TREND MICRO

Securing Your Small Business Online

Mitchel Chang

Senior Vice President, CSR and Education

Digital transformation is shifting the business landscape and impacting lives in ways we couldn't have imagined. Its wave has resulted in process automation, operational agility, reduced costs, and predictable growth across different industries. World Economic Forum refers to this transformation as "Industry 4.0", the 4th industrial revolution.

Technological advancements, such as cloud computing, internet-of-things (IoT), big data, machine learning, and artificial intelligence (AI), are at the forefront of this revolution, reducing outages, delivering cost savings, ensuring faster development and improving productivity. For example, the medical industry uses digital tools to diagnose, manage, and treat health conditions.

> "the 4th industrial revolution
>
> WORLD ECONOMIC FORUM

While digital transformation offers many benefits, it also comes with many challenges. For instance, investing in technology also increases cybersecurity risks. AI and machine learning have been known to potentially increase the attack surface for hackers, while big data and the cloud hold lots of information, which can pose a considerable risk in the wrong hands.

Investing in technology to support your business growth and gain a competitive edge is highly advisable as a small business owner. However, you must monitor cybersecurity trends to protect your business from potential breaches and attacks while harnessing the full potential of digital transformation. Here are trends you should pay attention to:

1. Attacks are Getting Sophisticated

As noted, advancement in technology also increases cybersecurity risk. Like businesses, hackers are also constantly searching for the best technologies and techniques to leverage in their craft. Cyberhacking is a multibillion-dollar enterprise, complete with R&D budgets; thus, hackers invest in advanced tools and processes to penetrate systems.

Today, hackers use machine learning, AI, and other technologies to launch sophisticated attacks. These technologies enable them to expedite attacks – from weeks to days. For example, Emotet, a malware program that targets banks, is believed to be capable of changing the nature of attacks. It can leverage AI and machine learning to automate attacks and send out contextualized phishing emails.

Other capabilities and technologies have also advanced over the years. For example, ransomware attacks have doubled since 2019, thanks to factors like ransomware as a service (RaaS) and cryptocurrencies, which have reduced the cost of launching attacks. These attacks are a growing pain for more than 50% of cyber leaders, and 80% believe that ransomware attacks are a significant threat to public safety.

The number of Remote Desktop Protocol and internet attacks has also grown, and 2022 already has record numbers of attacks.

2. Mobile is the New Target

The increased use of smartphones and tablets has made them potential prospects for hackers. Today, mobile devices hold lots of information and can be connected to your company's network at any time – this makes them prime targets for attackers.

Since mobile devices have software and internet access, they have security threats, such as data leakage, unsecured Wi-Fi, phishing or smishing attacks, spyware, spoofing, and SPAM. For instance, in 2020, every organization experienced at least one mobile malware attack, according to a report by Check Point.

Also, about 46% of organizations had at least one employee download a mobile app that threatened their systems and networks. Mobile devices are desirable to APT groups and actors, such as Rampant Kitten, which has previously targeted mobile users using an elaborate and sophisticated campaign.

3. Cloud is Potentially Vulnerable

Cloud computing is quite effective and efficient in delivering different services via the internet. It facilitates the on-demand availability of resources, such as servers, files, and applications, to support business operations in various ways.

However, the cloud can be vulnerable to flaws or weaknesses in a cloud environment, which attackers can exploit. The impact can even be worse for companies that count on a single cloud deployment for their business needs. Multi-cloud environments also add security and complexity challenges due to a lack of visibility and control. Therefore, businesses must now consider additional cloud cybersecurity protection tools and robust access control such as multi-factor authentication.

Between 2018 and 2019, up to 33 billion business records were exposed due to poor cloud security implementation. Also, up to 68% of organizations believe that cloud account takeovers pose a considerable risk to their operations. While the cloud has different benefits, its success hinges on secure implementation and use.

33 billion

business records were exposed between 2018 and 2019

SECURITY MAGAZINE

4. Misinformation/SCAM is Sill Rampant

In 2021, the Federal Trade Commission received fraud reports from over 2.8 million consumers. Imposter scams accounted for the majority of cases, and consumers lost $5.8 billion to fraud that year, representing a 70-percent increase from 2020.

This information highlights the prevalence of scams and how attackers can use them to exploit unsuspecting users to share valuable information or send money to bad actors. For example, an attacker can email or call your employee in the disguise of tech support, gov't agency, or bank support. They can then use the information to access your system and accounts.

In 2020, businesses filed 241,342 complaints of phishing scams, which cost them $54 million in losses. Scams targeting small businesses take different forms, including fake invoices, unordered office supplies or other products, directory listing scams, utility company imposters, business coaching scams, and counterfeit checks.

5. Remote Working has Risks

Working remotely is convenient, but the risk posed by employees is two-fold. Companies cannot control how their files and systems are used with employees working from home. Other factors, such as unattended computers and unsecured Wi-Fi connections, aggravate the risk when working remotely.

A survey by OpenVPN revealed that up to 90% of IT professionals believe that remote workers are not secure. Also, about 70% believe remote workers pose a higher security risk than onsite workers. This assertion shouldn't be taken lightly today, given that the lines between home and work are increasingly blurred.

A report by HP showed that about 30% of workers admitted to sharing their work devices, while 70% noted that they used the devices for personal tasks, too. Such behaviors pose a huge risk, particularly when roughly 71% of employees say they access company data more frequently while working at home.

Remote working has benefits and can be quite effective in improving employee productivity. However, hackers are taking note of these shifting patterns to improve their phishing and spam campaigns.

90%

Unsecured Remote Workers

An OpenVPN survey revealed that up to 90% of remote workers are not secure.

71%

Workers access Company Data

Workers say they access company data more frequently working at home.

30%

Remote Device Sharing

Remote workers admitted to sharing their work devices with others .

70%

Work Device for Personal

HP employees noted using their work device for personal uses.

6. Social Engineering, Human Factor

Social engineering is the preferred method for soliciting information by attackers – it's effective, and that's why up to 98% of cyber attacks rely on social engineering to penetrate systems. It's an effective strategy that can manipulate an elementary school student, a company's CEO, or even a seasoned IT professional.

It has even become relatively easy for attackers to implement this technique with increased social media platforms. To target users, they use blended attacks, such as spear-phishing, business email compromise, and deep-fake. Other attacks include quid pro quo, tailgating, pretexting, and baiting.

How to Protect Your Businesses

In the wake of heightened cyberattacks, small businesses must take cybersecurity seriously. The COVID-19 pandemic led to a spike in cybercrimes by up to 600%, with attackers exploiting the crisis to target more users. In 2020, up to 667 million new malware detections were recorded, and this trend is not expected to slow down anytime soon.

The cyber threat is real, but the available resources needed to protect businesses are far fewer. Still, there are essential steps you can take to reduce your cyberattack risk and prevent attacks.

1. Develop a Risk Management Plan

It's always advisable to prepare for the unexpected and inevitable, even if you have invested in advanced security systems. Being prepared means having a risk or incident management plan. Most organizations have this plan but are yet to test it – you shouldn't wait for your organization to be attacked to test it. A good plan should help you answer these questions:

- Which parties will you need to engage?
- How will your team respond in the event of an attack?
- How will your operational and communication teams react?
- How will teams work together to remediate the problem?
- What steps will be taken following an attack?
- How will your organization inform your partners, customers, and investors?

Knowing the answers to these questions will allow you to address the impact of an attack and bounce back quickly. You'll need to test and simulate different scenarios to answer these questions and gauge your cybersecurity preparedness. Tests and simulations should involve the technology and the people responding to incidents. National Institute Standards and Technology (NIST) has published a cybersecurity framework that consists of the following five major cybersecurity risk management steps:

A) Identify

B) Protect

C) Detect

D) Respond

E) Recover

A business may leverage this NIST Cybersecurity Framework to devise its cybersecurity risk management plan. (https://www.nist.gov/cyberframework)

2. Assess Your Cyber Risk

Cyber threat intelligence (CTI) is vital in addressing cyber threats – it allows you to detect and mitigate threats quickly. Collecting such intelligence requires regular cyber risk assessments that cover your business's internal and external aspects.

A good CTI approach should emphasize strategic responses and situational awareness while considering your crucial IT assets. Your cybersecurity risk assessment should test your CTI capabilities, including technology products and services and the human factor

Create a list of risks and threats you're likely to face—bear in mind this depends on your physical and logical assets. You should then identify potential consequences using simple scenarios that everyone in your team can understand. Analyze each risk individually while assessing the possible impact it can have in the event of an attack.

A good assessment should offer insightful intelligence and develop a complete picture of your threat environment.

3. Protect Your Information

As noted before, investing in advanced systems is not enough for your company's valuable information assets. Attackers exploit different weaknesses and vulnerabilities to gain access to your systems. They can be internal, external, or human. So, you need a well-rounded approach to build a more robust defense. This approach includes:

- Adopting and encouraging employees to use complex, stronger passwords
- Using multi-factor authentication to supplement passwords
- Encrypting your websites and key data
- Using commercial cybersecurity products to protect your systems from perpetrators
- Developing a comprehensive backup and recovery plan for easy restore
- Establishing an effective account management process for user access and roles
- Extending your security policy to include remote, personal, and mobile devices
- Installing network and system firewalls and using secured tunnels

Remember that fortification doesn't involve addressing only the software side – physical security still counts. Sealing all security loopholes that a disgruntled employee or an unauthorized user can use to access critical information would be best. Be sure to define roles and procedures for accessing sensitive physical areas in your organization.

4. Focus on Awareness and Training

Up to 94% of organizations have experienced insider data breaches, while IBM says that human error is the cause of over 95% of data breaches. So, cybersecurity is not all about software and hardware–the people who use these resources are key factors.

As such, you need to invest in comprehensive cybersecurity awareness and training. Providing these is a practical approach to preventing social engineering, spear-phishing, and ransomware attacks. Ideally, adequate training allows you to turn your employees into your first line of defense against attacks. Training will enable employees to:

- Spot fraud and spam emails with malicious links and attachments
- Adopt a cybersecurity culture and implement your policy
- Learn and adhere to compliance requirements

Cybersecurity training shouldn't be a once-a-year initiative. Instead, you should offer ongoing training, which should be fun, interactive, and educational. It should cover current and emergency cyber threats while introducing employees to handy techniques and skills for identifying and preventing attacks.

5. Keep Tracking and Monitoring your Systems

Continuous monitoring of your network and endpoints is key to detecting and preventing modern cyber threats and data breaches. Monitoring involves using automated solutions to scan your IT ecosystem and identify threats in their infancy before they can disrupt your operations.

You should invest in a comprehensive 24/7 monitoring solution that tracks your login and authentication, operating systems, threats, servers, cloud security, emails, and remote access. A good solution leverages cloud systems to scan your ecosystem against a current database of emerging threats, malware, and viruses.

Additionally, effective monitoring should also include regular reports on incidents and performance. These reports play well into your CTI strategy–the more intelligence you have, the better. Generally, continuous monitoring helps you detect various threats, reduce response time, and comply with industry and regulatory requirements.

Cyber-proof Your Small and Medium Sized Businesses (SMB)

Digital transformation delivers lots of benefits to SMBs. Its adoption has resulted in using extended networks, multiple clouds, multiple OSs, and many applications to spur growth. While these capabilities are excellent, they require advanced security solutions, which might not be accessible to some SMBs.

Digital transformation has increased the vulnerability of small businesses as they're three times more likely to get attacked than larger businesses. Hackers believe small businesses have poor security systems and don't invest in proper solutions for securing their businesses.

As such, you need to take the necessary steps to secure your business, particularly when up to 77% of cybercrimes target SMBs. Remember that cyber resilience is not helpful to your business alone – it also benefits your supply chains, partner networks, and external systems.

You should keep track of key cybersecurity trends to understand the latest developments and current threats. This intelligence is key to improving your cybersecurity strategy and response plan. Additionally, invest in employee training, enhance your IT systems, keep your software updated, fix all security holes, and have an effective security policy.

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