Cybersecurity Mistakes All Small Business Employees Make, from Entry Level to the C-Suite

SWITCHFAST®

Introduction

When cybercriminals strike, it's often large enterprises that make front page headlines. But don't be fooled — the small coffee shop down the street and the local grocer are even more likely to be targets for malicious hackers.

Despite common misconception, small businesses are prime targets for hackers because of their size. Thieves aren't concerned about how big a business is; as long as there is financial gain to be had from stealing, any company is fair game. The absence of a dedicated IT or security professional leaves small businesses vulnerable to otherwise preventable attacks, like phishing schemes and fraudulent activity. In 2016 alone, over 14 million American small businesses were breached by cybercriminals. And with over 30 million small businesses listed in America, that means 46 percent of all small businesses will likely become the victim of a cyberattack.

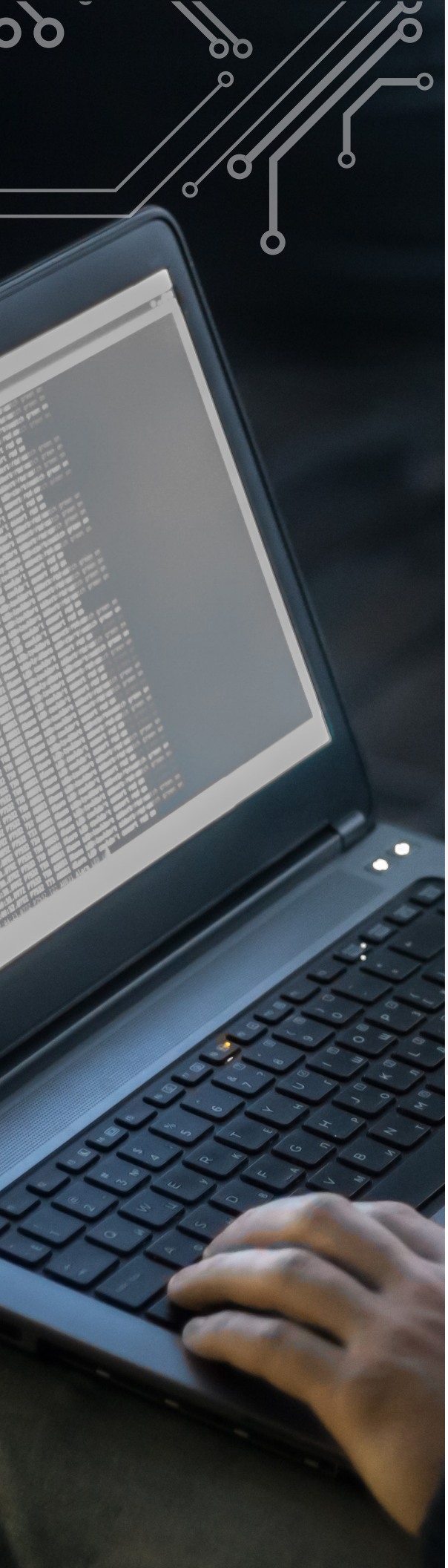
For many businesses, these cyberattacks can be financially devastating — 60 percent of small businesses that suffer a breach are likely to go out of business within six months. From a loss of customers to a damaged reputation, small businesses have a lot to lose, and one in three business owners have no safeguards in place to combat a cyber breach. With activities like electronic wire fraud and phishing scams becoming all-too-common, small businesses need to reevaluate the strength of their existing security protocols.

Today's cybercriminals employ a variety of complex attack methods to exploit business weaknesses and target employees with bad cyber hygiene, whether it's the CEO or an intern, bypassing the basic security measures most companies have in place. Until they recognize they are prime targets for hackers and adjust their security strategies, small businesses will continue to fall victim to rampant cyberattacks.

Switchfast, an IT consulting and managed services provider, surveyed over 600 full-time small business employees and 100 C-suite level leaders to uncover why small businesses continue to struggle with good cybersecurity practices and what can be done to correct those habits.

This report will explore how internal behaviors from employees at all levels contribute to the rising number of cyberattacks against small businesses, and how companies can begin to address poor cyber hygiene and mitigate risk.

One in three business owners have no safeguards in place to combat a cyber breach



Diagnosing the Problem Small Businesses are Underestimating the True Cost of Cyber Risk

Small businesses typically lack the manpower and budget enterprise-level businesses can count on to handle things like IT and security. One IT employee simply isn't equipped to handle the day-to-day technology responsibilities while running surveillance initiatives to keep the bad actors at bay, and small businesses are taking a huge risk relying on their employees to not fall victim to lurking hackers. In addition to a lack of resources, internal disagreements about the severity of cyberattacks complicate the cybersecurity dilemma. Thirty-five percent of employees and 51 percent of leaders are convinced their business is not a target for cybercriminals, which could explain why small businesses don't prioritize security education and best practices.

Consider a small marketing agency with fewer than 25 full-time employees. To accommodate their "work-from-anywhere" mentality, the agency migrated all of their work documents to a cloud-based platform like the G-Suite. After setting up multi-factor authentication (MFA) and briefing employees on how to access the server from anywhere, the agency adopts a "set it and forget it" mentality. In essence, because small businesses believe their security due diligence is complete after the initial set-up, they often neglect to check in on the health of their network. As a result, employees begin connecting to servers over public Wi-Fi spots at coffee shops and accessing social media accounts on their work laptops.

One day an employee accidentally sets the user permissions on a confidential spreadsheet to public and sends the link to a colleague over public Wi-Fi. A cybercriminal, sitting in the same coffee shop, intercepts the email with a man-in-the-middle attack and downloads the public spreadsheet to post on the dark web. In addition to compromising client information, employee data like social security numbers and home addresses are also at risk of exposure. Without a proper incident response plan in place, the marketing agency isn't sure who to inform about the security breach and chooses to notify clients with a short email. Unfortunately, clients — and some employees — become frustrated with how the agency handled the breach and take their business elsewhere.

The above scenario is all-too-common. While some small businesses may be tempted to take cybersecurity into their own hands, juggling both business operations and digital security can be overwhelming for one company to handle on its own.

Gone Phishing

Phishing, an attack method where hackers distribute malicious links via email, is a highly effective scheme employed by thieves to extract valuable information from victims. Ninety-one percent of cyberattacks originate with a phishing email, and companies are doing little to prevent employees from falling for these schemes. Routine phishing tests, for example, are an effective way to test workers' ability to recognize and respond to fake emails. Designed to simulate a real phishing attack, these test emails contain a link that monitors who falls for the scam and who responds in the appropriate manner. Unfortunately, 65 percent of SMB employees have never received a phishing test during their tenure.

In addition to targeting employees, cybercriminals employ an attack similar to phishing to exploit small business leaders known as "whaling." Just like with phishing, attackers will spoof emails to look like they come from trustworthy individuals in an attempt to get high-profile executives to divulge sensitive information. And with approximately 20 percent of small business leaders having fallen victim to a phishing scam before, companies should be concerned with how their leadership teams are taught to recognize and respond to whaling schemes.

When small businesses maintain a lax attitude towards cyber threats, it often leads to reactive policies that do little to mitigate damage when disaster strikes. Instead of waiting to take action after a breach occurs, small businesses should approach cybersecurity planning the same way they treat natural disaster protocols. For example, an organization found in an area prone to heavy rains buys flood insurance well before a flood damages the office building. For small businesses, cyberattacks are a matter of "when," not "if." Developing a cybersecurity plan beforehand ensures businesses aren't scrambling to stay alive after hackers breach a sensitive server or database.

Tips

Regularly update the contents of cybersecurity training

Cyber threats evolve at an unrelenting pace — making today's training materials already obsolete. Educational platforms should be routinely updated to include the latest threats, like the recently discovered VPNFilter malware, and should train users on how best to respond.

Adopt a multi-layered cyber defense plan

While antivirus software programs are a good first line of defense, sophisticated hackers will find always find a way to get past the front door. Small businesses can employ IT strategies like a "Defense in Depth," utilizing a combination of content filters, firewalls and a strong password policy to ensure hackers are met with resistance every step of the way.

Leverage third-party security experts

When disaster strikes, who does the small business employee turn to for help? For the resource-strapped company, a third-party security firm is a cost-effective way to both manage and address any questions regarding cybersecurity. In addition to removing uncertainty, third-party experts can also help small businesses stay ahead of the latest IT security threats with routine assessments and training.

Bad Behaviors Contribute to Small Business Cybersecurity Woes

Small to medium-sized businesses are hit with nearly 4,000 cyberattacks per day — and that number is only expected to grow. While small businesses can't influence the activities of criminals, they can take the steps necessary to address poor employee behaviors weakening organizations from within.

The problem? Despite paying lip service to cybersecurity, the actions of small business employees and leaders reveal little is actually being done to address the negligence towards security. Cybersecurity is complex — it requires a combination of both managing external factors while correcting internal behaviors. One such challenge plaguing small businesses is companies will focus on one issue over the other when both are needed to fully combat cyber risk.

Negligent employees remain the number one cause of data breaches at small businesses across America. Seemingly innocent actions, like connecting to a Wi-Fi hotspot at a coffee shop or hotel lobby, can cause some of the most damage to a small business. Hackers waiting in the wings can launch man-in-the-middle attacks or distribute malware when users connect to private servers over open networks. Another common mistake employees make involves how they handle their passwords. Writing down email passwords on sticky notes, for example, makes it easy for thieves to access otherwise secure accounts.

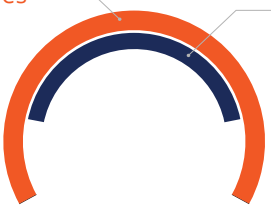
Modern cybersecurity is about managing, eliminating and mitigating risk wherever possible, and for small businesses that often means fixing bad internal behaviors. Whether intentional or not, employee habits can leave gaping vulnerabilities in a company's defenses that hackers are all too eager to exploit. In order to gain the level of resiliency needed to endure today's threats, small businesses should practice security fundamentals amongst their teams and consider outsourcing security management to third-party experts.

Top to Bottom, Bad Habits Are More Common Than You Think

Connecting to public Wi-Fi to do work

66%
SMB employees

44%
SMB leaders



Not activating multi-factor authentication

76%
SMB leaders have not activated MFA for their work email

69%
employees have not activated MFA for their work email

Sharing work email passwords with coworkers or assistants

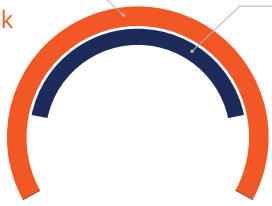
22%
SMB leaders share their password with a coworker or assistant

19%
employees share their password with a coworker or assistant

Using work computers to log into personal social media accounts

62%
employees use their work computers to access personal social media accounts

44%
managers use their work computers to access personal social media accounts



Tips

Establish a “bring your own device” (BYOD) policy

With employees using their personal devices for work, it can be difficult for small businesses to monitor who is accessing company files. One way to keep an eye on company access is for small businesses to establish a bring-your-own device policy, which dictates what work employees can do on their mobile devices. A BYOD policy can restrict associates from downloading work files to their personal computers or require employees to enable dual-factor authentication on their phone to access work email accounts.

Implement a content filter

Browsing the web doesn’t need to be outlawed at work, but employers do need to be careful about which sites their employees visit. By installing a content filter, companies can screen and block certain websites that are deemed inappropriate or harmful. Filtering software enables small businesses to control what content is viewed on their network and protects companies from sites carrying malicious payloads like malware, Trojan horses and spyware.

Protect remote workers with a VPN

What makes public Wi-Fi spots dangerous is anyone can hop on the same network and intercept traffic sent from an employee’s computer to a corporate server. As employees continue to work from remote locations and on unsecured networks, employers can enforce the use of a virtual private network (VPN) to keep prying eyes from spying on sensitive data transmissions. Small businesses should consider requiring employees to use a VPN whenever they work away from the office, providing another protective layer keeping hackers from breaching security protocols.

Enlist the help of managed IT security providers

Security continues to be an increasing challenge for small to mid-size businesses to handle on their own. A managed IT security services provider can offer features like dark web monitoring and deploy artificial intelligence solutions that proactively monitor for cyber threats. Third-party security experts can also provide monthly phishing exercises to eliminate vulnerabilities and compliance reports to help businesses determine which employees need additional security education.

Fixing Cybersecurity Gaps Starts with Improving Awareness and Asking for Help From the Experts

As companies begin to realize the immediate risk cybercriminals pose to their organizations, increasing education will be the key to strengthening SMB cybersecurity strategies.

Amongst all small businesses, confusion and uncertainty surrounding cyber risk is rampant. When it comes to reporting things like phishing schemes, employees are shown to be divided on how best to respond. Ideally, in the event of a security breach, employees should be able to shut down their accounts in a safe manner and immediately notify the appropriate personnel to handle the situation. More often than not, however, employees either don't know who to approach regarding threats or withhold information for fear of retribution.

Less than half
of Gen Zers know who to report a phishing scheme to

HR **20%** and Accounting/Finance **19%** are the least likely to know if their company has suffered a breach in the last 12 months

of employees don't even know if their company has an incident response plan in place

of SMB leaders don't know what a Clean Desk policy is

With the right balance of preventative measures and proactive education, small businesses can improve their cyber defenses and even thwart damaging threats. Above all, it's important for employers to remind employees they will not get in trouble for reporting a cyberattack, even if they were the cause of it. Everyone makes mistakes, and even the most tech-savvy employee is bound to have a misstep that results in an unintentional breach. By reassuring workers they won't be reprimanded for a cyberattack, small businesses will likely see the number of reported incidents rise, giving teams more time to respond to threats before they spiral out of control. **In an IT security crisis, every second counts.**

Businesses also can't address what they don't know — if cyber threats aren't treated as a priority by SMB leaders, then employees will also adopt a blasé attitude towards security. But it's difficult for small businesses to talk about cyber threats when they themselves aren't fully versed on all the cyberattacks used by criminals. Instead of trying to manage security on their own, small businesses can turn to a managed IT security services provider to protect them from digital threats. Awareness, education and subsequent training can help small businesses patch security vulnerabilities exploited by cybercriminals and prevent future attacks from occurring.

Conclusion

It's no surprise small businesses are struggling to keep up with the rapidly evolving cybersecurity landscape. Though they work with fewer resources compared to their enterprise counterparts, small businesses can no longer justify putting off investments in cybersecurity programs.

By increasing education and awareness and leaning on a service provider for proactive monitoring and response around cyber threats, small businesses can begin to improve their company's cyber hygiene habits and alleviate fears of a breach reaching the ears of customers. While it's important to install firewalls and filters to protect against internal threats, it's equally crucial for companies to strengthen resiliency among their employees. And small businesses don't have to embark on their cybersecurity journey alone. With the assistance of third-party security experts and buy-in from the top down, small businesses can meet today's security challenges head on and endure even the worst threats imaginable.

About Switchfast

Switchfast Technologies is an IT consulting and managed security services provider serving the Chicagoland area and small businesses since 2001. Switchfast offers everything from IT remote and onsite IT support to cybersecurity and cloud migrations, complete with a dedicated account team to handle small business technology.

Get in touch with the Switchfast team to learn how they can help your small business' IT and cybersecurity needs today.
773.241.3007 or TheFutureOfIT@switchfast.com

SWITCHFAST®