Hackers See Big Opportunities in Small & Medium Businesses

JULY 14, 2021

Aliya Daya
Senior New Business Specialist & Senior Account Executive, Commercial Lines

Businesses of all sizes are experiencing an increased risk of cyberattacks, but small and medium-sized businesses are the most vulnerable to cyber threats.

Cyber threats are on the rise with hackers launching an attack every 39 seconds, according to one estimate out of the University of Maryland.

Recent security trends have shown an increase in the hacking of and data breaches from common workplace devices like smartphones, tablets and Internet of Things devices—smart objects that connect with and exchange data via the Internet, such as thermostats, security systems, virtual personal assistants and more.

Additionally, COVID-19 and abrupt government 'shelter in place' mandates ramped up remote workforces, opening new avenues of attack targeted at employees and staff working from home on improperly secured networks and technology. In fact, according to IBM, remote work has increased the average cost of a data breach by $137,000.

> Google blocked 18 million daily malware and phishing emails related to Coronavirus in April 2020.
>
> (Source: Google)

The sophistication of threats against companies, governments and individuals also increased in both frequency and severity due to the application of emerging technologies such as machine learning, artificial intelligence, implementation of 5G, and especially from the greater tactical cooperation among hacker groups and state sponsored actors.

This has left many small and medium-sized businesses vulnerable to cyberattacks, which result in financial loss, system or data damage, regulatory fines or penalties, reputational harm and more. But what makes these organizations attractive to cybercriminals?

Easy Pickings

Cyberattacks are growing in both frequency and severity, particularly against small and medium-sized business.

According to the Canadian Federation of Independent Business, nearly 25 per cent of small businesses in Canada experienced a cyberattack between March 2020 and October 2020; this figure represents approximately 61,000 small and medium-sized businesses that were victimized by cyberattack relative to the whole economy. (Bear in mind these numbers only represent companies that reported an attack; many more may have opted to keep silent.)

While flashy headlines focus on larger security breaches at recognizable companies, their smaller brethren are actually the more common targets of cyberattacks; rewards may be less, but cybercriminals see smaller organizations as “easy pickings” because they usually invest less in IT security and don’t often educate their staff on cybersecurity risks. Small and medium-sized businesses have fewer resources, protections and preparation to counter cyberattacks.

Smaller organizations (1 – 250 employees) have the highest targeted malicious email rate at 1 in 323.

(Source: Symantec)

Hacking the Human

Social engineering is a generic term used for a broad range of malicious activities accomplished through human interactions. It uses psychological exploitation, rather than technical hacking techniques to gain access to buildings, systems, networks, accounts or data.

Nearly all (98 per cent by some estimates) of all cyberattacks use some form of social engineering. Small and medium-sized businesses tend to be more exposed to this risk because they:

- have less basic security in place, like two-factor authentication, regular data and system backups or encryption of sensitive data;
- do not often understand the risk or provide cyber security training for their employees;
- usually outsource critical aspects of their business to sub-contractors (like HR, accounting and the all-important IT and network security); and,
- almost always make and receive payments using wire transfers or electronic funds transfer protocols.

95% of cybersecurity breaches are caused by human error.

(Source: Cybint)

Zero Options and Saving Face

When targeting enterprise, ransomware gangs are aiming to paralyze organizations by encrypting financial records, customer databases, sales data and any other vital or sensitive information.

Faced with choosing between paying a ransomware demand that may get them back online faster or enduring a long

period of potentially business-crippling downtime (without the assistance or access to a cybersecurity professional), small businesses often feel that they have no choice but to pay these demands in the event of an attack.

Additionally, most small and medium-sized businesses would prefer to keep any cyberattacks secret as the long-term reputational harm to their brand or bottom line can be financially devastating.

> The average ransomware payment rose 33% in 2020 over 2019, to $111,605.
>
> (Source: Fintech News)

The Weakest Link

Many small and medium-sized organizations are networked to the IT systems of larger, partner or vendor organizations for ease of doing business.

So, when cybercriminals are looking to infiltrate these larger and more cybersecure organizations (and frankly, landing the “whale” is the ultimate goal), they are increasingly targeting their humbler downstream suppliers (the “minnows”) to see if these small businesses offer an easier doorway in.

> Damage related to cybercrime is projected to hit $10.5 trillion annually by 2025.
>
> (Source: Cybersecurity Ventures)

Big Game Hunting

Small businesses might think they are safe because they outsource their IT to managed service providers and their data is stored somewhere in the cloud; but if a cyberattack is launched against one of these technology providers, it’s the businesses that rely on these services left dealing with the fall-out.

They are often the collateral damage in large scale cyberattacks that have nothing to do with them, but they suffer the financial repercussions when it comes to business interruption costs, privacy notifications to customers, government penalties, reputational harm and more.

> Hackers attack every 39 seconds; on average 2,244 times per day.
>
> (Source: University of Maryland)

Stop Letting Your Guard Down

The losses and resulting costs of cyberattacks (both tangible and intangible) can be significant, especially for small and medium-sized businesses.

As frequency and consequences mount, small and medium-sized businesses can no longer delay taking action to prevent cyber fraud. Here are a few steps to get you started:

- Be aware of cyber risks to your business. Use sources such as the Insurance Bureau of Canada, the Government of Canada's National Security and Defense Cyber Security Unit, Canadian Federation of Independent Business and other business associations' websites and resources.
- Raise awareness among employees about cyberattacks and train staff to detect and avoid them. Provide education or third-party training tools.
- Consider whether Cyber and Privacy Breach Insurance would be advantageous for your business. Contact a cyber insurance professional at Rogers Insurance and discuss with them your concerns and what options are available.
- Report cyberattacks to local law enforcement, government authorities and other entities such as the Canadian Anti-Fraud Centre, the Competition Bureau and the Better Business Bureau.
- Share information on scams and best practices for prevention with other business owners.

Taking these steps will enhance your cybersecurity, helping to move the target from your organization!

It comes as no surprise that nearly 70 per cent of business leaders believe their cyber security risks are increasing.

(Source: Accenture)

Aliya Daya is a Senior New Business Specialist and Senior Account Executive, Commercial Lines, with Acera Insurance (formerly Rogers Insurance). With more than 20 years of experience in the insurance industry, Aliya specializes in innovation, technology, manufacturing/fabrication/wholesale/distribution, hospitality, religious organizations and disruption/emerging industries.