Phishing emails appear as though they have been sent from a legitimate organization or known individual.

These emails often entice users to click on a link or open an attachment containing malicious code. After the code is run, the computer may become infected with malware.

Many small businesses take advantage of the economies of cloud-based email services. These low-cost email providers are ideal for companies that have fewer employees and don't need a full-featured email service.

The FBI recently warned that cybercriminals are targeting organizations that use popular cloud-based email services to conduct Business Email Compromise (BEC) scams.

The scams are initiated through specifically developed phish kits designed to mimic the cloud-based email services to compromise business email accounts and request or misdirect transfers of funds. Between January 2014 and October 2019, the Internet Crime Complaint Center (IC3) received complaints totaling more than $2.1 billion in actual losses from BEC scams using two popular cloud-based email services.

While most cloud-based email services have security features that can help prevent BEC, many of these features must be manually configured and enabled. Users can better protect themselves from BEC by taking advantage of the full spectrum of available protections.

Video-teleconferencing threats

As large numbers of people turn to video-teleconferencing (VTC) platforms to stay connected in the wake of the COVID-19 crisis, reports of VTC hijacking (also called “Zoom-bombing”) are emerging nationwide. The FBI has received multiple reports of conferences being disrupted by pornographic and/or hate images and threatening language.

While the current COVID-19 pandemic has forced many companies and individuals to turn to video-teleconferencing as a primary communication tool, small businesses have historically relied on these tools to support virtual offices and remote employees.

Common cyber vulnerabilities

A vulnerability is a weakness that can be exploited by an attacker to gain unauthorized access to or perform unauthorized actions on a computer system or device. Vulnerabilities can allow attackers to run code, access memory, install malware, and exfiltrate, destroy or modify sensitive data.

While many cyber vulnerabilities affect the risk of enterprises large and small, the most common for small businesses include

behavioral, code injection, sensitive data exposure, endpoint protection, and credential management types.

These vulnerabilities are interrelated, and often two or more will be exploited in a cyberattack.

Behavioral vulnerabilities

As stated earlier, 97% of cyber threats include some element of social engineering. While not all human-caused vulnerabilities are the result of social engineering, this statistic highlights the fact that human behavior is the single most significant factor in cybersecurity. The behavioral vulnerabilities (weaknesses) class includes:

- Poor password practices
- Clicking on malicious links in phishing emails
- Browsing to unsafe websites
- Downloading malicious files
- Failure to take prescribed steps to protect sensitive information
- Failure to keep systems updated and patched

Industry analysts have written much about the susceptibility of end-users to social engineering, but it continues to be a significant issue that plagues organizations. The 2019 Verizon DBIR states that end-user error is the top threat action in breaches. Many organizations find the initial point of attack is through targeted social engineering, most commonly phishing.

Injection vulnerabilities

Injection attacks are becoming more commonplace. Injection vulnerabilities are those flaws that allow cyber attackers to inject malicious code into the victim’s system.

A common injection attack is the placement of malicious code in SQL statements, via web page inputs. Hackers accomplish these attacks by exploiting applications that allow user inputs to a database, shell commands, or the operating system.

These flaws are usually a result of insufficient input validation. Other causes involve failure to filter or sanitize a user’s input.

Sensitive data vulnerabilities

Security experts recommend that PII and other valuable data are stored in an encrypted format. This precaution, while helpful, does not ensure that data is always protected. There are other precautions to consider.

Data in transit, not just at rest in storage, must be protected. Transmitting encrypted data requires that the receiver have the capability of decrypting the data. This requirement introduces its own set of risks.

Humans failing to take the prescribed precautions for protecting sensitive data also adds a layer of vulnerability. Whether it is saving data in plain text or in an inappropriate location, humans are often the weakest link in protecting data.

Even encrypted data is susceptible to a ransomware attack. At the individual file level or the entire system on which the data resides, ransomware malware can prevent access to critical information.

Endpoint vulnerabilities

Every laptop, desktop, mobile phone, and tablet connected to the business network is an endpoint. Each device is a potential entry point for malware.

The number of applications on each device and whether each application complies with security policies will define a small business's exposure due to endpoint vulnerabilities. Because of compromised applications and missing or outdated operating system and application patches, a small business could have thousands of endpoint vulnerabilities.

Many security experts no longer consider standard signature-based antivirus systems good enough, as many savvy attackers can easily bypass the signatures. Unusual activity at the endpoint is often the best indication that an attacker has breached the defenses.

Credential management vulnerabilities

One of the most common causes of system or account compromise is a lack of sound credential management. Users reusing the same password for

multiple accounts, even reusing passwords for personal accounts on business systems, represents one of the most exploited vulnerabilities for small businesses.

Of the behavioral vulnerabilities class, this vulnerable behavior is at the heart of many of today's high profile breaches. Each year hackers exfiltrate vast amounts of data, mainly in search of usernames and passwords.

Hackers value this data because they can use it in a type of cyberattack called credential stuffing. Credential stuffing is when bad actors use automated tools to attempt logins across a wide array of popular sites using credentials stolen in previous breaches.

Because credential management vulnerabilities are of the behavioral class, they can be corrected without expensive security systems. Avoiding them does, however, require discipline from small business owners and employees.

Cybersecurity mitigation strategies

In the basic risk equation of **Risk = Threat x Vulnerability x Impact,** risk can only be improved if the threat and vulnerability factors are reduced. Since the impact factor is the adverse effect of an attack, it seldom changes.

Mitigation strategies are those processes, policies, and tools that a small business owner can put in place to decrease the threat and diminish the vulnerabilities. Risk is rarely reduced to zero, but it conceivably could be if a vulnerability were to be eliminated entirely.

Mitigating behavioral vulnerabilities

In a word, training is the best way to mitigate behavioral vulnerabilities. This is true for businesses of all sizes, but it would be difficult to overestimate the importance of cyber training for small business owners and employees. Without sufficient resources to invest in sophisticated cybersecurity systems and tools, training will provide the best cybersecurity results for small businesses.

The most probable cause of a successful social engineering attack is a lack of security awareness training and end-user validation. Many small businesses are struggling with how to train users to look for social engineering attempts and report them.

More companies need to conduct regular training drills, including phishing tests, pretexting, and additional social engineering ploys. Many training programs are available to help reinforce security awareness concepts; the training needs to be contextual and relevant to an employee's job functions whenever possible. It is essential to track a user's success or failure rates on testing, as well as "live fire" tests with phishing emails and other tactics. For users who don't improve, look at remediation measures appropriate for that organization.

Mitigating injection attacks

Monitoring computer systems for abnormal input behavior has proven to be an effective mitigation strategy for injection attacks. Next-generation antivirus tools are available that watch for actions not consistent with human input and behavior patterns that are known to be used by malicious actors. These tools provide a more comprehensive analysis of malicious behavior, along with more flexible prevention and detection options.

Small businesses would be well advised to consider investing in security systems that employ some aspects of behavioral inspection techniques. Legacy signature-based antivirus tools are quickly becoming outdated as hackers find new ways to work around these systems. Some of these more modern mitigation tools provide real-time response capabilities as well.

Mitigating attacks against sensitive data

Encrypting data is not an expensive endeavor, and small businesses should follow best practices for using encryption for protecting data. Using a VPN to encrypt data as it is transmitted is a common and effective solution.

Data at rest should remain encrypted even when access controls such as usernames and passwords fail. Following this practice will ensure that if social engineering efforts to gather system login credentials are successful, the data will still be protected.

Increasing encryption on multiple levels is recommended. Cryptography can be implemented on the database containing the data and on the physical storage where the databases are stored. Data encryption keys should be updated regularly. Encryption keys should be stored separately from the data. Periodic auditing of sensitive data should be part of a security policy and should happen on scheduled occurrences.

One solution that many small businesses find satisfactory for protecting data in transit is the use of encrypted flash drives. If encrypted data is needed in a remote location, physically moving the information on an encrypted drive may be the right solution in some circumstances.

To protect data against ransomware, small businesses will benefit from a multi-pronged backup and recovery strategy. This strategy should include system snapshots and replication, database backups, and end-user storage (often cloud-based).

Mitigating endpoint vulnerabilities

Constructing and enforcing policies that require all applications and operating systems on any endpoint connected to the business network be updated and patched is the most effective and yet least expensive endpoint protection measure.

As the expression goes, it is easier said than done, however. Owners and employees of small businesses often use one device for both personal use and business use. Enforcing security policies that may affect or restrict the use of mixed-use devices can be challenging. Setting clear expectations for endpoint security from the outset is vital for avoiding future misunderstandings and policy non-compliance.

Antivirus and endpoint protection software vendors are continually improving their solutions. Small business owners should make every effort to stay abreast of the latest technologies that fit in their budget.

Mitigating credential management vulnerabilities

For most organizations, implementing stringent password controls can help. This measure may consist of longer passwords, more complex passwords,

more frequent password changes, or some combination of these principles. In practice, longer passwords, even when not changed often, are safer than shorter passwords that are changed regularly.

Relatively inexpensive password management tools help simplify and enforce password policies. These tools eliminate the need for users to try and remember a large number of passwords. With each person needing access to so many systems, devices, and applications, remembering unique passwords for each is nearly impossible.

Password management tools, used in a team environment, give small business owners the ability to change the access rights of individual employees.

For any sensitive access, users should also use multi-factor authentication when accessing sensitive data or sites. Multi-factor authentication tools can aid in this process.

While researchers often spot other significant cybersecurity vulnerabilities in the wild, the issues addressed here are some of the most common seen by small businesses everywhere. Look for opportunities to mitigate threats and vulnerabilities to reduce risk more effectively.

Cybersecurity resources for small business

The National Cyber Security Alliance's (NCSA's) CyberSecure My Business™ is a national program helping small and medium-sized businesses (SMBs) learn to be safer and more secure online. https://staysafeonline.org/cybersecure-business/

The Federal Communications Commission offers a cybersecurity planning tool to help businesses build a strategy based on their unique business needs.

The Department of Homeland Security's (DHS) Cyber Resilience Review (CRR) is a non-technical assessment to evaluate operational resilience and cybersecurity practices. Assessments can be self-administered or request an on-site assessment by DHS cybersecurity professionals.

DHS also offers free cyber hygiene vulnerability scanning for small businesses. This service can help secure internet-facing systems from weak configuration and known vulnerabilities.