"... SMBs might be even more at risk because many of them lack the necessary resources to effectively defend themselves."

Introduction

It seems you can hardly go a day without seeing another headline concerning the latest cybersecurity incident somewhere in the world. And most of those stories focus on large global organizations with thousands of employees, multiple data centers and networks, dozens of offices or other facilities, and perhaps millions of customers.

That fact, however, tends to mask the risk facing nearly ALL organizations or any size, as it perpetuates the misconception that cyber-criminals are focused solely on large enterprises. For small and medium-sized businesses (SMBs), believing that to be true could be a potentially fatal error. Companies of all sizes and in every industry are vulnerable to cybersecurity threats, and they face many of the same risks as larger enterprises. In fact, SMBs might be even more at risk because many of them lack the necessary resources to effectively defend themselves.

Despite the size of the organization, all of them possess valuable data (e.g. trade secrets, customer transaction records, intellectual property, etc.) and that data can be a potential target for cybercriminals. Some organizations in "niche" industries ... particularly those working on innovative new technologies ... might manage the exact type of information that some hackers are looking to steal.

And it's not just about data loss, as an equally impactful risk is losing access to systems, networks, and data as a result of an attack. Such downtime, even for a few hours, can have a significant impact on a company. That's especially true if the company does most of its business online.

In general, SMBs are subject to the same kinds of cybersecurity threats that larger businesses face. Similarly, they are also vulnerable to data loss from ineffectual backups. Additionally, it's worth noting that the potential damage from a cyber-attack extends beyond security and systems availability issues, as many SMBs need to be compliant with a number of data privacy regulations ... and failure to do so can result in steep and crippling fines.

This white paper examines some of the key risks small and mid-sized businesses face today and why they need to address them. It also presents some best practices for bolstering security and recovery capabilities.

"No organization is too small to be a target."

The Fallacy of Immunity

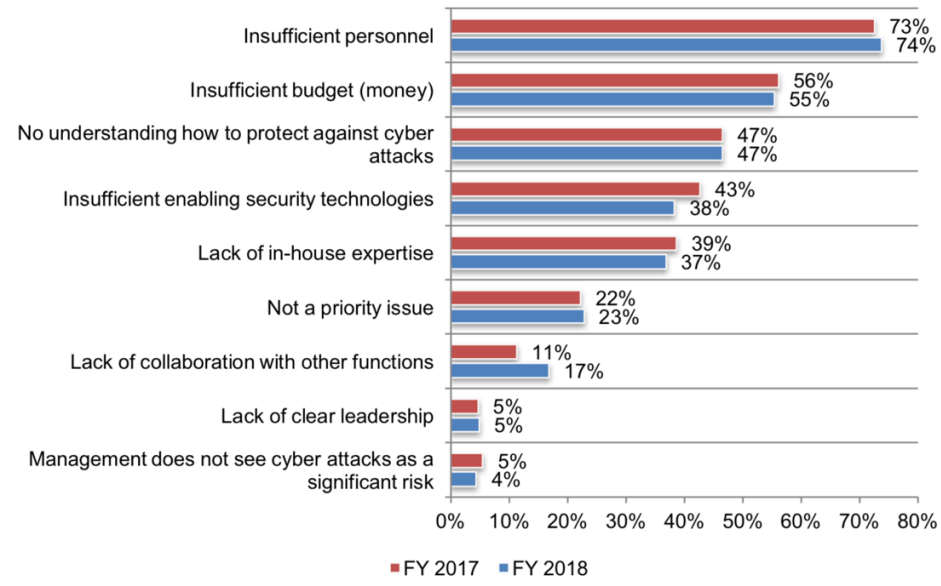
Many SMBs see themselves as flying under the radar as far as security threats are concerned. They view cyber-attacks and other cyber-criminal activities as being designed for large enterprises that have large IT infrastructures, numerous entry points, and a virtual treasure trove of valuable data to steal.

The fact is, however, that is simply not the case. Small and mid-sized businesses have a wealth of data resources that attackers would like to get their hands-on, and the reality is that they are aggressively going after these companies. No organization is too small to be a target.

A 2018 study by research firm The Ponemon Institute showed that small businesses increasingly face the same cybersecurity risks as larger ones, but only a minority of those same businesses would rate their ability to mitigate threats, vulnerabilities, and attacks as "highly effective."

The institute surveyed about 1,000 Information Technology and IT security practitioners from companies in the United States and United Kingdom with headcounts ranging from 100 to 1,000 and found that 67% said they had experienced a cyber-attack in the previous 12 months. Despite this, nearly half of the respondents (47%) said they have no understanding of how to protect their companies against cyber-attacks.

Figure 13. What challenges keep your IT security posture from being fully effective?
Three choices allowed



Source: Ponemon Institute/Keeper Security

"Unlike a lot of larger enterprises, SMBs typically have limited resources for protecting their networks, systems, applications, and data."

The Biggest Security Threats

As we have already established, SMBs are subject to the same security threats as their larger counterparts. The following represents a summary of some of the most prominent types:

1. **Viruses and Other Malware ...** This is software designed to cause damage to networks, servers, desktop computers, mobile devices, and other client systems. The damage is inflicted once malware is introduced into a target's environment. Common types of malware include viruses, worms, Trojan horses, spyware, and adware, and each can do significant damage to SMBs.

2. **Ransomware ...** This is a specific type of malware that deserves its own description because it has become so insidious. Ransomware might threaten to expose a victim company's data, shut down systems or block access to them, or encrypt files unless the company pays a ransom using Bitcoin or other difficult-to-trace cryptocurrencies. Ransomware attacks, which are aimed at all types of companies, are generally carried out via a Trojan disguised as a legitimate file downloaded by a user.

3. **Phishing ...** Using phishing tactics, attackers try to gain access to sensitive data such as credit card numbers, social security numbers, usernames, passwords, and other information. They do this by disguising themselves as trustworthy entities, often through emails or instant messages sent to employees in a company. Oftentimes users are instructed to enter personal information at a fake Web site that appears legitimate. Variants include spear phishing, which are attacks aimed at specific individuals or organizations; and whaling, which are spear-phishing attacks directed toward senior executives and other high-profile targets.

4. **Distributed Denial-of-Service (DDoS) ...** These types of attacks can be among the most damaging because they can shut down vital servers. DoS typically involves an attacker overloading a target system with requests, rendering it unavailable to users. A DDoS attack is similar in nature, however the incoming traffic flooding the network originates from multiple sources, making it far more difficult to stop.

5. **Botnets ...** These are any number of Internet-connected devices, each running one or more bots, which can be used to perform DDoS attacks, steal data, and allows attackers to access the devices and their connections. Attackers can control botnets using command and control software. Many recent botnets rely on existing peer-to-peer networks to communicate.

6. **Advanced Persistent Threat (APT) ...** With an APT, an attacker quietly gains unauthorized access to a company's network and remains undetected for an extended period of time. The goal might be to steal data, cause damage, disrupt systems or perform some other malicious act. Typically, attackers have access to intelligence-gathering techniques and prioritize a specific task, such as data theft.

7. **Drive-By-Downloads ...** These incidents can happen when users visit Web sites or open email attachments and unknowingly download malware or other unwanted software. In some cases, malicious content on a site might be able to exploit vulnerabilities in a user's browser to run malicious code.

8. **Insider threats ...** Any malicious threat that comes from employees, former employees, contractors, or others working within a company is an insider threat. These people generally leverage inside information about security tools and systems to inflict damage or steal or delete data. These types of threats can come from malicious insiders, negligence, or external parties who gain access credentials without authorization.

In addition to those specific threats, SMBs are vulnerable to data loss from ineffectual backups. If data is not backed up adequately and there's an attack or other incident that renders data unavailable, users can be without access to the information or it might be lost or damaged permanently.

Again, it is worth noting that many SMBs need to be compliant with a variety of regulations pertaining to data privacy. Failure to safeguard systems and data effectively can lead to fines. Adding to the complexity of the compliance challenge, the number of data protection regulations is on the rise.

Unlike a lot of larger enterprises, SMBs typically have limited resources for protecting their networks, systems, applications, and data. Many lack formal cybersecurity programs or an executive dedicated to security. Given the ongoing shortage of security professionals, acquiring the needed skills is a big challenge.

"Many SMBs simply don't have the internal resources or budgets to create and maintain a robust cybersecurity program ... That's why it's a good idea to consider bringing in expert help from the outside."

Best Practices for Strong Security and Backup

What are the most important things small and mid-sized businesses can do to protect their networks, systems, and data from cybersecurity issues and/or data loss? The following represents some recommended best practices ...

Deploy the solutions needed to protect and backup data:

- SMBs need to be willing to invest in tools that can boost security and reduce risks. This includes platforms that automatically and continually monitor files across internal systems and the cloud.
- A backup and recovery solution should be designed to rapidly recover lost, deleted, and ransomed files. Administrators should be able to retrieve actual file contents so that they can determine whether a file contains sensitive data during investigations; recover prior file versions and deleted files; and (ideally) provide self-service so that users can recover from everyday data loss events.

Practice good security maintenance:

- Cybersecurity is not a "set-it-and-forget-it" proposition. New threats and vulnerabilities are constantly emerging. Companies need to regularly update and patch operating systems and other software resources and instruct users to change passwords on a regular basis.
- They also must maintain and update security tools such as firewalls, intrusion detection systems, and anti-virus software as needed. Good security maintenance also includes conducting periodic and comprehensive risk assessments, taking into account any situations that might have changed since the last assessment, such as the addition of new cloud services.
- One good way to stay on top of the latest threats and vulnerabilities is by subscribing to threat intelligence services and following (verifiable) experts on social media.

Establish and enforce security policies and procedures.

- Security is also not just about tools and services; management needs to create and enforce policies to ensure that employees, contractors, and partners are practicing good security hygiene.
- The policies should cover areas such as the need to create strong passwords and revise them on a regular basis; how, where and by whom sensitive data (e.g. customer information, trade secrets, etc.) can be used; when to remove sensitive data files from systems; the proper and safe use of mobile devices; how and when to use data encryption; and how social media and other online sites should be used.

- In addition, security policies should cover what steps IT staff, managers, and employees who are leaving the company should and should not do to ensure strong security and data protection. They should also provide detailed instructions on what should be done in the event of a cyber-attack or data breach.

Provide employee education and training:

- One of the most important things executives at SMBs need to do when it comes to cybersecurity is educating their employees—and themselves—about the potential risks and how to go about mitigating them.
- They should provide mandatory training programs for all new employees and refresher courses for the existing workforce. Among possible topics to cover are how to avoid phishing and spear-phishing scams, how to practice good password usage and management, how to spot potentially harmful links and downloads, best practices when using public wi-fi, the proper use of mobile devices in the workplace, and social media behavior.
- Many insider threats due to user negligence can be avoided with proper training and retraining. Senior executives can set a good example by promoting their importance to the organization and participating in these training programs themselves.

Evaluate the security posture of external partners.

- Today's business environment is more complex than ever, with companies typically engaging multiple suppliers, service providers, equipment vendors, consultants, and others. Ensuring that those outside entities are working in a secure manner is vital to the overall security of the company.
- SMBs should not be afraid to inquire about the steps their partners are taking to ensure strong security and data backup.

Hire outside experts for help:

- Many SMBs simply don't have the internal resources or budgets to create and maintain a robust cybersecurity program. Even many larger companies struggle to do this. That's why it's a good idea to consider bringing in expert help from outside.
- Utilizing a contracted vCISO (virtual Chief Information Security Officer), as offered by **CISO ToGo, LLC**, can provide help to identify and select affordable tools/services, develop effective policies appropriate for your business, and design/implement a technology risk management program to protect the various aspects of your business.

Source: HelpNetSecurty.com

"... security needs to be a priority for every organization – including start-ups and mid-sized businesses ..."

More Than Shiny Gadgets

As stated in the previous section, security is not just about tools and services ... management needs to create and enforce policies and procedures to ensure that everyone is practicing good security hygiene. Information security needs to be a high priority for every organization – including small start-ups and mid-sized businesses looking to expand – and it is a shared responsibility that must be "owned" by every employee at every level of the organization.

To get a sense of how important data protection has become, consider that a growing number of boards of directors and C-suite executives are now weighing in on security issues. Furthermore, companies, in general, are investing more in security tools and services.

SMBs can't afford to operate with lax security. In addition to data loss and systems downtime, they can experience a decline in brand reputation, a loss of customers, a rise in legal fees and regulatory fines, and other negative impacts.

For those companies that have not developed a strong security strategy and infrastructure, the time is now ... **and this is where CISO ToGo, LLC can help!** If you'd like to discuss exactly how we can help, get in touch or visit us at:

www.CISO-ToGo.com

Email: WRichmond@CISO-ToGo.com

Phone: 401-264-0880

CISO ToGo
Technology Risk Consulting

... because security is everyone's concern, but it's OUR business!