WHITE PAPER:

The Cybersecurity Survival Guide for Small- and Medium-Sized Businesses

Your company's data is squarely in the cross-hairs of criminals. While breaches of Fortune 500 organizations still capture the occasional headline, the number and severity of those attacks pale in comparison to those launched against small- and medium-sized businesses every day.

TeamLogicIT®
Your Technology Advisor

TeamLogicIT.com

Sixty-six percent of all organizations have been targeted with ransomware over the past year, according to a recent study[1], and experts suggest that many more go unreported. IT professionals stopped many of those attacks (around 20% by one estimate) before any company data could be encrypted and ransomed. The true numbers may never be known. With the stigma attached to cybersecurity issues in the business community, many organizations continue to remediate without disclosing these threats and attacks to the general public.

One well-founded fear is that news of an attack could damage a company's reputation and scare away current and prospective customers. The reluctance of many businesses to disclose those security breaches has been the driving force behind a growing number of government regulations and industry requirements that now necessitate organizations to report data breaches, including Sarbanes-Oxley, HIPAA (Health Insurance Portability and Accountability Act), and the EU standard, GDPR (General Data Protection Regulation).

One purpose of these rules is to notify the affected parties whose private information may have been compromised. Regulations such as HIPAA and Sarbanes-Oxley also provide a framework for protecting businesses from cybercriminals. Even though compliance can be a costly and never-ending headache for small businesses, especially for those with few IT resources, these rules have legitimate purposes.

The regulatory and cybersecurity concerns were rising fast enough for businesses even before the pandemic. As "non-essential" employees transitioned to remote or Work from Home (WFH) situations, with less than optimal network and data protection protocols, IT teams have been scrambling to triage potential issues and enhance system defenses.

With all the uncertainly, the list of cybersecurity-related issues that make owning an SMB a riskier proposition today. Without skilled professionals assessing the systems and addressing the problems, organizations can waste a lot of time and capital and still not meet their data protection objectives.

Failure is never a good option, especially in cybersecurity, yet it happens to an increasing number of companies every year. The trick is learning how to cushion the attacks and overcome the challenges. A proactive approach that combines managed IT services and risk awareness programs for employees is the perfect place to start. Businesses that put the time and effort into building and executing a comprehensive cybersecurity strategy, including those elements, are more likely to survive.

Cybercrime Is Big Business

Why would hackers and other troublemakers go after SMBs' data? The simple answer is that cybercrime has become a very rewarding vocation. Not just for the international syndicates that collect billions using highly automated tools, but for the kid down the street with a knowledge of computers. Businesses with minimal or outdated IT security systems are no match for a determined hacker.

Cybercriminals also see the continually expanding remote workforce as a major opportunity. Transitions related to the COVID-19 quarantine, when some businesses literally had just hours to

1. The State of Ransomware 2022, Sophos, https://news.sophos.com/en-us/2022/04/27/the-state-of-ransomware-2022/

move employees offsite and set up home offices, created a prime environment for cyberattacks. Even when organizations have more time to plan and implement remote work options for their employees, things can fall through the cracks, including IT oversight, security training, and electronics policies. Well designed and carefully executed remote work strategies help businesses secure their people (and their data).

The most valuable resource companies possess is the information they gather, store, and leverage to grow their business. That data is prized by others as well, and cybercriminals have access to a plethora of methods and tools designed to overcome even the most secure environments today.

The **costs associated with small business cybersecurity attacks** rise exponentially each year. Between **remediation and restoration charges, regulatory fines, damage to reputation, lost productivity and legal expenses**, breaches are putting massive holes in many companies' budgets. Factoring in productivity losses and reputational damage, cybersecurity issues could significantly impact the bottom line of most organizations.

Cyber Survival 101

The best defense for SMBs is to adopt a two-part network and data protection strategy. The first and most crucial step is to raise awareness. Do all employees, including the management team, understand the ongoing threats and their role in preventing data breaches? End-user education and training help ensure that workers understand their responsibilities, including following safe online practices and identifying and reporting potential cyber attacks.

Of course, awareness alone won't stop employees from making poor decisions. Another recent study found that **55% of U.S. workers surveyed admitted to taking a risky action in 2021.**[2] Experts blame that contradiction on everything from a "dangerous curiosity" to overwork and confusion. The rising quality and complexity of phishing email schemes are likely contributing to that latter point, as it continues to get more difficult to distinguish between good and suspect messages.

The second part of an effective cybersecurity strategy addresses those concerns. Businesses must proactively counter cybercriminal's plans of attack. Activities such as ongoing network and threat monitoring and other advanced security practices have proven quite effective at reducing data breaches and vulnerabilities.

Stopping cybercrime is never easy, or always successful, but with the right plan in place, every organization can improve its chances of survival.

Recognize the Risks

A critical first step in cybersecurity is ensuring everyone (employees, managers, and others with network access) has a firm understanding of the current threats. Numerous studies suggest that, despite all the news and information on breaches, people's actions are still the primary cause of most security incidences.

2. Proofpoint 2022 State of the Phish, https://www.proofpoint.com/us/newsroom/press-releases/proofpoints-2022-state-phish-report-reveals-email-based-attacks-dominated

In fact, a recent survey found that 52% of businesses think employees are their weakest link[3], putting their protection strategies at high risk. The need for education and training to counter those concerns has never been greater and the value of IT managed services continues to rise. With informed employees and remote monitoring solutions watching for irregularities and bad behavior in the networks, it's much easier for IT teams to locate, isolate and address potential threats.

Here are a few of the top trends everyone with access to corporate networks should become more familiar with:

RANSOMWARE

Bad Rabbit, WannaCry, and CryptoWall, and similar types of malware have become an effective weapon for cybercriminals, generating billions of dollars in ransom each year by targeting virtually everyone. No business is immune, no matter how big or small. These attacks typically start out deceiving users into downloading an e-mail attachment or clicking a link that then launches the malware, which can spread quickly throughout the network. Ransomware locks down files and workstations until the specified bitcoin ransom has been paid (following the instructions provided on the screen).

THE REAL-WORLD COST OF RANSOMWARE

An attack against the borough of Matanuska-Susitna, Alaska, forced employees to revert to old-school technologies, including typewriters, to keep things running until their systems could be restored.

The ransomware outbreak denied the municipality use of its computers, servers, telephone and security systems, and back-up data. Officials stated that some of their email files and other information were irretrievable.

The average cost of a ransomware attack, including rectifying it, is $1,400,000[4], and the average time to recover is one month. The amount demanded upfront by cybercriminals may appear to be small (less than $1000 in some cases), but the financial losses rise quickly.

Businesses must also factor in the costs associated with downtime and restoration services, as well as security upgrades to minimize the chances of future attacks. A single ransomware incident could financially devastate most organizations.

Don't be fooled by the news: hospitals and municipalities are not the only targets. Public entities often disclose cybercrimes and other security issues to keep citizens and stakeholders informed (in some cases, it's required). Businesses and other organizations often play by a different set of rules and are more likely to cover up, or at least not open to sharing details of ransomware attacks or breaches.

NETWORK ATTACKS

The lone wolf hacker may not be a thing of the past, but cybercriminals are becoming increasingly more organized in their actions. Nation state-supported groups (i.e., North Korea, China, Russia) and crime syndicates are reportedly behind many of these activities that target businesses and other organizations. Ransomware is not their only tool.

3. Kasperski, The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within, kaspersky.com/blog/the-human-factor-in-it-security/

4. The State of Ransomware 2022, Sophos, , https://news.sophos.com/en-us/2022/04/27/the-state-of-ransomware-2022/

The business community is ripe with opportunities for the "traditional hackers." Outdated protection measures and poor software patching/updating practices make it easy for cybercriminals to succeed using a variety of methods, including Distributed Denial of Service (DDoS) and Advanced Persistent Threats (APT), as well as password and insider attacks.

The motives behind these attacks range from gaining access to valuable data, such as credit card and personal information, to revenge for firing or inflicting damage to make up for perceived injustices. Businesses can thwart many of these crimes by implementing effective password management practices, monitoring network security, and performing required system updates.

GDPR: COMPLIANCE OF THE FUTURE

Some have suggested that the EU's General Data Protection Regulations extend too far, imposing potentially huge fines and the risk of class action law suits on third-country processors that don't comply. Organizations may also be held be liable for the actions of other entities where they transfer data.

Most compliance experts believe the opposite, that more GDPR-type rules are needed, and many states and federal regulators concur. In fact, several entities plan to adopt similar measures in the next few years to protect consumer data and compensate impacted individuals.

PHISHING

These attacks often begin with a legitimate-looking but fake email or social media message. Sadly, the imitation versions are becoming increasingly more difficult to detect with cybercriminals using the information gathered through data mining and other processes to mimic trusted senders. The correspondence may appear to be from the recipient's credit card company or a recruitment agency, encouraging the user to click a link or open a file that will install a malicious program on their computer.

Spear phishing goes a step further, with the senders imitating trusted individuals, often company executives or people with influence. The message may unleash malware that infects the corporate network, or it asks the recipients to reveal sensitive personal or business information. The third type of attack, whaling, specifically targets executives such as the CEO, CFO, or other high-level managers with access to their organizations' most sensitive data. The objectives and targets may differ, but the consequences of each can be just as costly.

SOCIAL ENGINEERING

As mentioned previously, people are the weakest link in cybersecurity. Social engineering plays off their vulnerabilities, using various techniques to manipulate individuals into giving up confidential information such as passwords and other sensitive data. The goal for cybercriminals targeting the business community is to get through the firewall and gain access to the treasure trove of data. These attacks are not limited to email phishing. Pretexting and baiting are methods criminals use to gain access to personal information using electronic communications such as IM (instant messaging) and social media to trick users into sharing login credentials or downloading malicious viruses.

REGULATORY COMPLIANCE

Cybersecurity plays a significant role in a growing list of government regulations and industry business standards. From small healthcare organizations and credit unions to restaurants and municipalities, virtually every organization is (or will soon be) required to protect their data using specifically

prescribed methodologies. Just as important, those organizations must prove the processes and systems used to collect, store, and secure that information work effectively.

Meeting each specific requirement can be tricky. Government regulations and industry standards change frequently, and the constant introduction of new data protection rules makes it hard for business owners to keep up. Violations can carry significant fines and other penalties, which is why most companies are investing more time and money in the development of their security strategies.

ROGUE AND SHADOW IT

Bringing non-approved technologies into a business can create havoc for the IT department. Un-tested devices and applications can compromise network security and data compliance and create an opening for skilled hackers. The practice falls into two categories, which often overlap.

1. **Rogue IT** is when employees connect personal smartphones, tablets, wearable technologies (i.e., fitness trackers, connected-watches), and other devices to the company network. The term also applies to the use of individual cloud services and applications in the workplace.

2. **Shadow IT** typically refers to technologies implemented or procured by individual departments that the company's IT team may not know about or support. While company executives may have approved of the application or device, if not adequately protected, it could compromise the organization's security, data retention policies, and workflow.

3. **Remote work environment** can elevate those risks. With less oversight, employees tend to follow company rules and electronics policies with less urgency and may feel less inhibited about uploading non-approved applications and connecting external accessories to their PCs and laptops.

BEWARE OF CYBER OPPORTUNISTS

National or regional emergencies may not only threatened lives, homes, and businesses, but those situations are often used to launch new cybersecurity attacks. In times of uncertainty or trouble, people want information and will often skip security protocols when something strikes their interest. For example, the COVID-19 pandemic inspired cybercriminals to launch numerous phishing attack with email subject lines promising details on the disease, testing locations, government stimulus programs and other related "hot" topics.

Natural disasters such as floods, tornadoes, and wildfires often motivate scammers to create similar attacks. Those email messages typically include a link or an attachment that launches malware or ransomware or asks the recipient for personal or company information. The goal for cybercriminals is either to extract valuable data that can be sold on the dark web or to receive a bitcoin ransom for releasing encrypted files.

INTERNAL THREATS

In a recent study, **53% of businesses reported having experienced an insider cybersecurity attack in the previous 12 months.**[5] Employee misuse of computer systems is a serious concern for SMBs. Some attacks are intentional, while others are the result of carelessness and poor security practices.

5. Cybersecurity Insiders Insider Threat Report, https://www.cybersecurity-insiders.com/portfolio/insider-threat-report/

For example, some staff members may think nothing about forwarding confidential information to their personal (unprotected) email accounts to finish work projects at home. Another danger is managers with full system access leaving their workstations unattended without logging out. Simple mistakes can have devastating consequences.

Reduce the Risks

Understanding the cybersecurity threats is just the first step. That knowledge helps business leaders prioritize their risk abatement projects and evaluate options. In many cases, the list of vulnerabilities and potential issues is quite long and requires a mix of short and long-term strategies to resolve effectively.

Companies that manage sensitive data and fall under certain regulatory requirements might need additional protections, as could those with significant downtime costs and other mitigating risk factors. No matter how big the business, evaluation and prioritization can be complicated. However, experienced IT security professionals who understand these processes tend to focus on these four key areas:

1. Assess the Current Environment

Before making a single recommendation or change, a skilled cybersecurity professional should always evaluate the current situation. What devices are sitting on the corporate network? Which technologies are protecting the IT infrastructure? Who has access to which systems?

Cybersecurity assessments should never be a "one and done" activity. A company's IT environment changes daily, with applications, devices, and users constantly added; increasing the number of endpoints to protect. As companies transition to flexible workspaces or remote work, the number of systems the IT team has to secure and manage can grow exponentially, which can increase the need for monitoring applications and protection tools.

Of course, some of the latest technologies carry their own threats. With lax security protocols and few industry standards for innovations such as the Internet of Things (IoT), drones, and 3-D printers, additional protection measures may be needed.

2. Address System Vulnerabilities

Network assessments identify potential cybersecurity issues. The information they gather helps IT professionals spot troubling issue and vulnerabilities, set priorities for future projects, and develop long-term data protection plans. Common post-assessment activities include:

- Installing patches and updates
- Ensuring backup and disaster recovery solutions are fully operational
- Developing improvement plans: set investment priorities, schedules, and budgets

3. Focus on the "People Problem"

Humans are the wild card when it comes to cybersecurity. There are too many tales of companies getting hacked after investing thousands implementing cutting-edge network and data protection systems because a worker used poor password management techniques.

No business can fully prepare for the mistakes and intentional misdeeds of its employees, but there are a few best practices that can minimize the results of their actions. These are some of the offensive cybersecurity actions companies should implement to reduce their risks:

- **Create and strengthen security policies:** If the rules are not in writing, they don't exist. What good are best practices if no one understands the directions or their specific responsibilities? Each policy must be clearly written, with detailed explanations and step-by-step directives for each process; from password management to reporting a suspected breach or cybersecurity problem.

- **Implement awareness training programs:** Cybersecurity education helps companies keep pace with the changing threat landscape. Employees who understand how social engineering schemes work and know the value of proper password management and data protection schemes are more likely to adhere to company policies—and minimize the risk of potentially catastrophic mistakes.

- **Watch for anomalies:** Everyone should be on the alert. IT teams should be looking for irregularities in network traffic and email systems, as well as abnormal computer usage and odd employee behavior. Trust is crucial, but with the increasing threats, companies must be more proactive if they wish to keep cybercriminals at bay.

4. Monitor and Validate

No matter how strong a company's data protection strategy seems, with enough time and resources, a skilled hacker will find a way around those defenses. Businesses can minimize those threats and limit cybercriminals access to valued information by proactively monitoring network activity, noting potential issues, and responding promptly when an attack is underway.

A proactive cybersecurity approach reduces the windows of opportunity for hackers and malware. Effective monitoring and detection services (those typically included with a managed IT service) will identify and quarantine suspected issues and limit access to protect critical information systems.

Verification is essential. The best-designed systems and procedures must still be tested regularly to account for changes in personnel, applications, and equipment. That validation process is mandatory for companies that adhere to regulations such as PCI, Sarbanes–Oxley, HIPAA, and GDPR.

With cybercriminals employing complex tools and highly deceptive practices, IT professionals must counter those threats with more comprehensive assessments, including penetration (pen) testing and dark web scans. The first process, commonly referred to as "ethical hacking," is an authorized simulated attack on a company's technology systems to evaluate the effectiveness of the tools, processes, and people charged with keeping them secure. This procedure identifies vulnerabilities and strengths and typically includes detailed recommendations, such as any changes the company needs to make to comply with mandatory regulations and standards.

Dark-web scans (and monitoring) looks for sensitive company information in the hidden areas of the Internet. Stolen passwords, credit card and social security numbers, and a host of other "private" information is sold on these sites, intentionally hidden from search engines and authorities, and only accessible through special browsers.

The validation part of cybersecurity is best left to a neutral third-party. With the complexity of the threats and the potential costs of a single failure rapidly escalating, the perspective (and approval) of unbiased professionals is invaluable. Those occasional "checks and balances" help companies ensure their security investments are effective and reduce the risk of fines, lawsuits, and other liabilities.

Conclusion

There are no surefire guarantees with cybersecurity. As the workplace continues to evolve, with WFH and flexible office options, businesses have to adapt their network and data protection capabilities to meet the shifting threats.

However, by following established best practices and implementing proven managed IT services, organizations can reduce their legal and financial exposure and protect the best interests of their employees, customers, and other stakeholders.

Data protection is a commitment. It's also a potential point of failure for today's businesses, and those who experience breaches and other significant lapses often find it harder to hire, borrow capital, and attract new clients.

To that point, advanced cybersecurity services are no longer an option for the SMB. Between the increasing complexities of protecting businesses from the most devious cybercriminals, to the demands of securing a remote workforce, robust defenses are mission critical today. Data protection has evolved from a one-time product purchase or service contract that was implemented and forgotten to a 24-hour-a-day commitment requiring the support of experienced and knowledgeable professionals.

IT services providers with strong cybersecurity skills play an invaluable role in that process for the small and mid-size business community. After all, proactive support is the heart of the managed services value proposition. Network and data protection, including periodic assessments and monitoring, is a natural extension of that support.

Businesses can expect to face an ever-increasing number of threats and compliance requirements in the coming years. As if dealing with a global pandemic was not enough, the community continues to face a severe shortage of IT security professionals, so managing the risks without outside assistance will not be easy. Fortunately, high quality support is available. With a multitude of firewall and endpoint management solutions, and a litany of advanced cybersecurity offerings, IT services providers are equipped to handle all those challenges. From assessing the risks and infrastructure to designing data protection systems, processes, and policies; they deliver the support small businesses need to survive today's (and tomorrow's) cyber offensive.

For help with your technology, contact your local TeamLogic IT office.

TeamLogic IT is a national provider of advanced IT management services for businesses. With locations across the U.S. and Canada, TeamLogic IT provides managed services, computer consulting and support services focused on helping companies minimize downtime and improve productivity. TeamLogic IT helps businesses compete better through the effective use of information technology.