TREND MICRO™

New Cybersecurity Challenges in Managing Risk

Introduction

As entrepreneurship exploded in the U.S. in the late 1990s, so did small business owners' dependence on the internet. But along with the wealth of information and tools the internet has brought us, it has also brought challenges.

The available data, its numerous applications, and the increasing use of the internet provided enormous opportunities for business owners and cybercriminals. As a result, small businesses are now more vulnerable to cybersecurity risks, including data breaches, malware, cyberattacks and more. In 2022, Trend Micro detected and blocked 146.4 billion threats, "a staggering 55.3% increase" from the number of threats in 2021.

In this e-Guide, we'll explore the cybersecurity challenges small business owners face daily running their companies and some solutions to help overcome them.

Why is it so difficult to understand and manage risk?

The risk of cyberattacks is particularly tough for small businesses to manage because they have fewer resources, including skilled tech personnel and the money to invest in understanding and managing cyberthreats.

In addition, because so many workplaces are now scattered, with employees working in the office and at home (or often both), the risks are also spread out.

Top Challenges of Managing Risk

1) Too many alerts
2) Limited visibility due to silos of data
3) Too many tools and vendors
4) Compliance pressures
5) Not enough resources

Stronger Security Measures

All this exposure increases the need for more robust security measures, including solutions like firewalls, antivirus software and encryption technologies. It's critical for small businesses to protect their vulnerable attack surfaces, including their server, cloud services, email and network security.

WFH Challenges

The COVID-19 pandemic drove many businesses home for months and months. This opened up new risk areas since home internet networks rarely have the same levels of security as those in offices, even in businesses that require VPN (virtual private network) usage.

Specifically, the challenges of working from home include the following:

- An increase in the number of vulnerable access points, with few, if any, protections
- Employees are isolated from the tech team and don't have the fundamental knowledge to recognize or manage cyberattacks
- Reluctance in using MFA (Multi-Factor Authentication)
- Failing to use the VPN
- Everyone, from the owner to the staff, is unaware of the risks and subsequent dangers of cyberattacks

From the company's perspective, the challenges include the following:

- The surge of remote working
- Expansion, including adding more virtual employees scattered across the country or opening new facilities
- The large and growing volume of data generated by the business
- Inability to implement strategic planning
- Reliance on tactical solutions that aren't integrated into other solutions

Social Engineering—The Human Factors

Many small business owners also aren't aware of the dangers social engineering presents in a business environment. Wikipedia explains, "In the context of information security [businesses], social engineering is the psychological manipulation of people into performing actions or divulging confidential information."

Essentially, social engineering is about the human factor in cybersecurity. Without sounding too hyperbolic, the adversaries small businesses face include:

- State actors
- Organized criminals and hackers who appear to be "trusted sources" using various techniques, such as
  - Phishing: Hackers trick people into revealing confidential information.
  - Baiting: Hackers persuade people to click on links, open attachments or download walmare.
  - Impersonating: Hackers pretend to be someone else to gain confidential information or account access.

These scams take various forms, including fake donation requests, offers of technical support, email purportedly from friends and family urgently requesting help, prize winner announcements, etc. Employees are particularly vulnerable to these schemes. Acting on that knowledge, most business email compromise threats target victims in America.

Because these scams appear real, unwitting employees click on them, inadvertently inviting malware into the business's network. These attacks can crop up via the web, online files, emails, the cloud, networks, endpoint devices and more.

Other Cyber Challenges

Rethinking Tactics reports a troubling trend—an increase in incomplete or faulty patches. Patches are software and operation system (OS) updates that address security vulnerabilities within a program or product. Bad patches happen for several reasons but are most likely due to businesses not having the resources, expertise or time to create the comprehensive solutions needed to fix the problem.

There are four attack techniques to be aware of:

1. Remote Services: Hackers may use valid accounts to log into a service designed to accept remote connections and perform actions as the logged-on user.

2. Valid Accounts: Hackers may obtain and abuse credentials of existing accounts to gain initial access and bypass access network controls to access data.

3. OS Credential Dumping: Hackers may attempt to dump credentials to obtain account login and credential passwords to access restricted information.

4. HTML Smuggling: Hackers use email to gain access via a malicious HTML file attachment. When opened, the file loads malware into the system, which can disable a company's web pages and applications, severely limiting its ability to communicate and do business with its customers.

Small Business Vulnerability

Do not make the mistake of assuming your business is too small for cybercriminals and hackers. Nothing could be further from the truth. The predatory nature of cybercrime means malicious actors specifically target organizations or technologies perceived as highly vulnerable and lucrative.

Last year, we saw ransomware actors increasingly target small and midsized businesses. Unfortunately, these smaller companies can be held hostage when faced with cyberthreats since they have fewer IT security resources to help avoid or respond to complex attacks. In fact, small businesses (those with 200 employees or less) were victims of more ransomware attacks in 2022 (1,213) than medium-sized and large businesses put together (1,154).

Solutions: Privacy Acts

Solutions to some cyber challenges have already been addressed by implementing privacy compliance regulations, such as the California Consumer Privacy Act (CCPA), a state-wide data privacy law regulating how organizations handle the personal information of California residents. This applies to anyone doing business in California. Failure to comply with these regulations can result in significant fines and other legal consequences.

Solutions: Cyber Hygiene

It is critical for small businesses to educate their employees about the numerous cyberthreats they face and how adopting new cyber-hygiene habits can help prevent cyberattacks. This is especially important today since cybercriminals, using social engineering techniques, can more easily bypass existing cyber-protection programs. And since so many U.S. employees still work remotely, whether part- or full-time, these workers also need to educate their families.

Here are some cyber-hygiene recommendations to increase cybersecurity awareness in small businesses:

- **Require employees to use strong and unique passwords for all their accounts, personal and business.**
- **Provide password management tools to employees to help them manage their accounts.**
- **Require employees to change their passwords every six months.**
- **Educate your staff about phishing and social engineering scams. Show them examples of what to look for.**
- **Establish a point of contact whom employees can call in case they fall for one of these schemes.**
- **Require MFA (Multi-Factor Authentication), also called 2FA (Two-Factor Authentication)**
- **Install robust cybersecurity measures in your stores, restaurants, offices, and at your and your employees' homes.**
- **Beware of misinformation by using a cybersecurity tool or service.**
- **Your company's vulnerability is heightened when you or your employees are traveling. So be sure to take extra precautions when on the road. Even taking a laptop to a coffee shop can leave your data vulnerable, so be cautious anytime you or your team are out of the office.**
- **Remind everyone, "Think before you click!"**

Solutions: Security

The risk to businesses from cybercrime is heightened because the threat actors are leaning into more legitimate business tactics. Unfortunately, cybercriminals are innovating with the tools they use and the targets they choose. And they're building resilient organizations that can exploit multiple areas of attack surfaces in a single campaign.

Because most small companies don't have the skilled personnel to defend the business from cybercrimes, they need a comprehensive solution that manages the entire attack surface. Here are some security practices companies can institute to stay safe:

ASSET MANAGEMENT: Examine your assets and determine their critical importance, potential vulnerabilities, the level of threat activity, and how much threat intelligence is being gathered from the asset.

CLOUD SECURITY SETUPS: Ensure that the cloud infrastructure is set up with security in mind to prevent attackers from capitalizing on known gaps and vulnerabilities.

PROPER SECURITY PROTOCOLS: Prioritize updating software as soon as possible to minimize exploitation of vulnerabilities. Options such as virtual patching can help businesses while vendors provide their security updates.

ATTACK SURFACE VISIBILITY: Monitor the different technologies and networks within your businesses and any security systems that protect them. It may be difficult to correlate the different data points from siloed sources.

Be Alert

There is a bright note—awareness of cybersecurity risks seems to be rising among many small business owners. Hopefully, this will drive them to take advantage of innovative new technologies and strategies and be more proactive about protecting their companies from cyber threats.

For more information

For more information about cybersecurity and online best practices, visit trendmicro.com. To get help with your business, including security needs, reach out to a SCORE mentor or other SCORE resources.