How Small and Large Businesses Can Adapt to Emerging Cyber Threats

Dr.S. Sujatha, Associate Professor, Faculty of Management, SRM Institute of Science and Technology, Chennai, Tamil Nadu, India. sujathas@srmist.edu.in

Introduction

Cyber risks do not target particular company sizes; although news stories often focus on cyber risks for large international companies, small to medium-sized companies (SMBs) become increasingly vulnerable due to lack of necessary resources for cybersecurity in comparison to larger companies that have complex systems. Thus, large companies are also confronted with their unique set of challenges, such as the complex nature of their attack surface and coordination of the security system across various international locations. The adaptation process to new cyber risks requires developing unique adaptation strategies based on organizational resources and potential risks.

This paper discusses the unique cybersecurity risks for SMBs and large companies, current cyber risks that concern these businesses, and ways to adapt to new risks based on unique organizational characteristics.

Emerging Threats in the Cyber World

There are various new trends that are changing the face of cyber threats facing businesses of different sizes.

AI-based Threats. Cyber criminals are increasingly relying on AI technology to design phishing messages, conduct automated reconnaissance operations, and create deep fake audio/ video to perform social engineering activities, where they pretend to be a business executive or a known contact of their victims.

Ransomware Changes. Ransomware attacks have moved beyond simply encrypting files and demanding ransom. They now include the "double extortion," whereby attackers steal data from the victim's system and threaten to release it to the public in addition to encrypting systems.

Supply Chain Risks. As more companies of all sizes are using interconnected software and services, a supply chain breach through any small software company or a cloud service provider can impact many downstream businesses.

Cloud Misconfigurations. The adoption of cloud solutions by companies of all sizes has resulted in the continued exposure of confidential data due to cloud misconfiguration caused by lack of skills in cloud security.

Legal/Regulatory Challenges. Increasing regulatory requirements in cybersecurity and data protection do not only impact large firms but also businesses of all sizes, which may lack legal/compliance resources.

Unique Challenges for Small Businesses

Despite being a popular opinion, many small businesses tend to fall victim to cyberattacks because they underestimate themselves as not interesting enough for hackers to attack. The fact is that small businesses become prime targets for cybercriminals because attackers are aware of the fact that there is no proper security team, tools or funds available to fight against the problem.

The main challenges for small business include:

Lack of Budget and Skills. Being unable to invest in hiring a team of professionals and paying for sophisticated tools, small businesses remain unprotected.

Dependence on Default Settings. In the absence of IT security specialists, small businesses use default settings which happen to be easy to hack and are known to attackers.

Misunderstanding of Risks. Being unaware of the danger of becoming a target, small businesses neglect their security.

Vendor/Supply-chain Targets. Small businesses functioning as vendors or suppliers for big companies may become attractive targets through attacking larger company.

Challenges for Large Organizations

There is a set of unique challenges that is faced by large organizations that are caused not by the lack of resources but by the scale and complexity of work.

Vast Surface of Attacks. Due to the fact that large organizations are using a lot of systems, applications, and endpoints in their work, they experience problems with visibility and security enforcement in all these systems.

Organizational Complexity. Implementation of policies, coordination of response measures, and risk management within large organizations become more difficult due to the fact that there is an increased degree of decentralization and many separate departments.

Legacy Systems. Large organizations use a lot of legacy systems that are difficult or expensive to replace due to the fact that they cannot be easily adapted to current threats.

High-value Target Status. Large organizations become good targets for hackers, state-sponsored groups, and cybercriminals who can conduct long-term attacks against them.

Regulatory requirements. Large organizations usually have more regulations to deal with.

Adaptation Techniques for Small Businesses

There are several effective techniques that will help small businesses achieve higher levels of security.

Focus on Fundamental Security Controls. The implementation of multi-factor authentication, software updates, good password policies, and basic network segmentation brings great risk mitigation benefits compared to the expenses made.

Take Advantage of MSSPs. Small businesses do not need to invest in building a team of specialists to manage security since it is more efficient for them to collaborate with managed security service providers (MSSPs).

Use Security Capabilities of Cloud Platforms. Nowadays many cloud platforms include advanced security capabilities such as automated patch management, threat detection, and access control, which can replace in-house skills.

Employee Training. In order to minimize technical limitations of small businesses, it is necessary to develop a security culture among employees.

Back Up Your Data Thoroughly and Effectively. Making sure that your business is regularly backing up its critical data in a way that is isolated is an important safety measure that helps you recover from ransomware attacks and data loss cases without having to pay any ransom.

Have An Incident Response Plan Ready. A simple written plan of action in case of any security incident will save you precious time and help you avoid unnecessary losses, whereas not having such a plan will increase the losses from the incident.

Large Enterprise Adaptation Strategies

Large enterprises face the challenge of dealing with the issue of scale and complexity in their security adaptation strategies.

Deploy a centralized security governance structure. By adopting a centralized security governance model, which includes security policies and standards, an organization will be able to tackle the fragmentation problem that is inherent to enterprise security programs.

Develop a comprehensive solution for asset and attack surface management. In view of the size of enterprise environments, the deployment of continuous and automated discovery and management of assets, vulnerabilities, and configuration is imperative.

Implement modernizing legacy systems with a strategic approach. When a legacy system cannot be replaced, an organization needs to adopt compensating controls such as segmentation and monitoring to minimize the risks associated with legacy systems.

Create an organization’s security operations center. Large enterprises need to have mature security operations centers that can detect and respond to sophisticated threats 24/7.

EBroaden security requirements to include the whole supply chain. Given the magnitude of the ecosystem for vendors in an enterprise setting, comprehensive third-party risk management

programs involving security assessment, contractual stipulations, and continuous monitoring are critical in handling supply chain risks.

Perform comprehensive testing frequently. Large enterprises should adopt advanced testing methods such as red teaming and purple team collaboration for validating and improving the security of their systems against realistic and sophisticated attacks.

Common Ground: Common Principles Across All Sides

While there may be many distinctions between the approaches employed by large and small businesses in dealing with cyber threats, there are several common principles which apply to both types of organizations. First, both will find it beneficial to approach cybersecurity not as a project but as an ongoing process. Both will need to commit resources, including leadership time, to their cybersecurity initiatives proportional to their magnitude. Both will need to foster security culture among employees since people always play a critical role in the security of any organization. Finally, both will need to realize that security incidents, to some extent, are inevitable and, therefore, prepare for them properly.

Conclusion

Cybersecurity threats of today carry their own unique, but no less dangerous, challenges to any business, regardless of its size. Small companies will have to cope with resource limitations by investing in proper controls, managed services, and staff education efficiently. Large corporations will need to tackle the problem of scale and complexity by using centralization of governance, visibility, and detection and response. Whichever the size, those businesses which see cybersecurity adaptation not just as an objective but as a continuous process will have more chances to survive in the constantly changing threat environment.