RETAIL COUNCIL OF CANADA

# RETAIL CYBERSECURE

MODULE 3

# CYBER SECURITY FOR RETAIL IT


## Securing your teams, devices, assets, and business.

A guidebook to help retail IT and organization decision-makers protect their teams and businesses against the impacts of cybercrime

RCC RETAIL COUNCIL OF CANADA

CCCD CONSEIL CANADIEN DU COMMERCE DE DÉTAIL

## About Retail Council of Canada

Retail is Canada's largest private-sector employer with over 2 million Canadians working in our industry. The sector annually generates over $85 Billion in wages and employee benefits. Core retail sales (excluding vehicles and gasoline) were over $462B in 2022. Retail Council of Canada (RCC) members represent more than two-thirds of core retail sales in the country. RCC is a not-for-profit industry-funded association that represents small, medium, and large retail businesses in every community across the country. As the Voice of Retail™ in Canada, we proudly represent more than 143,000 storefronts in all retail formats, including department, grocery, specialty, discount, independent retailers, online merchants and quick service restaurants.

Retail Council of Canada acknowledges the support of The Ministry of the Solicitor General (Ministry), 2022-2024 Safer and Vital Communities (SVC) Grant.

Ontario



**Contact Retail Council of Canada:**

1881 Yonge Street, Suite 800
Toronto ON M4S 3C4
Telephone (toll-free): (888) 373-8245
E-mail: education@retailcouncil.org

# Table of Contents

# i. Introduction

When it comes to supporting today's digital retail ecosystem, there isn't a role more integral than the Information Technology (IT) professional. Involved in every single aspect of a retail organization's digital journey, they oversee and orchestrate just about every tweak, adjustment and implementation made to a retailer's ever-expanding and evolving digital network and technological infrastructure, and are accountable for its maintenance and optimization. Included in this purview of responsibility, today's retail IT professional is also charged with ensuring the security of the organization through the use of a number of different safeguards, tools and protocols, defending the business from the potential threats posed by cybercriminals.

Despite the size of your IT department, or organization, it's critical to develop and enforce a range of standard procedures by which those working within the organization will operate, providing consistency to tasks and outcomes and the assurance of safe and secure behaviour within the digital retail ecosystem. It's also important for IT professionals, or for individuals responsible for carrying out technical maintenance and upkeep, to institute the necessary tools and software in order to protect the organization's computers, devices, networks and systems.

In fact, when considering the proliferation and increased frequency of cyberattacks (a recent Mastercard study estimates that cybercrime has risen 600 per cent since the start of the pandemic), the overall role and range of responsibilities of today's retail IT professional becomes that much more important to the health and success of the retail organization.

To help support the efforts of those within the industry responsible for safeguarding their organizations' digital ecosystem and enabling future growth for their brands, Retail Council of Canada has developed the Cyber Security for Retail IT guidebook. Addressing the most critical elements and layers of the digital retail business that require protection, this guidebook provides practical information, direction and best practices meant to serve as a go-to resource and reference for retail IT professionals in their efforts to fend off the threats of cybercrimes.

## The Impacts of Cybercrime:

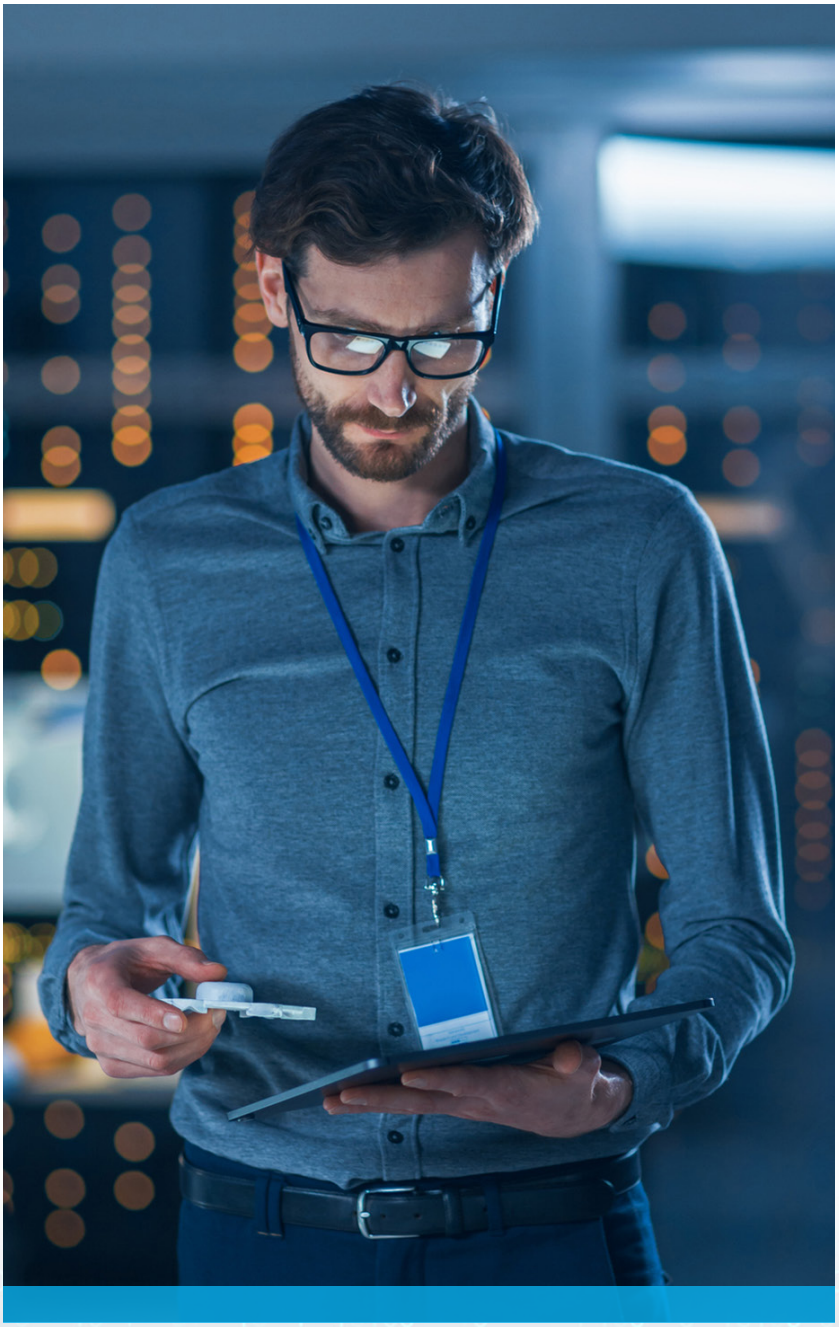
- * The average cost of a data breach in Canada is $5.64 million - $1 million more than global averages – with 99 per cent of victims agreeing the hack impacted their operations.
- The most common ramification reported by retailers as a result of a data breach was a loss of customer data.
- **Cybercrime and fraud cost Canadians more than $500 million in 2022 alone.
- ***24 per cent of cyberattacks each year target retailers, more than any other industry.
- ****When data is compromised in an attack, 42 per cent is payment-related and 41 per cent is personally identifiable data.

** according to Mastercard's 'Securing the digital economy' study*
*** according to RCMP data*
**** according to Trustwave*
***** according to Verizon*

# ii. Assessing Cyber Threats and Risks

From the beginning, the IT function within an organization is going to be involved in every step of a retailer's' digital journey. And, each one of these steps is critical in ensuring a safe and secure digital ecosystem, especially those at the start, including the development of the business' security plan and policies.

## Define and Prioritize



Before developing the plan, however, to better understand what tools and practices need to be put in place in order to ensure a safe and secure digital environment for retail organizations, IT is central in determining the potential cyber threats that are faced by their business, and the associated risks that may result.

Once threats and their associated risks have been identified, IT must then work with management in order to prioritize the threats based on a number of different factors, including the likelihood of their occurrence as well as the nature and severity of the risk involved.

## Develop a Plan

As soon as threats and their associated risks have been identified, it's time to develop a comprehensive cyber security plan that will outline policies, procedures and protocols, highlighting the appropriate safeguards, tools and resources that are necessary to implement in order to mitigate threats and limit any potential risk to the business.

The plan will clearly define the roles and responsibilities of employees within the organization, as well as what is expected from them when it comes to upholding the safety and security of the business.

# iii. Developing Policies and Procedures

Once a comprehensive list of cyber threats have been identified and categorized by the company, IT must get to work developing the policies and standard operating procedures that will help guide employees through just about every task that they'll undertake as they relate to the digital ecosystem. These policies and procedures will go a long way toward driving operational consistency, in addition to becoming go-to resources and references that support the intent and objective of a formal and comprehensive cyber security plan

## Employee Do's and Don'ts

Lending real meaning and teeth to any cyber security plan, a strong set of policies, procedures and protocols outline and explain clearly employee dos and don'ts when it comes to cyber security. IT own the development of these policies and procedures and will work with management to ensure employees adhere to them.

The cyber security plan will include policies related, but not limited to, Internet use, social media use, the handling of information, the proper use of mobile devices and computers, and remote communication. Essentially, a cyber security plan intends to serve two purposes from a retail organization's' perspective, 1) to protect its assets, employees and customers, and 2) to create standards by which business will be conducted within the digital domain and landscape, diminishing room for internal error.

To further underscore these standards within the cyber security plan, they can be developed into standard operating procedure documents which are reviewed and referenced by employees on an ongoing basis.

When beginning to develop cyber security policies and procedures that are specific to their organizations, IT will want to consider the following:

**Start with simplicity –** It's best to begin by developing a relatively basic cyber security plan containing fundamental policies and procedures, from which more complex and detailed information can grow and expand.

**Identify and adapt existing standards –** When beginning development of the cyber security plan, IT will want to incorporate as many effective existing policies and procedures as possible in order to maintain operational consistency and eliminate guesswork.

**Explain rationale –** In order for policies and procedures to have the greatest effect and impact, they should be explained to employees so they understand why they are in place and how they help to protect the business, its assets, employees and customers.

**Revisit, review and revise –** As is the case with just about every other living, breathing document, a retail cyber security plan needs to be reviewed on a consistent basis, and revised and updated accordingly.

It's clear that, despite the expertise and knowledge that's behind any cyber security plan, the execution of that plan and enforcing of its best practices requires leadership from IT, including the provision of guidance and direction to all employees concerning cyber security activities; their active involvement in various cyber security-related projects; and collaborating with external experts, including legal counsel, when required.

While the process to develop a cyber security plan may seem daunting at first, remember that you can always revisit and expand your plan over time.

## iv. Secure Software Configuration

Another incredibly important responsibility of IT within the retail environment is to ensure that any and all devices and software that are implemented into the already existing network or system of devices and software are done so securely and that they do not compromise the organization or create any unforeseen vulnerabilities.

It's especially important for smaller organizations to be mindful of their device and software configurations, as manufacturer default configurations are not often set up with the security of the end-user in mind. Basic controls, open services and ports, default accounts or passwords, pre-configured Domain Name Systems (DNS) settings, and other factors can leave a retailer open to the threat of cybercrime. In addition, IT teams will want to consistently manage updates to their configurations in order to prevent security degradation.

There are a number of safeguards and best practices that can help IT leaders and their teams ensure the security and maintenance of their software configurations:

- Establish and maintain a secure configuration process
- Establish and maintain a secure configuration process for network infrastructure
- Configure automatic session locking on enterprise assets
- Implement and manage a firewall on servers and devices
- Securely manage enterprise assets and software
- Manage default accounts on enterprise assets and software
- Uninstall or disable unnecessary services on enterprise assets
- Configure trusted DNS servers on enterprise assets
- Enforce automatic device lockout on portable end-user devices
- Enforce remote wipe capability on portable end-user devices
- Separate enterprise workspaces on mobile end-user devices

# v. Securing Accounts

The tactics employed by cybercriminals to gain unauthorized access to sensitive information are becoming increasingly sophisticated. However, none will ever be as effective as the use of valid user credentials. In light of this, it's of paramount importance to the overall health and security of a retail organization's digital ecosystem that IT ensure the use of processes and tools to assign and manage authorization to credentials for all user and administrator accounts within the business. It's particularly useful to strictly manage administrative accounts given the fact that users can be added, and changes can be made to enterprise assets, from within them.

## Tracking Accounts

In order to properly and effectively manage the many different accounts that are used within a retail organization, IT will be required to inventory and track them. It's also important to inventory and track account logging activity as many accounts offer primary entry points into an organization's network and systems, providing cybercriminals with an easy way in.

## Managing Access

In addition to inventorying and tracking accounts, it will also be the responsibility of IT to use processes and tools in order to create, assign, manage, and revoke access credentials and privileges for any and all accounts used within the organization.

In order to maintain strength of security controls for accounts, IT should assign authorization to accounts based on roles, minimizing access to accounts wherever possible. To support this process, consistent access rights for each role is an excellent best practice to employ. It will involve a process by which access to accounts can easily be granted and revoked when necessary.

In order to effectively and accurately manage accounts and user access to them, IT will want to make sure they do the following:

- Establish and maintain an inventory of accounts
- Use unique passwords
- Disable dormant accounts
- Restrict administrator privileges to dedicated administrator accounts
- Establish and maintain an inventory of service accounts
- Centralize account management
- Establish an access granting process
- Establish an access revoking process
- Establish and maintain an inventory of authentication and authorized systems
- Centralize access control
- Define and maintain role-based access

# vi. Web Security

In order to properly and most effectively secure the digital retail environment from the potential threats of cybercrime, IT leaders and their teams will want to make sure to protect and safeguard the Internet and everything else web-related. And, given the amount of online activity conducted by retail employees, the more holistic their approach in doing so, the better.

Two of the most common areas most vulnerable to the threat of cybercrime are email communications and Web browsing. As a result, IT should focus much of their effort on ensuring best-in-class protections and detections of the range of cyber threats.

## Web Browser

It's critically important for IT leaders and their teams to remain up-to-date concerning the latest browser patches and security features to ensure safe and secure browsing within their organizations. By simply configuring the business' Web browser for all users, retail organizations can prevent employees from intentionally or unintentionally installing malicious software when perusing the Internet by limiting the ability of a user to install add-ons, plugins, extensions, or anything else of the like, while also preventing harmful content from automatically executing on devices.

## Hosting and Business Web Security

Another area of the business' digital ecosystem that could present vulnerabilities to attack is its website. If not properly secured, it could serve as an easy target for cybercriminals seeking to take advantage.

Businesses host their websites in different ways. Depending on your organization's hosting preference, there are some recommendations to follow.

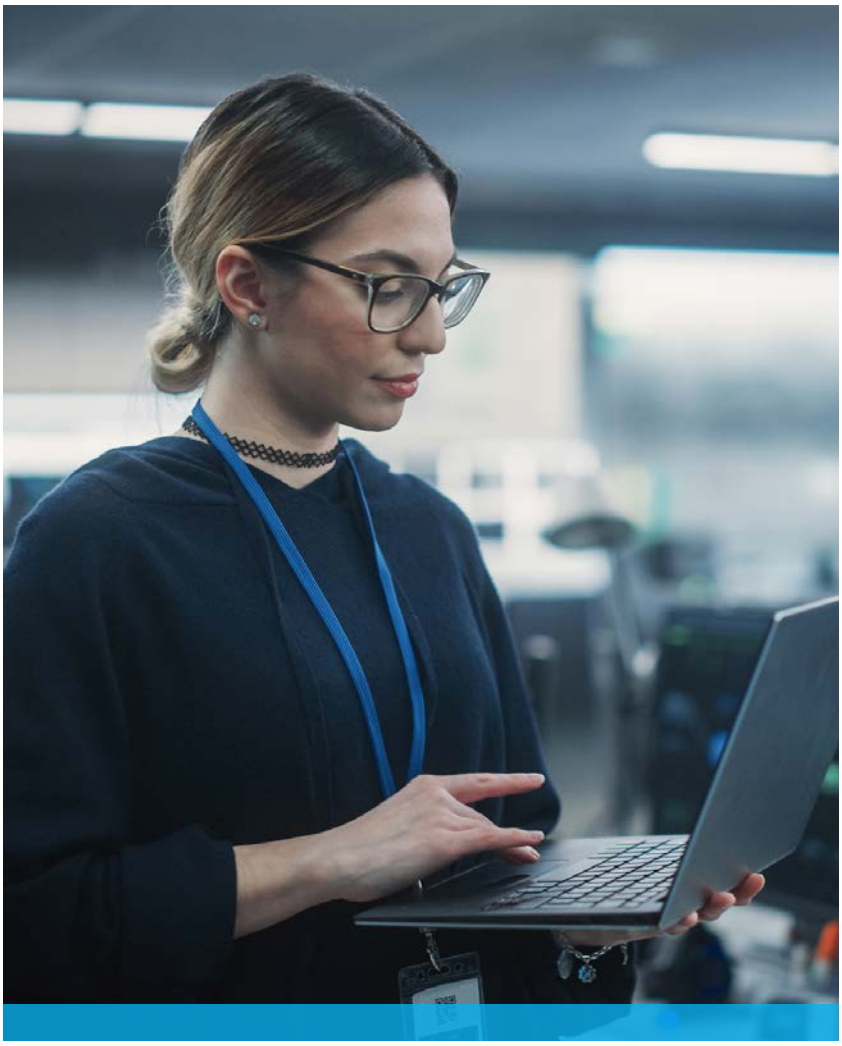
## Hosted on internal servers:

**Restrict access –** Allow only authorized employees to gain access.

**Apply upgrades –** IT professionals should make sure that all available upgrades have been applied to operating systems in order to avoid issues and vulnerabilities.

**Back up regularly –** IT professionals should make sure that business systems are backed up regularly, preferably to a server housed at a separate location. They should prescribe a process to be followed.

**Ensure server logging –** Make sure that someone is in charge of the servers, and that they regularly review the server logs for suspicious activity.



## Hosted through a service:

**Ensure a plan is in place –** IT must make sure that the service provider has its own security plan and that some of their operational best practices include scanning their Web servers and your website for potential issues and fixing those issues upon their identification; the monitoring of your organization's website and systems for suspicious activity; the protection of your organization's website and the restoration of disruptions or failed service caused by cybercriminal activity.

It's also important that IT is prepared in the event of the system becoming compromised as a result of a cyberattack, understanding that actions could include reducing service, switching to a backup server, leveraging the help of an alternate service provider, or, in the worst case scenario, temporarily shutting down altogether. In light of this, IT will want to consider scenarios involving a compromised server in order to develop a plan to address it and the tactics that will be used.

## Email Communication

Most, if not all, communication between colleagues, associates and business partners today is conducted via email. However, as mentioned, email is highly targeted by cybercriminals as a way by which to infiltrate retail organizations' computers, devices and systems in their quest for sensitive personal and business information.

In order to prevent cybercriminals from easy access to a retail business' network and internal systems, IT can take the following precautions to secure the organization's email communications:

**Filter it –** By implementing a spam filter, retail organizations can ensure that most potentially harmful emails sent by cybercriminals will be prevented.

**Encrypt data –** Make it impossible for cybercriminals to read and understand data by encrypting Web-base email by enabling https.

**Strict passwords –** Promote the use of strict passwords for all email accounts that are used within the business, whether they are for business or personal use.

**Generic emails –** Whenever possible, IT should promote the use of generic emails in order to avoid using employee names.

## Defending Against Malware Attacks

Given the fact that the entire retail digital landscape and ecosystem is supported by, and connected to, an endless series of software, systems, programs and applications, the threats posed by malware are innumerable and, most often, highly disruptive and destructive. There are a number of different types of malware capable of infecting operating systems before making a copy of itself and infiltrating another device, including worms, trojans, ransomware, spyware, adware, and more.

### What Can IT Do?

Although malware is often incredibly effective in serving its purpose, IT can safeguard their businesses systems and digital information by ensuring the implementation of the following:

**Anti-malware software –** As a result of the proliferation of different types of malware, a range of anti-malware software now exists, providing users with the ability to scan all files that are incoming to the organization and block anything that it deems suspicious or that it suspects is embedded with malware.

**Firewalls –** Retail organizations may also want to install firewalls within their computers and systems in order to prevent connection to malicious and nefarious websites. In addition, a number of different firewalls are also able to prevent many types of malware from even entering the system.

## Ensuring Proper Authentication Practices

When dealing with such large amounts of sensitive data and information, it's incredibly important that the authentication practices that have been designed by retail organizations are followed by all employees and enforced by IT.


## Passwords

Commonly used to protect a range of different accounts and systems containing a plethora of business information and tools, passwords are a necessary layer of protection within the retail digital ecosystem. However, if not used properly, passwords can become a vulnerability within businesses that expose them further to the threats of cybercriminals.

**Maintain control and confidentiality –** Ensure that employees understand the importance of keeping their passwords safe, secure, and unknown to others around them.

**Avoid using weak passwords –** Employees should avoid using easy-to-guess passwords that can enable others to gain access to their files and information.

**Avoid using the same password –** It should be made clear to all employees that, in addition to avoiding the use of easy-to-guess passwords, they should also avoid using the same password for every account and device.

**Change password frequently –** Passwords should be changed frequently by all employees to avoid complacency and reduce predictability.

**Develop a policy –** It might be a good idea for IT to work with management to develop a password policy that identifies for employees simple rules to follow when creating passwords.

**Avoid common and simple –** When creating passwords, employees should avoid the use of common phrases such as "password" or "enter", simple sequences of numbers such as "1234", and easy-to-guess personal names such as a child's first name.

**Size matters –** The more characters that are in a password, the more effective it is. So, be sure to advise the creation of passwords that are at least eight characters long.

**Combined strength –** Passwords are also stronger when multiple types of characters (uppercase letters., lowercase letters, numbers, and special characters) are used in combination with each other.

## Passphrases

For some retail organizations looking for a more enhanced form of security, the use of passphrases instead of passwords might be a smart consideration.

For instance, rather than using the password "G0bLUe!", a passphrase such as "Thosewhostaywillbe-champions!" becomes that much harder to guess. In addition, acronyms can be used in place of longer phrases (i.e., "hailtothevictorsvaliantthechampionsofthewest!" becomes "httvvtcotw!"), requiring fewer characters to be typed, but maintaining its effectiveness in protection and security.

Cybercriminals are constantly developing newer pieces of software designed to hack and guess passwords. In light of this, IT professionals should recommend the use of tools that demonstrate for users the relative strength or weakness of any given password or passphrase.

## Two-Factor Authentication

Much more difficult to guess than passwords or passphrases are two-factor authentications, which have the ability to add a layer of complexity and security to any retail organization's systems.

Essentially, as the name implies, two-factor authentication requires the person or system seeking authorization to provide two pieces of authentication – one factor is known by the person or system (like a password), and the second factor is something, permanent or temporary, that can be used to authenticate the person or system's identity (such as a fingerprint or temporary password).

As technologies continue to become more powerful and intuitive, and the capabilities of artificial intelligence and machine learning increase unabated, two-factor authentication is increasingly becoming a necessary implementation in order to enhance the protection and security of a retail organization's assets, information and systems.

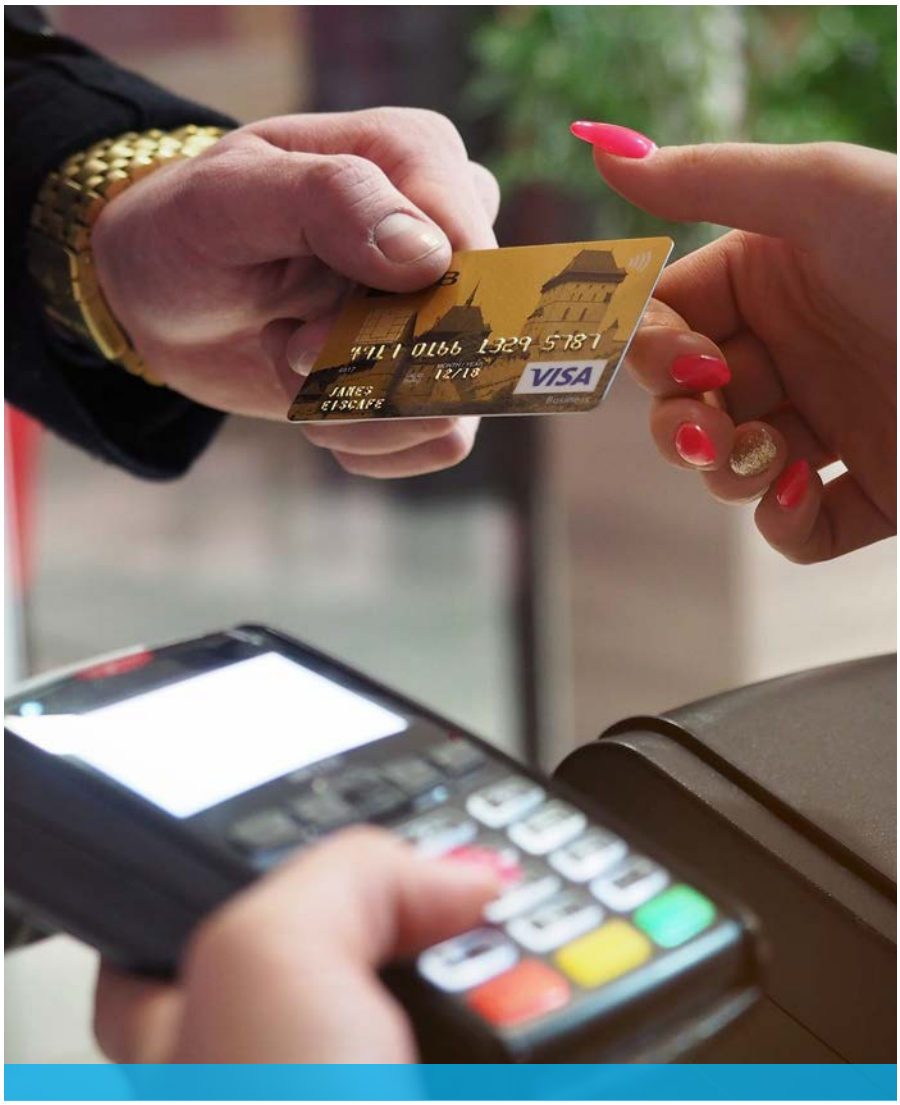
## Reporting Incidents

If an incident of cybercrime occurs that is suspected to have compromised the business in any way, retail IT leaders should:

- ***Report the incident to local law enforcement.***
- ***Report the incident on the National Cybercrime and Fraud Reporting System here, alerting the Royal Canadian Mounted Police (RCMP), the National Cybercrime Coordination Centre (NC3), and the Canadian Anti-Fraud Centre (CAFC), in order to protect the organization today and help safeguard it against similar threats in the future.***

## vii. Securing a Point-of-Sale System

Within today's expanding digital ecosystem, it's more than likely that your organization uses an electronic point-of-sale system (POS) to execute and process financial transactions within stores. It's a form of technology that has become ubiquitous with business today, enabling merchants to accept payment via credit and debit card. However, as is the case with all things digital, POS systems also come with security concerns, requiring IT leaders and their teams to ensure the utmost in payments security for their customers and business.




To enhance the security of POS systems, IT can do the following:

**Ensure firewall is in place –** Placing your POS system behind a security firewall is a must, and the only way in which to restrict the amount of incoming and outgoing network traffic. You're organization's/store's Internet provider has likely included a firewall with your router. But, it's best to check and to ensure its reliability.

**Set up strong encryption –** It's incredibly important to set up strong encryption for the transmission of all transactional data involving cardholder information between your POS system and the POS service provider.

**Ensure creation of unique usernames and passwords –** It's strongly recommended that your organization avoid using the default username and password that came with your POS system. These serve as an open door to cybercriminals looking for the easiest way into your digital ecosystem and business.

**Limit access –** It's critical that your organization limit access to client and customer data only to those who require it and who are authorized.

**Maintain updates –** It's always a good idea to remain on the front of antimalware software, updating all digital systems as frequently and consistently as possible.

# viii. Data Security

Within this ever-digitizing world, retailers are in possession of, and handling, an enormous amount of data at all times. Given the importance of the data that they're collecting every day to the growth of their businesses and optimization of their operations, it only makes sense that it be secured and protected as tightly as any other asset.

## Why Back Up Data?

Backing up digital and physical files is a practice that helps to retain important data, and restore lost or damaged files. In addition, and perhaps most importantly, if executed properly and effectively at a regularly scheduled frequency, back up plans allow retailers to recover quickly and seamlessly in the event of a system crash, data corruption or other setback.

## Backing up Data

The most effective way for retailers to ensure the proper maintenance of data is to develop a back up plan for it – one which all employees of the company will abide by, adhering to a strict set of back up practices.

**Back up frequently –** IT should ensure that all employees back up data regularly as per the back up plan, whether hourly or daily.

**Physical storage –** In conjunction with frequency, ensure that data is backed up in a number of different ways, including on physical hard drives, in order to add another layer of security.

**Data destruction –** Data that has not been backed up, which will be discarded by the company, should be thoroughly destroyed. Delete all digital files and shred all physical documents to avoid the potential of its use against the business.

## Back Up Options

There are a number of ways by which data can be backed up by retail businesses, ensuring its short- and long-term security.

**USB hard drive –** Depending on the size of the business, portable or desktop USBs might serve as a suitable back up option.

**Server –** Ideally, data should be stored on the business' Local Area Network (LAN) and back up automatically from there.

**Online –** Retailers can also choose to back up their data to the Internet, allowing third-party service providers to take care of backup and restoration.

## Handling Sensitive Information

Given the amount of data that retailers are working with on a consistent basis, at least a portion of it can be deemed sensitive, including personal employee information, as well as customer and financial data. As such, the mishandling of this data could result in unauthorized access to it, its loss, manipulation or modification, as well as a range of damages to the business and its customers. In light of this, all employees should be versed in best practices related to the handling of sensitive data.

**Restrict access –** When data is not being used, whether digital or physical files, it should be locked up with restricted access to a small number of employees, and secured by a combination of electronic and physical safeguards.

**Label correctly –** In order to ensure proper maintenance of sensitive data, files and documents should be properly labelled and stored accordingly.

**Total destruction –** If sensitive information must be destroyed, it should be shredded using a high-quality paper shredder that crosscuts the sheets into small pieces. When destroying physical records and information stored on discs, the destruction should be just as thorough. To destroy information stored on drives or computers, commercial 'erase' or 'deletion' tools can do the trick.

## Classifying and Labelling Sensitive Information

In order to properly label sensitive information correctly, IT leaders and their teams need to first possess a deep and confident understanding concerning which types of information is sensitive.

To do this, they'll want to consider the following:

**Where is it located? –** It's important for IT to identify were information resides within the organization, whether on a server, in the cloud, or elsewhere.

**What's the damage? –** In order to determine the proper sensitivity of information, it must be rated with respect to the severity of potential impact as a result of its loss or damage. Simply assign a rating of 1-5, 1 being the least impactful and 5 being the most impactful.

**Handle with care –** The information rated at the higher end of the scale (this will depend on the sensitivity of each organizations' information) should be labelled and handled with appropriate care.

In addition to the number rating applied, in order to provide another layer of security and controls to the labelling and handling of sensitive information, IT may want to consider working with each department within the organization to classify the information as well.

**Public –** This type of information is not sensitive at all in nature and is available to everyone, whether inside or outside of the company, and does not require any special labelling or handling.

**Restricted –** This type of information has an increased level of sensitivity and should be labelled 'restricted'. Access to it is required by a select group of individuals and is controlled via a number of different safeguards.

**Confidential –** This type of information can only be accessed by an extremely limited group of authorized personnel. It should be labelled 'confidential' and should never be permitted to be taken outside of the organization's systems, for any reason.

## Cloud Security

One of the most celebrated recent innovations to crop up within the digital age is that of cloud storage and computing. Allowing for the use of resources that are available on the Web, outside of an organization, it's a power of computing that's most commonly used in conjunction with payment providers and processors, document and account management, and so much more. Driven by powerful software, cloud computing often allows users to customize the services they use to fit the needs and budget of their organizations. However, given the amount of data that's at play, much of which is highly sensitive, IT leaders will want to ensure due diligence when researching cloud options for their businesses.

Things for IT to consider when exploring cloud software for their organizations:

**Read reviews –** It's important for IT to read as many reviews as possible and to seek out recommendations regarding any potential cloud service provider that they're considering.

**Ask about reliability –** When speaking with a cloud service provider, ask them upfront about the reliability of its service and past performance.

**Manage access –** Just as is the case with all other accounts within the organization, access to cloud services should be limited and determined ahead of time.

**Take your time –** Deciding on a cloud service provider is a big move with potentially serious consequences. IT leaders should refrain from making a final decision until they are comfortable with their level of understanding concerning their options.

# ix. Remote Access

A lot has changed within the North American business environment over the course of the past few years, with the popularity of remote access working surging among employees, and the adoption of these new work arrangements by companies everywhere increasing. It's proven to be a real boon for business, saving companies time and money, while boosting employee productivity. However, along with this evolution of work conditions and environment comes greater risks of exposure to cybercriminals and their digital schemes. Though, with the right controls in place and practices assured, much of the threat posed by cybercriminals can be allayed.

## Remote Computing Basics

For retail businesses that have decided to grant their employees the benefits of working remotely, access to their networks will likely be provided via the Internet. And, although it proves to be an easy and efficient way to connect employees to their work, despite their location, connecting over the Internet is not considered a secure way to exchange information, providing cybercriminals with more opportunities than ever before to exploit weaknesses in digital policy and practice.

As a result, it's a good idea for IT to ensure the use of a secure Virtual Private Network (VPN) to connect employees to their networks, as they allow for the encryption of the connection, rendering communication and the transfer of information unusable to anyone aside from the person that the message was sent to.

IT should combine the use of a VPN with other safeguards and layers of protection mentioned throughout this guidebook, and should work with management to ensure that employees follow a set of best practices related to the security of remote access working.

In order to ensure security of remote working, IT should:

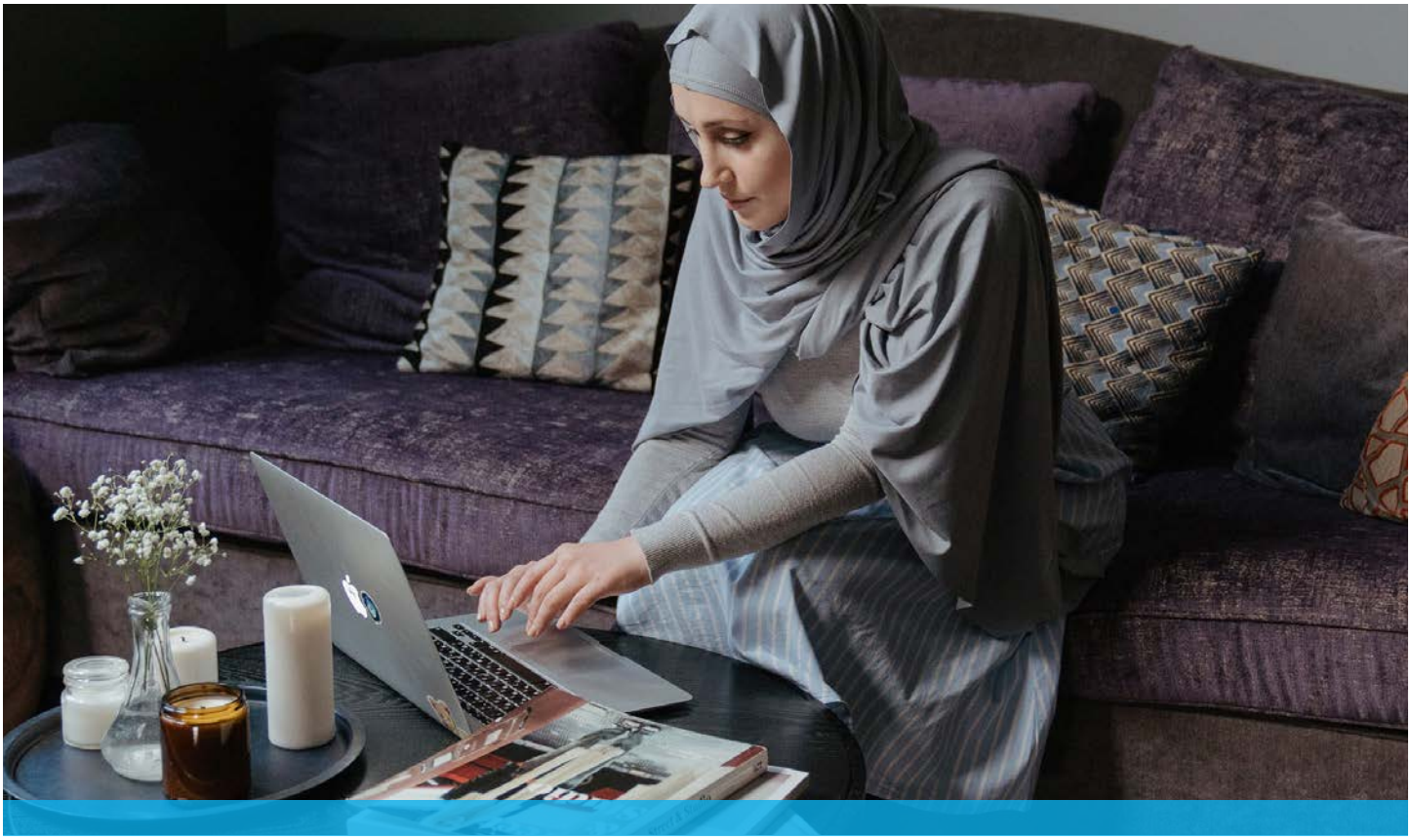
**Limit access –** Remote access should be limited to authorized employees with a clear business need. Access should only extend to the applications, information and services that are required for work to be performed.

**Present Remote Access Agreement –** All employees who enjoy remote access to do their work should be required by IT and management to sign a Remote Access Agreement which outlines and highlights the related roles, responsibilities and best practices.

**Adjusting access –** IT should allow for the adjustment of remote access privileges in the event that responsibilities of individuals within the company change.

**Assigned computers –** In order to add an additional layer of security to remote access working, IT should ensure that employees are provided with business computers that have been set up and enabled with the software and safeguards decided upon by the business to ensure greater security and control.

**Label and record device information –** As with all other digital mobile devices, IT should label all computers assigned to employees with remote access working privileges with serial numbers that are recorded in order to help track their configurations or with their recovery if they are ever lost or stolen.



## Working From Home and While Travelling

The most common remote access arrangements are made between retailers and their employees who work-from-home and those who work while travelling. They provide for simple and convenient ways for employees to connect with their employers when they are not physically in the office. However, if using a personal computer or laptop to do so, additional risks could be exposed.

In order to minimize these risks, IT should:

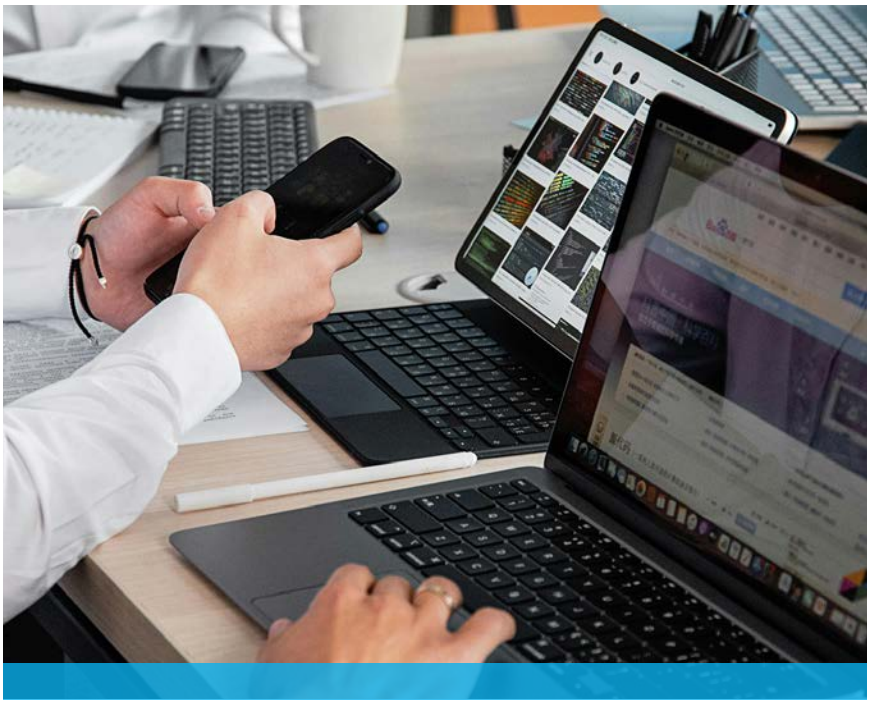
**Restrict wireless access –** IT should ensure that all employees working-from-home on a personal computer are connecting their computer directly to a router using an Ethernet cable, and to connect the Ethernet cable to the modem, in order to prevent anyone outside of the network from intercepting communication.

**Secure Wi-Fi –** IT should make sure that employees are using secure Wi-Fi connections in order to prevent cybercriminals from gaining access to sensitive business information.

**Change default network name –** IT should work with employees who are working from home or while travelling to change the default Wi-Fi network name and the router access password on the network router, allowing for a more secure connection.

**Ensure network encryption –** IT should make sure to enable network encryption, preventing any intercepted communications and sensitive information from being used by cybercriminals.

# x. Digital Devices



Some of the more significant and important tools within the evolving digital retail ecosystem are the different devices that are leveraged by retail businesses and their employees in order to communicate, share information and collaborate on work. But, given the fact that each device represents one more possible entryway into a network or system, cybercriminals are increasingly targeting them in hopes of facilitating a breach. Therefore, it's becoming incredibly important for IT to implement the proper safeguards and enforce appropriate behaviour in order to ensure the security of these devices that are mobile and in frequent use.

Some of the most common devices used by retail businesses and their employees are tablets, smartphones, and portable data storage devices. And, if any of these devices go missing, they are all susceptible to a number of negative outcomes, from damage and loss to the exposure to malware. And, worse, sensitive information and network tools can be vulnerable to misuse.

In order to avoid the worst, or mitigate any loss caused by stolen or damaged devices, there are a few things that IT can do:

**Record serial numbers –** Recording the serial numbers of all mobile devices and portable storage devices being used by employees within the organization is a very good idea in the event of loss or theft.

**Frequent back up –** IT should enforce the regular backup of contents on employee devices.

**Use security apps –** IT should ensure that all appropriate and effective security apps are installed, leveraging encryption, locators for lost devices and anti-malware.

**Use existing safeguards –** Most mobile devices today are equipped with security features, including anti-malware software, which should be enabled on each business-issued device.

**Ensure encryption –** All portable data storage devices should be encrypted to ensure that any and all information placed on them is protected and secured.

**Label devices –** It's a good idea to make sure that all portable devices are labelled with the business' name and contact information in the case of loss.

# xi. Incident Response Management

In addition to the development of a comprehensive cyber security plan, IT must also serve an integral role in developing an Incident Response Plan, containing policies, procedures and best practices related to the ways in which to respond to a cyber security incident.

## Developing a Plan

Working in conjunction with the overall cyber security plan, Incident Response Plans serve to enable retail organizations to prepare for cyber security incidents, detect them, and quickly respond to attacks in the event of their occurrence. They are critical in the protection of any retail organization's digital ecosystem and business as a whole, and key in defining steps and actions to take and the responsibilities of employees meant to support them.

In essence, a strong Incident Response Plan should address the following:

**Protections and detections –** A clear definition of the sources for protections and detections that the organization currently has in place.

**Policies and procedures –** A clear and comprehensive list of rules, policies and procedures related to incident response for employees within the organization to adhere to in the event of an incident.

**Resources and assistance –** A list of all resources and assistance available depending on the nature of the incident in question.

**Roles and responsibilities –** Clearly defined roles and responsibilities for individuals within the organization as they relate to incident response.

**Reporting incidents –** Direction for employees concerning when and how to report an incident that they believe is compromising the organization in any way.

**Response process –** An extensive list of types of cyberattacks and incidents, and the steps that are to be taken when responding to the attack or incident.

**Mechanisms for communication –** A detailed process by which communication is to be made, both with internal colleagues and partners and with external stakeholders, in the event of a cyberattack.

**Post-incident process –** Clearly defined direction with respect to the recovery post-incident, as well as the steps that need to be taken in order to properly and effectively understand the cause of the incident, the ways it could have been avoided, and ways to mitigate its future occurrence.

## Penetration Testing

An important part of the maintenance and reliability of any cyber security program, and an integral component to include within a retail organizations' Incident Response Plan is the scheduling of regular penetration testing. Meant to test the effectiveness and resiliency of the business' assets, devices, network and systems, penetration testing does just that – it looks for the weakest points of protection and defense, exploiting them to demonstrate vulnerabilities to attack.

By simulating the actions of an attacker, driven by simulated objectives, penetration tests strive to achieve the following:

**Expose outdated technology –** Exposing the technologies that are outdated and vulnerable to the increasingly sophisticated tactics employed by cybercriminals helps IT maintain the reliability of the organization's network and systems.

**Understand potential depth –** Understanding the depth to which a cyberattack could get to reaching sensitive business information is critical in recognizing the strength of protections and controls.

**Determine at-risk data –** In addition to understanding the potential depth of cyberattacks, it's also important for IT to work with management in order to identify the data that is most at risk and that which poses the greatest threat to the company if systems are breached.

**Identify gaps –** Identifying where weaknesses and gaps are in an organization's protections allows IT to understand which safeguards are required to further strengthen security.

***Note:*** *Penetration testing should be conducted by an experienced professional who understands the risks inherent in running such a test.*

## Network Monitoring and Defense

In addition to the execution of regular penetration tests, IT will also want to keep a constant eye on their organization's network and systems. Despite the effectiveness of any given cyber security plan, or the ability of an organization to prepare itself well enough to respond to incidents in the speediest and most efficient way possible, the diligent monitoring of threats and defenses against them is critical.

The thorough and consistent monitoring of an organization's network and systems in many ways serves as both the first and last line of defense for any retail business, and may include some of the following benefits:

**Provides visibility –** With the consistent monitoring of potential threats to the security of a retail organization's network and systems (which is advised to include both technology-driven systems and software, and human intervention), IT is granted incredible visibility into the ecosystem that supports its digital activities, allowing for a greater understanding of the business' infrastructure needs and abilities.

**Prevents spread of threats –** By monitoring threats, cyberattacks can often be caught before they happen, or, in the least, recognized quick enough to mitigate most potential damage.

**Business intelligence –** Monitoring the organization's network and systems also allows for the generation of a considerable amount of valuable activity reports and metrics that can be used to help enhance security policies, and support regulatory compliance.

**Enables proactive approach –** In addition to an organization's ability to detect threats before they happen, monitoring also enables a proactive approach to be taken to security, informing the safeguards, tools and best practices that will be implemented going forward.

## xii. Security Awareness and Skills Training

In order to ensure that the plan and all of its policies and procedures have the greatest impact within the organization, it's critical that awareness and education concerning cyber security and its importance take place. And, it's just as important that IT lead the education to ensure the proper transfer of information and knowledge.

Within an organization's cybersecurity awareness program, IT will want to work with management to include training and education resources and materials concerning the potential threats faced and risks that are associated, along with the businesses' own cyber security plan.

The cyber security awareness program should involve all retail employees working within the organization at all levels. Training and education should be experienced and received as a group, enhancing the spirit of teamwork and collaboration, and allowing for the proper and effective reinforcement of policies and standard procedures among employees.

Training and education can be supported by quizzes, contests and rewards, and can serve as a valuable way by which critical safety and security information is relayed by management and absorbed by employees.

In addition, any and all security awareness training should be reviewed and updated regularly in order to maintain its relevance, and is suggested to include content that covers the following:

- Social engineering
- Phishing
- Social media behaviour
- Online browsing habits
- Authentication practices
- Data handling
- Recognition and reporting of incidents
- Mobile devices
- Remote working

# xiii. When Support is Needed

Developing and overseeing an entire retail cyber security program to effectively protect an organization against the host of threats posed by cybercriminals is no easy task. This is especially true for small- and medium-sized retailers that may not have the expertise on hand required to do so, or the teams necessary to execute on all initiatives and ensure best practices are being adhered to among staff. As a result, it's important to understand when and where to get help to protect the business.

## When to Ask for Help

With so many different aspects involved in any robust cyber security plan, including the selection and implementation of an array of security solutions, the safe handling and management of mountains of data, the administering of ongoing training and education for staff, in addition to a multitude of other critical layers, managing it can be overwhelming for some. If you're concerned about your organization's level of cyber security preparedness and don't believe that you can meet all of the associated needs of the business, it's definitely time to reach out to third party service providers that possess the specialized knowledge to help. Depending on your cyber security needs, there are a number of companies that offer a range of services, including consulting and customer care, that could serve to benefit your organization immensely.

## Safeguarding Your Business

If your organization lacks the resources required to begin developing a comprehensive and effective cyber security program, or if you're operating within a tight budget, there are some free tools that can be found online that can help. However, retail organizations will want to be careful when researching these types of tools, making sure to confirm the legitimacy of the tools through verification of their sources and the review of user comments. It's important to understand that the development of any strong cyber security program and infrastructure will involve at least an initial investment, in addition to ongoing payments for continued services. It may seem to be a costly expense to some. But many cyber security software providers also offer vendor support, product warranties, installation and set-up technical support, and any updates that may be required along the way.

## When to Contact the Authorities

Despite the amount of tools and technical support that an organization has at their disposal, there are times when local law enforcement needs to be contacted. In cases of serious cyber attacks, which could include threats made or harm posed to employees or assets of the business, retailers should not hesitate to:

- *Report the incident to local law enforcement*
- *Report the incident on the National Cybercrime and Fraud Reporting System here, alerting the Royal Canadian Mounted Police (RCMP), the National Cybercrime Coordination Centre (NC3), and the Canadian Anti-Fraud Centre (CAFC), in order to protect the organization today and help safeguard it against similar threats in the future.*

# xiv. Cyber Security Self-Assessment

In order to help you and your company get started with respect to enhancing your cyber security efforts, this cyber security self-assessment is a great first step. In fact, reviewing and answering this short list of questions before reading this guidebook in its entirety will help IT departments and their teams better understand the current state of their cyber security capabilities and, by proxy, which portions or content within the guidebook might be worth highlighting and focussing on.

**Before answering, note that these questions have been developed assuming that your business, despite its size or format:**

1. Utilizes business computers,
2. Utilizes business mobile computing and communications devices,
3. Connects at least a portion of those devices to the Internet at least some of the time,
4. Contains and uses an intranet in order to internally share applications software, documents, and other pieces of information, sensitive or otherwise, with others.

To properly and accurately complete the self-assessment, circle one answer for each question asked. If you don't know the answer to the question asked, circle 'Don't Know'.

## Cyber Security Self-Assessment Questions

**1. Is cyber security currently a priority within your retail organization?**

0. Don't Know 1. No 2. Yes

**2. Is someone within your retail organization responsible for cyber security activities, strategy and performance?**

0. Don't Know 1. No 2. Yes

3. If you circled 'yes', is the individual working within an ongoing role that's supported by management? (circle if your response is 'yes')

**3. Has your retail organization ever conducted a risk assessment or threat analysis, or any other similar type of review, before?**

0. Don't Know 1. No 2. Yes

3. If you circled 'yes', have the risks and associated threats been prioritized and monitored in efforts to limit or eliminate them? (circle if your response is 'yes')

**4. Is there a cyber security plan or strategy in place within your retail organization?**

0. Don't Know 1. No 2. Yes

3. If you circled 'yes', are managers within the organization adhering to the plan or strategy? (circle if your response is 'yes')

**5. Are there cyber security policies in place within your retail organization?**

0. Don't Know 1. No 2. Yes

3. If you circled 'yes', are the policies supported by ongoing employee training or education? (circle if your response is 'yes')

**6. Is there an emergency response plan in place within your retail organization?**

0. Don't Know 1. No 2. Yes

3. If you circled 'yes', is the plan maintained and reviewed on a regular basis? (circle if your response is 'yes')

**7. Does your retail organization provide its employees with training and education related to the safe and secure handling and labelling of sensitive business and/or personal information?**

0. Don't Know 1. No 2. Yes

3. If you circled 'yes', is the training or education standardized for all employees and supported by policies? (circle if your response is 'yes')

**8. Does your retail organization provide its employees with training or education related to the secure use of mobile devices and/or computers?**

0. Don't Know 1. No 2. Yes

3. If you circled 'yes', is the training supported by mobile device management tools? (circle if your response is 'yes')

**9. Does your retail organization have a firewall installed between business computers (including the point-of-sale systems), and the Internet?**

0. Don't Know 1. No 2. Yes

3. If yes, is maintenance conducted on a regular basis by someone with the right amount of experience and training? (Circle if your response is 'yes')

**10. Does your retail organization leverage an encryption tool in order to secure digital communication before sending it outside of the business?**

0. Don't Know 1. No 2. Yes

3. If yes, have employees been trained concerning the use of such tools, and is their use monitored by IT? (Circle if your response is 'yes')

**11. Does your retail organization leverage spam filters in order to make email more secure?**

0. Don't Know 1. No 2. Yes

3. If yes, have employees received training concerning spam and phishing reporting? (Circle if your response is 'yes')

**12. Does your retail organization leverage anti-malware software?**

0. Don't Know 1. No 2. Yes

3. If yes, are all business computers within the organization equipped with it and updated regularly? (Circle if your response is 'yes')

**13. Does your retail organization encourage the use of strong passwords and passphrases?**

0. Don't Know 1. No 2. Yes

3. If yes, are password rules and policies enforced? (Circle if your response is 'yes')

**14. Does your retail organization regularly back up data and applications used within the business?**

0. Don't Know 1. No 2. Yes

3. If yes, are backups tested regularly and kept off site in the event of damage? (Circle if your response is 'yes')

**15. Does your retail organization have policies in place regarding securely working remotely?**

0. Don't Know 1. No 2. Yes

3. If yes, is remote work supported by the use of a virtual private network (VPN)? (Circle if your response is 'yes')

## What's Your Assessment Score?

When you've completed the questionnaire, add up the total of the circled numbers to the left of each response (0, 1, 2, and 3). Your total score will help you understand the level of cyber security within your organization and the work that might need to be done in order to enhance your business' security.

**0-15:** If you scored within this range, it's advised that you make it a priority to review this entire guidebook in order to better understand the importance of a solid and comprehensive cyber security plan for your organization. And, once you've read the guidebook and have amassed your own recommendations, begin meeting with colleagues and superiors to begin developing and implementing a cyber security strategy and supporting tools and procedures.

**16-30:** If you scored within this range, it could be suggested that your organization is aware of the risks associated with cybercrime, but that there's some more work and research to be done. In light of this, it's advised that you thoroughly review this entire guidebook, taking note of the areas in which improvements can be made to your organization's plan and strategy.

**Greater than 30:** If you scored within this range, congratulations – your organization seems to be on the right track toward maintaining a safe and secure digital environment for its retail brand, employees and customers. Though, given the rate at which the digital retail landscape is changing, it's always a good idea to continue reviewing best practices to remain in-the-know with respect to the latest in cyber security efforts.

## xv. Resources for Retailers

In order to assist retail IT leaders in their efforts to protect their retail organizations from the threats of cybercrime, below is a list of additional resources to reference and access when needed:

Retail Council of Canada's Retail Cyber Secure Program:
https://www.retailcouncil.org/retail-cybersecure-program-rcc/

Canadian Centre for Cyber Security:
https://www.cyber.gc.ca/

Canadian Centre for Cyber Security - Alerts and Advisories:
https://www.cyber.gc.ca/en/alerts-advisories

Canadian Anti-Fraud Centre:
https://antifraudcentre-centreantifraude.ca/protect-protegez-eng.htm

Government of Canada - Cyber Security:
https://www.canada.ca/en/services/defence/cybersecurity.html