Cyber Risk Management

We all know technology and the internet have revolutionized the way we communicate, do business, and manage data. Organizations are now increasingly dependent on computers, tablets and smartphones to conduct their day-to-day activities. Unfortunately, this has coincided with a significant rise in those looking to exploit the technology for financial gain, or to cause damage and interruption to systems and services.

What is cyber risk?

Cyber risk is the potential for business disruption, financial loss, or reputational damage due to failure of an organization's information technology (I.T.) systems. The risk can come from state-sponsored cyberwarfare, criminal hackers (for financial gain, activism, or mischief), or an organization's own employees—through accident or malicious intent.

Who is at risk?

Between 2013 and 2015, the Government of Canada detected more than 2,500 statesponsored cyber activities against its own networks annually. But smaller entities In Canada are also attacked frequently. An Ontario college recently suffered a ransomware virus that knocked a number of services offline, at a critical time in the school year. And a church group forfeited over half a million dollars to thieves who stole employee credentials and made transfers from their bank accounts. In fact, since educational institutions, charities, and smaller organizations typically have fewer resources to defend themselves, they may be at even higher risk.

Cybercrime

In many instances, online crime has now overtaken physical crimes, such as burglary or robbery, with the cost of cybercrime expected to surpass $2 trillion by 2019.

Cyber criminals are highly organized and are finding a myriad of new and sophisticated techniques to access data and information for the purpose of financial gain. This can result in money being taken from a bank account, or credit arrangements (such as loans or overdrafts) being arranged in your organization's name for the benefit of a fraudster.

Some more common examples of the techniques used by cyber criminals include:

Malware

Malware is malicious software, designed to disrupt, damage, or gain access to a computer system. It can be introduced to your network through email attachments, website downloads, or hardware connections (such as an infected USB key). One serious form of malware is ransomware.

Ransomware

After ransomware takes control of your network, someone attempts to extort money by preventing you from accessing your digital files until you a pay a ransom.

Denial of Service (DoS/DDoS)

A Denial of Service attack is a flood of simultaneous requests sent to a website to view its pages, causing the server to crash.

Web Hacking

Over 75% of legitimate websites contain vulnerabilities. Sites can be defaced, databases with customer details can be extracted, and malware can be inserted to infect future visitors, or harvest their online activity (such as recording the passwords or credit card details they enter).

How do criminals gain access to your network or website hosting?

Criminals will use any technical, procedural or physical vulnerabilities they can find to exploit or disrupt your systems. Some of the typical methods your organization is potentially at risk from include:

Phishing, SMiShing, Vishing, Spear Phishing & Whaling

The fraudulent practice of sending messages purporting to be from reputable organizations to have the recipient reveal passwords or financial information. The messages can be sent by email (phishing), SMS text (SMiShing) or voice mail (vishing), with business accounts targeted six times more frequently than personal ones.

When a phishing message appears to have been sent by a trusted individual, it's sometimes referred to as "spear phishing". Similarly, "whaling" is when a message asking for sensitive information appears to be coming from a senior executive of your organization.

Email, Website & Software Update Malware

Each time an employee downloads an email attachment, clicks on a website link, or updates their software without up-to-date antivirus software, there's the potential for malware to be unknowingly installed on their computer and spread throughout the network.

Online Information

Details found through your organization's and employees' internet presence (websites, LinkedIn, Facebook and other social media accounts) may be used to exploit staff naivety and goodwill and elicit the information needed to gain network access.

Weak Network Defenses & Passwords

A firewall creates a barrier between your computers and the internet—a kind of security checkpoint that controls information entering or leaving your network. If your firewall is not constantly running or properly configured, criminals can get access. Similarly, weak email account, computer, network or website hosting passwords can be bypassed by sophisticated software.

Physical Theft

Stolen laptops, mobile phones, USB keys and paperwork can provide sensitive access details.

Insiders

A recent survey by Forrester found the top source (36%) of data breaches in a 12-month period were insiders—a combination of inadvertent misuse of data by employees, and malicious leaks.

How can cybercrime affect your organization?

Theft

If cybercriminals access your bank accounts, steal information, or find another way to divert assets, your organization may lose substantial equity.

Business Interruption

Cybercrime incidents can take down your website, or disable your entire network, leaving you unable to conduct the day-to-day business of your organization, and leading to potentially significant financial loss.

Ransomware is especially stressful for all involved. Note: in the event that someone is holding your data for ransom, it's important that you do not pay without first seeking specialist advice. Even a small sum can increase your risk of being targeted again, and in many cases, access to the locked files is not always restored after payment.

Damage to Computers, Networks and Websites

Depending on the type and extent of damage incurred, significant expenses may be incurred to get you back up and running.

Fines and Lawsuits from Privacy Breaches

Canadian privacy laws (The Personal Information Protection and Electronics Documents Act and the Digital Privacy Act), as well as some similar provincial laws, mandate that organizations have a duty to protect the private information they collect. This means your organization must use appropriate safeguards against the theft of customer and employee data—including physical measures, technological tools (like encryption and firewalls), and organizational controls.

Failure to abide by a law can result in stiff fines. It can also lead to expensive lawsuits from the exposed individuals. The law also details your responsibility to notify all affected individuals should you incur a data breach.

Damage to Your Reputation

From harmful content on your website, through to business downtime and privacy breaches, cybercrime has the potential to inflict serious damage to your brand. It can take years and a significant investment in public relations efforts to recover.
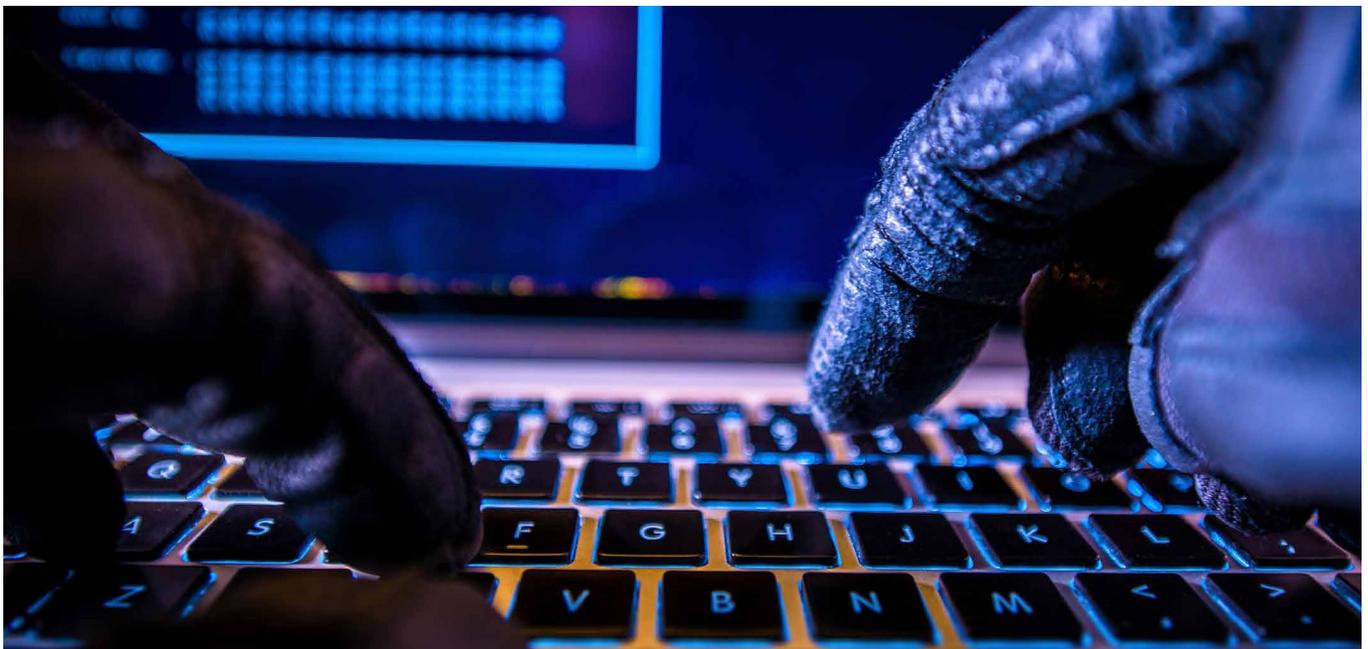
How Can You Reduce Your Cyber Risk?

It's not possible for cyber risk to be managed solely by your I.T. department. Education and follow-up with all team members is essential. Make sure they attend training sessions, understand the potential problems, and are kept up to date on the measures they need to take on their own computers, or as part of their specific job duties. Both the available technologies and the risks keep changing, so do periodic checks to answer questions and ensure all security procedures are being followed.

Here are some things everyone should be aware of in your organization:

Don't Disable Defenses

Keep network firewalls and all anti-virus/ malware/ spyware programs active. Keep all software updated, as security updates patch potential hazards. Note: never install unapproved protection software, as it's often the opposite of what's advertised.

Protect Customer Privacy

Whether you have student health information or charitable donor details on file, it's essential that all sensitive data be protected. From locking file cabinet doors, to ensuring credit card details are encrypted, make sure all privacy measures are in place and followed consistently.

Back It Up & Prepare an Action Plan

Identify what data needs to be backed up. Keep the backup in a separate location (ideally protected off site or in the cloud) and test backups regularly. Have an accessible printed plan for the steps to take, should the digital world suddenly fail.

Be Extra Cautious with Email

According to a 2017 report from Symantec Security Response, 1 in 131 emails contain malware. Before opening any email attachments or clicking on provided links, it's essential to review the accuracy of the sender's information and make sure the content or writing style of the message itself doesn't seem suspicious (in case a legitimate sender's account has been hacked).

Watch Out for Websites

Stick to trusted sites whenever possible. Avoid clicking anywhere on banner ads, unexpected pop-up messages, or warnings. Instead, press Alt+F4 (or Cmd+W on a Mac) to close the window. Hover over any links and carefully check the URL and spelling to see where they go before clicking on them. A link like unknown.trustedsitename.com should be okay. But beware of trustedsitename.unknown.com

Have your own website scanned frequently for unpatched vulnerabilities. If appropriate, install trusted site security plug-ins to help block access by unknown entities.

Use Unique, Complex Passwords

Wherever permitted, make sure passwords are long and complex with letters, numbers and special characters. Never use dictionary words, only numbers, guessable content (like combinations of family/pet names and important dates) or passwords in use on other devices (such as phones or home computers).

Consider using a trusted password manager if you have several to recall. For added security, never send passwords by email or text message. And when an employee leaves an area, ensure access passwords are updated immediately.

Be Aware When Away from the Office

Keep devices and materials physically secure at all times when working away from the office. Use password protection. Encrypt all confidential data

on devices, and make sure they can be tracked, and locked or wiped in case of theft. Report the theft of a business tablet or smartphone promptly. If you use a public Wi-Fi network, look for a password-protected connection that's unique to you, even if you have to pay for it. If it's not available, do not perform any financial transactions, log into company servers, or download any software updates.

Use USB Drives with Care

Never put an unknown drive into your computer, as it could be infected with malware. On your own drive, don't open files you don't recognize.

See Something? Say Something!

If you see something that looks suspicious, report it to your system administrator who can evaluate the situation and warn others if needed.

An ounce of prevention...

Technology will continue to evolve, and so will the risks associated with it. Risk management is about understanding potential hazards and minimizing the exposure to loss. It can be daunting to see that cyberattacks are becoming more frequent and increasingly sophisticated. But when everyone builds the small steps required to protect the organization into their daily routines, it doesn't need to be a formidable task.

ABOUT ECCLESIASTICAL INSURANCE

Ecclesiastical Insurance Office plc is a specialist commercial insurance company. We are deeply committed to protecting the needs of organizations that enrich the lives of others; to preserving Canada's distinct communities, cultures and history; and to supporting initiatives that help improve the lives of people in need.

ecclesiastical

BENEFACT GROUP

Proudly part of the Benefact Group - specialist financial services companies built to make a difference.

ecclesiastical.ca | @EIOCanada