CYBER INSIGHTS

IRIDIUM
RISK SERVICES EVOLVED

NAVACORD®

How to Prioritize Cybersecurity

Organizations today are under constant threat of cyberattacks as technology continues to evolve rapidly.

Cybersecurity threats can not only compromise an organization's data, but they can also be costly. According to IBM's Cost of a Data Breach report, Canada has the third-highest average cost for data breaches at $4.5 million.

While 88 per cent of organizations believe they have either maintained or decreased their vulnerability to cyber threats, 44 per cent of organizations still expect to suffer a major breach.

The following are steps organizations can take to prioritize their cybersecurity:

1. IDENTIFY RISK

Cyber threats come in many forms, such as malware, ransomware or internal error. Organizations should take the time to identify and understand which risks make them the most vulnerable. During this stage, identifying an organization's key assets can help IT departments prioritize which risks require the swiftest action. Control risks, systemic risks and integration risks should all be accounted for and considered.

2. ASSESS RISK

The primary purpose of a cyber risk assessment is to help inform decision-makers and support proper risk responses. After identifying key assets, this stage determines how those assets may be attacked from a technical point of view. Attacks should be evaluated based on their probability.

3. MANAGE RISK

Once an organization has identified and assessed its most vulnerable points, it can begin to properly manage those risks. At this stage, management should know which data is the most valuable and vulnerable and can make decisions regarding budget, policies and procedures.

The Positive Impact of AI on Cybersecurity

Artificial intelligence (AI) algorithms are trained to learn how to respond to different situations by copying and adding information as they go along.

Organizations can invest in AI to avoid cybersecurity threats, as AI can recognize patterns in data to enable security systems to learn from past experiences. AI can also reduce incident response times while complying with security best practices.

AI can improve cybersecurity in the following ways:

- **Threat hunting**—Replacing traditional threat hunting techniques with AI has been known to increase detection rates by up to 95 per cent.
- **Vulnerability management**—AI can analyze the typical behaviour of user accounts, endpoints and servers to identify any strange activity, and it works to eliminate vulnerabilities before they become a threat.
- **Data centres**—Utilizing AI in data centres can help optimize and monitor essential processes such as backup power, cooling filters, power consumption, internal temperatures and bandwidth usage. This can improve the effectiveness and security of hardware and infrastructure.

The Cost of Ransomware Demands

According to cybersecurity company Emsisoft, ransomware demands increased by more than 80 per cent globally in 2020, and it's estimated that hundreds of millions of dollars have been paid out in Canada alone.

In the country-by-country breakdown, the report estimated that Canada had experienced more than 4,000 ransomware incidents in 2020. The minimum cost estimate was $164,772,274, and the maximum cost estimate was $659,246,267.

The majority of ransomware attacks—which entail attackers gaining access to a victim's data, encrypting it and then demanding ransom for the return of and access to the unencrypted data—are made using the cryptocurrency Bitcoin as the medium for payment. Bitcoin is known for being easily accessible yet hard to trace, making it difficult to identify cybercriminals.

According to Statistics Canada, while 21 per cent of Canadian businesses have been impacted by cybersecurity incidents, only 12 per cent have reported these incidents to police. Businesses were reported to have spent a total of $7 billion directly on measures to prevent, detect and recover from cybersecurity incidents in 2019.

A number of factors may leave organizations vulnerable to ransomware attacks, including outdated software, inconsistent backups and insufficient attention to cybersecurity. To better prevent a ransomware attack, organizations and their employees should:

- **Never click on unsafe links**—Don't click on links in spam messages or on unknown websites. Malicious links can initiate automatic downloads that could lead to data being compromised.
- **Avoid disclosing personal information**—Do not reply to calls, text messages or emails from untrusted sources requesting personal information. Personal information can be later used by cybercriminals to tailor phishing messages directly to the victim.
- **Avoid opening suspicious email attachments**—Ransomware can access devices through email attachments. Pay close attention to the sender and check that the email address is correct before opening any email attachments.
- **Keep programs and operating systems up to date**—Updates give programs and operating systems the latest security patches. Regularly updating makes it harder for cybercriminals to exploit vulnerabilities.

Contact an Iridium Risk Advisor today to learn more about prioritizing cybersecurity and protecting your organization against ransomware threats.