ecclesiastical

White Paper

Cyber Risk Management

Security & Protection in an Online World

Technology and the internet have revolutionized the way we communicate, do business, and manage data. Organizations are increasingly dependent on computers, tablets and smartphones to conduct their day-to-day activities. Unfortunately, this has coincided with a significant rise in 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 resulting from failure of an organization's information technology (I.T.) systems. The risk can come from state-sponsored cyber warfare, 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 state-sponsored cyber activities against its own networks annually. 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. Educational institutions, charities, and smaller organizations typically have fewer resources to defend themselves, they may be at even higher risk.

Cyber crime

In many instances, online crime has now overtaken physical crimes, such as burglary or robbery, with the cost of cyber crime 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. Successful fraudsters withdraw money from an unsuspecting organization's bank account or take out a loan in that organization's name.

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 or network. 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, cyber criminals will attempt 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.

Hacking

Over 75% of legitimate websites are vulnerable to cyber attacks. 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?

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

Cyber criminals who are 'phishing' send out fake emails, texts and voice messages in the hopes of luring someone into disclosing 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

Every time an employee downloads an email attachment or clicks on a link, your organization is at risk. Up-to-date anti-virus software and clear internal policies help protect your network against malware - which can quickly infect your entire system. Everyone has a role to play in protecting your digital assets and network.

Online Information

The information that your employees and your organization share online can provide cyber criminals the detail they need to lure someone into a scam.

Whether it's your website, LinkedIn, Facebook or other social media accounts, exercise discretion before posting.

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. Without strong cyber defenses, their sophisticated software and hacking expertise can easily bypass network firewalls and websites.

Physical Theft

Stolen laptops, mobile phones, USB keys and paperwork are rich sources of information for criminals. Your organization's digital assets and sensitive information need strong protocols and safeguards.

Insiders

A recent 12-month survey by Forrester revealed that 'insiders' are responsible for 36% of data breaches, leaks and misuse.

How can cyber crime affect your organization?

Theft

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

Business Interruption

Cyber crime 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. In the event that someone is holding your data for ransom, it's important 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, you may be subject to significant expenses to get back up and running.

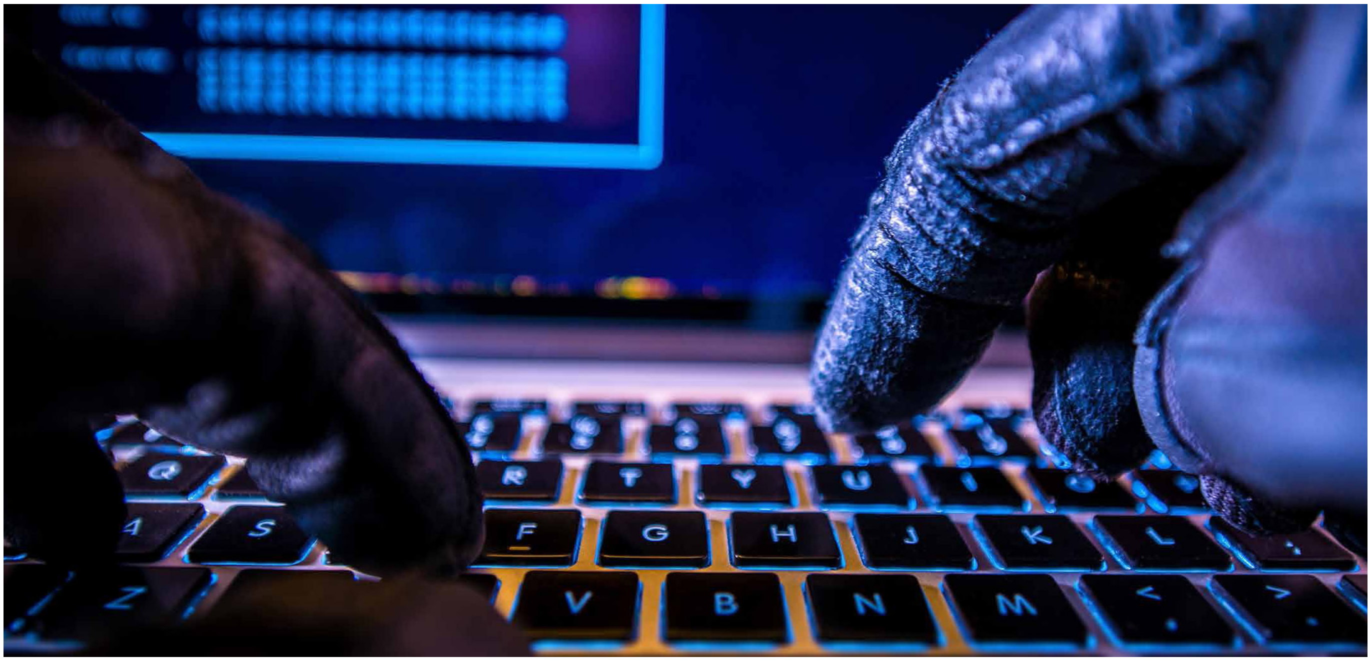
Fines and Lawsuits from Privacy Breaches

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 if you experience a data breach.

Damage to Your Reputation

From harmful content on your website, through to business downtime and privacy breaches, cyber crime 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. 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).

Visit Trusted Websites Only

Stick to trusted sites whenever possible. Avoid clicking 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

Scan your website 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 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 application if you have several to recall. For added security, never send passwords by email or text message. It's also important to update passwords regularly and especially whenever a change in your organization occurs (employee departure/termination).

Be Cyber Vigilant

Keep devices and materials physically secure at all times, especially 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. Don't open files on your own drive if you don't recognize them.

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 cyber attacks are becoming more frequent and increasingly sophisticated.

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

This advice or information is provided in good faith and is based upon our understanding of current law and practice. Neither Ecclesiastical Insurance Office plc nor its subsidiaries accepts any liability whatsoever for any errors or omissions which may result in injury, loss or damage, including consequential or financial loss. It is the responsibility of the Insured or any other person to ensure that they comply with their statutory obligations and any interpretation or implementation of the above is at the sole discretion of the Insured or other party who may read these notes.

ecclesiastical.ca | @EIOCanada