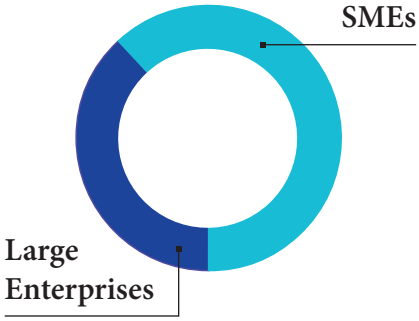
Cyber Attack Inevitability:
The Threat Small & Midsize Businesses Cannot Ignore

CHUBB®

Contents

Targets of Cyber Crime



62 percent of all cyber crime targets were small and medium-size enterprises.

For the past several years, headline-grabbing cyber attacks against large companies, governments, universities, states, and even countries have become commonplace.

Although large-scale incidents garner major media focus, data shows that cyber criminals are increasingly turning their attention to smaller companies. In fact, 62 percent of all cyber crime targets were small and medium-size enterprises (SMEs), according to Small Biz Trends[1]. And evidence shows that this trend of targeting SMEs will continue to rise.

Why are smaller businesses the favoured targets of cyber criminals? Most likely, it's because bad actors know that SME leaders often mistakenly think that cyber security services are beyond their means, making them under protected and easily breached.

Why SMEs May Not Believe They Are at Risk

Cyber attacks against SMEs often go unreported by the media, so these quite-frequent crimes tend to fly under the radar, and smaller companies may subsequently fail to understand the true extent of the risk.

Given the pace of operational change, SMEs are increasingly digitally transforming their business processes to prevent falling behind their competitors. Yet, this necessary move into increasingly complex digital technology creates a corresponding increase in cyber crime vulnerability.

At the same time, such crimes are low risk for criminals, and for a similar reason. The technology that yields business efficiencies also enables criminal elements to employ their breach and exploitation capabilities quickly, cheaply, and anonymously.

Unfortunately, SME leaders all too often lack sufficient information about risk protection, and assume that their cyber attack risk is relatively small. Cyber criminals bank on this naivety and deploy

The Chubb Cyber Index℠[2] notes that it costs an average of $400,000 to recover from a cyber incident.

many of the cyber-crime strategies outlined in the following real-life examples:

- **Stolen Email Account:** After a cyber criminal gained access to an email account belonging to a real estate office, he convinced a client of the firm to wire transfer $300,000 to a fraudulent bank account set up by this criminal.
- **Ransomware Scam:** When an employee at a nonprofit accidentally visited a malicious website at work, the company's shared server became infected with a virus that encrypted all of its files. Cyber criminals then tried to extort money from the nonprofit in exchange for releasing their stolen documents.
- **Phishing Scam:** When an accounting employee at a social services agency got a seemingly legitimate email request, he provided the W-2 forms of current and former staff members, thus handing over their information and facilitating identity theft.
- **Computer Heist:** When a small healthcare company was the victim of a broad-daylight laptop theft, sensitive employee payroll information stored on that laptop was lost and compromised.

From device theft to ransomware, and phishing scams to unauthorized access, cyber criminals can access sensitive information by targeting organizations from the outside, as well as the inside. Technology has made these criminal activities both possible and comparatively low risk.

Increasing Cyber Attacks Can Be Fatal to SMEs

The Chubb Cyber Index℠[2] notes that it costs an average of $400,000 to recover from a cyber incident. This high price tag can result in the catastrophic end for an SME. The hefty cost of repairing the business and its reputation is exacerbated by the disconcerting fact that cyber crimes are not rare events. An FBI report[3] notes that since January 1, 2016, 4,000 cyber incidents have occurred every single day – a 300 percent increase from the year before.

How Can SMEs Protect Their Businesses?

Despite these statistics, there is a ray of hope. According to the Chubb Cyber Index℠, the most common actions that cause a cyber incident are preventable. These include lost or stolen devices, programming errors, falling victim to phishing schemes, and employee policy violations. This means SMEs can prevent many threats by adopting the following preventative measures:

1. **Create a cyber-attack response plan** and invest in the resources to ensure you can execute on the plan.

Simple Steps to Help Protect Your Business:

1. Create a response plan.
2. Use a secure password manager.
3. Educate your employees.
4. Install good antivirus software.
5. Update your operating systems and applications.
6. Protect your networking activity.
7. Purchase a comprehensive cyber insurance policy

Since January 1, 2016, 4,000 cyber incidents have occurred every single day.

2. **Use a secure password manager** to make it easier for your employees to manage their credentials in a secure manner.
3. **Educate your employees** about the risks of cyber crime and deploy software that can reduce social engineering attacks such as phishing.
4. **Install good antivirus software** and ensure it is always up-to-date.
5. **Update your operating systems and applications** regularly to ensure they are supported by the manufacturer.
6. **Protect your networking activity** with a secure router on your internal network and a Virtual Private Network (VPN) externally.

In addition to these six preventive measures, every company should consider a comprehensive cyber insurance policy. In fact, many comprehensive cyber policies will facilitate the services and resources listed above. In addition to the built-in loss mitigation services to reduce the risk of being targeted in the first place, a cyber policy will likely include incident response services if an attack succeeds. This includes, but is not limited to, access to a diverse team of experts in the legal, computer forensics, notification, call center, public relations, fraud consultation, credit monitoring, and identity restoration fields to help limit exposure to a loss. And, of course, an insurance carrier will carry the burden of the financial risk after a cyber crime incident.

SME Cyber Insurance in Action

Remember the small business cyber crime scenarios we mentioned earlier? Fortunately, all four companies had purchased cyber insurance long before they were targeted by criminals. The policies mitigated the losses and helped the SMEs recover, while simultaneously strengthening them against future attacks:

- **Stolen Email Account:** The real estate company victimized by unauthorized email access notified its insurance carrier, which then handled the claim brought against the company by the home buyer after a cyber criminal convinced the buyer to wire transfer $300,000 to a fake bank account. The buyer's funds were restored, according to the terms

of the company's policy, and the company's email accounts were more aggressively protected.

- **Ransomware Scam:** The nonprofit victimized by a ransomware attack that resulted in stolen and encrypted files notified its insurance company and the insurance carrier engaged a forensic computer investigator and a law firm on their behalf. The combined efforts foiled the ransomware scam and got the nonprofit up and running without paying a ransom.
- **Phishing Scam:** After the social services agency victimized by a phishing scam notified its insurer, the cost of retaining a law firm to contact regulators, hiring a notification service to inform the impacted individuals, and providing victims with credit monitoring for two years were all covered by the cyber insurance policy.
- **Computer Theft:** The small healthcare company whose laptop containing payroll information with employees' names, social security numbers, and addresses was stolen and never recovered, quickly notified its insurance carrier. The insurer engaged a law firm and a forensic firm to mitigate the insured's losses and assist in the recovery effort.

In each case, the financial and reputational losses these companies would have incurred could have been insurmountable without the help of a cyber insurance policy.

Given the statistical likelihood of falling victim to a cyber attack, it makes good business sense to take the above preventive measures seriously. After all, the continued survival of your business may very well depend on it.

Endnotes

[1] Alton, Larry. "How to Protect Your Small Business as Cyber Security Threats Rise" Small Business Trends: https://smallbiztrends.com/2016/06/cyber-security-strategies.html (June 3, 2016)

[2] The Chubb Cyber Index℠ www.chubbcyberindex.com (March 2023)

[3] "Protecting Your Networks from Ransomware" https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

About the Authors

Patrick Thielen is a Senior Vice President, Financial Lines, with Chubb and is product lead for the Cyber and Technology E&O lines of insurance for North America. Since ACE and Chubb became one company, Mr. Thielen has been part of the leadership teams that have launched the Small Commercial Insurance division, the Cyber ERM and DigiTech® ERM product offerings, and the Masterpiece® Cyber Protection product. Mr. Thielen is currently leading Chubb's efforts to enhance and expand cyber coverage and risk mitigation solutions for small and midsize businesses, as well as for successful individuals and their families.

Dave Charlton is an EVP of Westchester®, A Chubb Company. In this capacity, he is responsible for development and delivery of specialty commercial and professional products designed for small and micro businesses in North America.

www.chubb.com/ca

Chubb. Insured.[SM]

Updated 02/23