RETAIL COUNCIL OF CANADA

RETAIL CYBERSECURE

MODULE 2

CYBER SECURITY FOR RETAIL MANAGEMENT

Securing your teams, devices, assets, and business.

A guidebook to help retail management 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

Management of a retail organization has traditionally required a great deal of focus and effort in order to achieve success. However, far more important than any other quality or characteristic that they could possess, a retail manager must above all be able and willing to adapt and evolve with continuously changing trends, consumer tastes and behaviour, employment standards and regulations, employee work preferences, and so much more. And, they've got to do so while organizing the entire operation, assigning and managing staff responsibilities, and overseeing the general performance of each individual as well as the overall business.

Today, most recent evolutions and industry forcing functions, driven primarily by the digitization of the world around us, are requiring retail management to also maintain the digital security of the operation, helping to prepare staff to protect against the threat of cybercrime. And, given the growth of the criminal underworld, the number and range of cyberattacks that are launched against unsuspecting businesses multiply tenfold every day. By targeting websites, email addresses, social media accounts, and other digital properties associated with a retail organization, cybercriminals hope to collect, by any means necessary, valuable sensitive business or personal information. And, the frequency of these attacks are increasing. According to a recent Mastercard study, there has been a 600 per cent rise in cybercrime since the start of 2020.

In light of this worrying trend, and in an effort to help retail management best prepare themselves and their staff to achieve and maintain a strong level of safety and security surrounding their digital environment in order to safeguard their businesses, Retail Council of Canada has developed the Cyber Security for Retail Management guidebook. Containing a host of practical information, suggestions, direction and best practices, the remainder of this guide is meant to serve as a go-to source and reference for retail managers in support of their efforts to protect their employees and retail organizations from the threat of a range 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, while more than a third said the hack strained their relationships with vendors or customers.
- **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

A big component of a retail manager's responsibilities when it comes to maintaining an organizations' security policy is to accurately recognize and prioritize a range of ongoing potential cyber threats and their associated risks to the business. And, just as important, laying the foundation for the organization's approach and efforts, management is also responsible for development of a thorough and comprehensive security plan that will be used as a document that will be updated and referenced on an ongoing basis, and which will be central to all employee awareness and training, with respect to the safety and security of the retail organization.

Define and Prioritize

Before understanding what tools and practices need to be put in place in order to ensure a safe and secure digital environment for retail organizations, management is critical 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, management must then 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. Categorize the threats to your business as low, medium, and high to help you get started.

Develop a Plan

As soon as threats and their associated risks have been identified by management, 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.

It's recommended that, despite the size of the retail organization, one member of management be assigned responsibility for the performance of the cyber security plan, including the implementation and updating of tools, the adherence of employees to standards and best practices, and the budget allocated for resources.

Employee Awareness

Management must ensure that all employees within the organization are well-versed and acquainted with the information within the cyber security plan and that they review it on a consistent basis, developing a deep understanding of the policies, procedures and tools meant to protect the digital integrity of the organization.

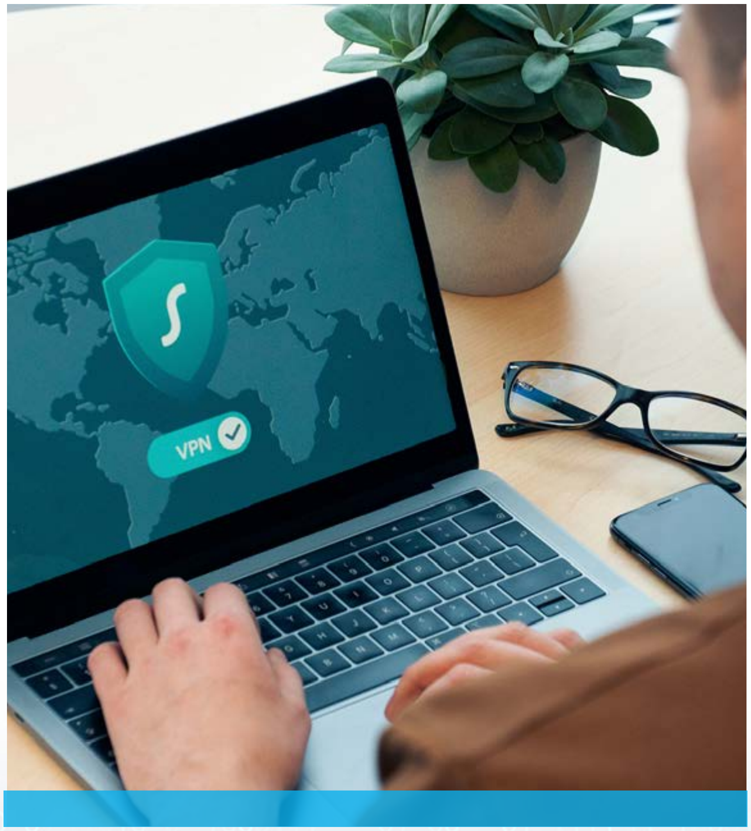
iii. Managing Cyber Security

Once an organization has recognized the fact that they, indeed, require a formal and comprehensive cyber security plan in order to protect the business from cyber threats, action needs to be taken in the way of building the plan, developing the policies, procedures and protocols that will be included and highlighted within the plan, and assigning individuals who are to be involved in actively enforcing the plan.

Developing Policies and Standards

In order to lend real meaning and teeth to any cyber security plan, a strong set of policies, procedures and protocols need to be developed and honed, outlining and explaining clearly employee do's and don'ts when it comes to cyber security. Management will play a critical part in developing these policies and procedures and will be responsible for their employees' collective adherence 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.

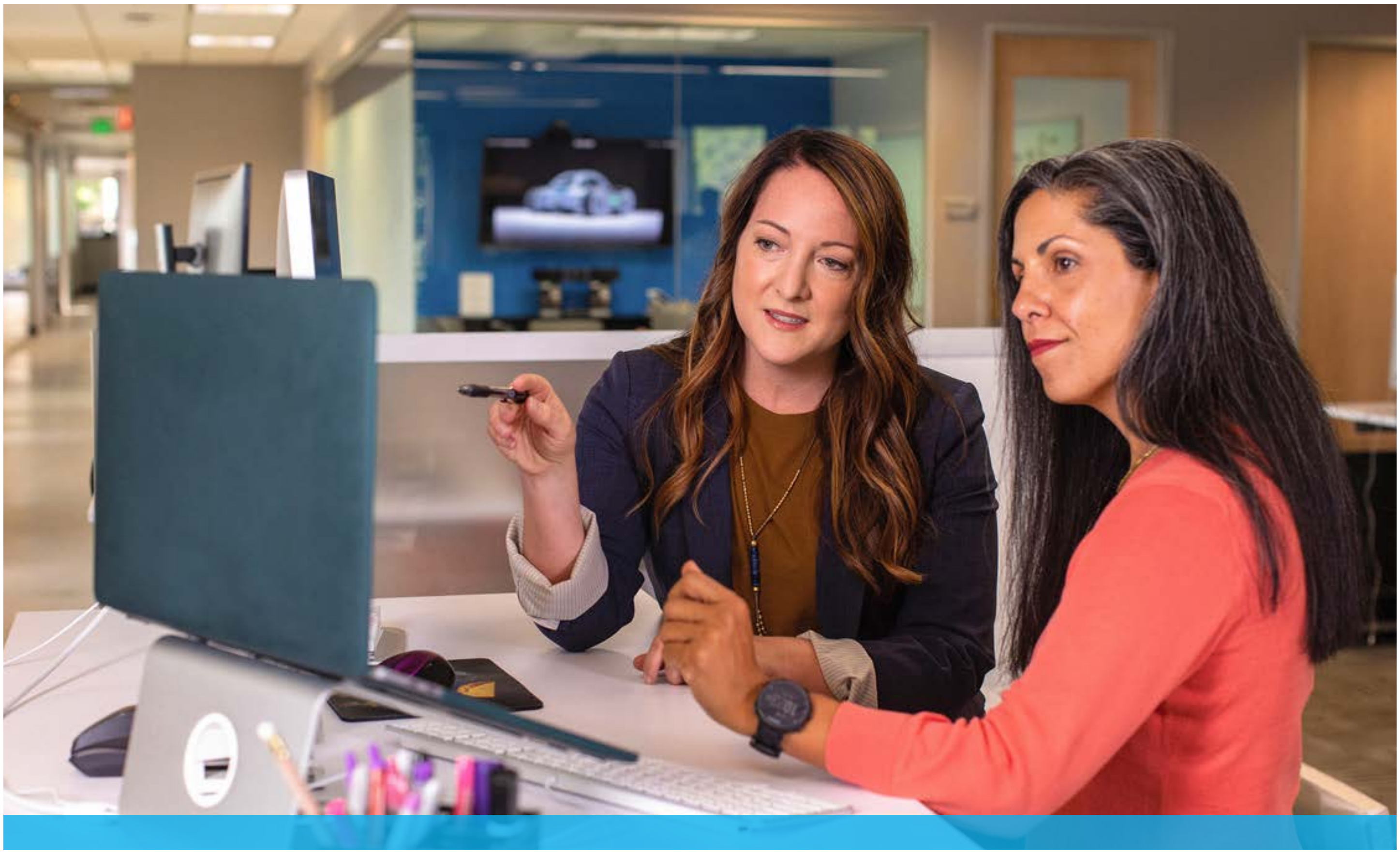


To further underscore these standards within the cyber security plan, they can be developed into standard operating procedure documents which are reviewed and referenced by employees on an ongoing basis.

When beginning to develop cyber security policies and procedures that are specific to their organizations, retail management 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, managers will want to incorporate as many effective existing policies and procedures as possible in order to maintain operational consistency and eliminate guesswork.



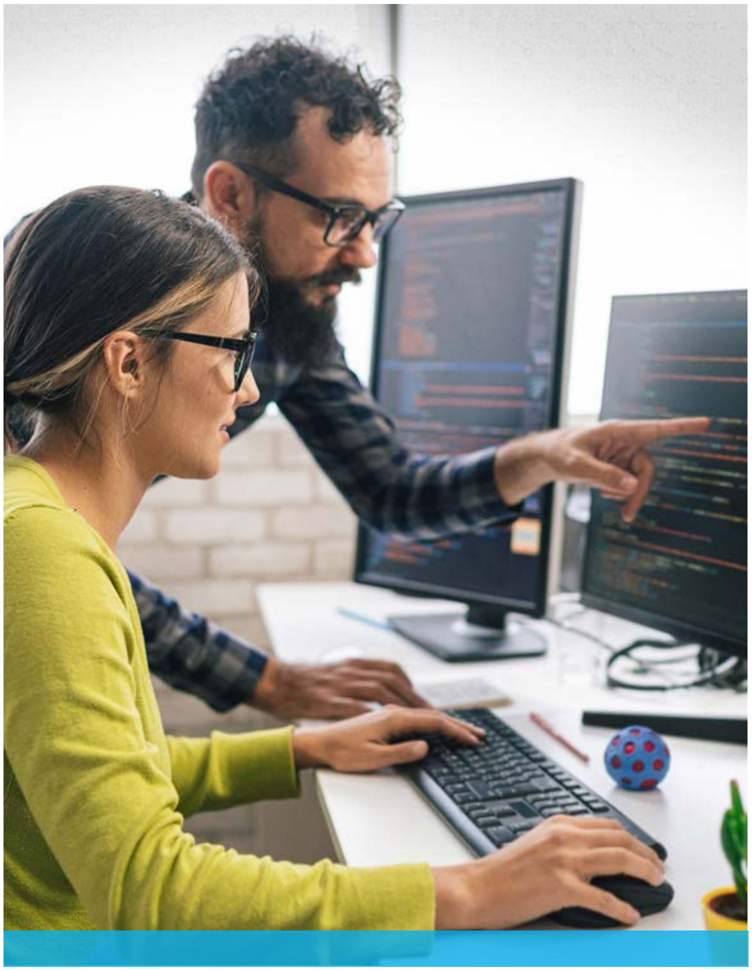
Explain rationale – In order for policies and procedures to have the greatest effect and impact, they should be explained to employees so they understand why they are in place and how they help to protect the business, its assets, employees and customers.

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.

Assigning Roles and Responsibilities

With a cyber security plan in place, it's time for management to assign specific roles and responsibilities to individuals, with one person charged with the following:

- Maintaining an awareness of current trends, threats and their associated risks to the business,
- Remaining on the cutting-edge of security tools and implementing them as necessary,
- Leading cyber security awareness and education within the organization,
- Ensuring that cyber security policies, procedures and best practices are being adhered to by all employees,
- Conducting consistent and thorough review and updating of cyber security tools and safeguards.



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 the support of management, 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.

Enhancing Security Awareness

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.

Within an organization's cybersecurity awareness program, management will want 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 be led by management and involve all retail employees working within the organization. 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.

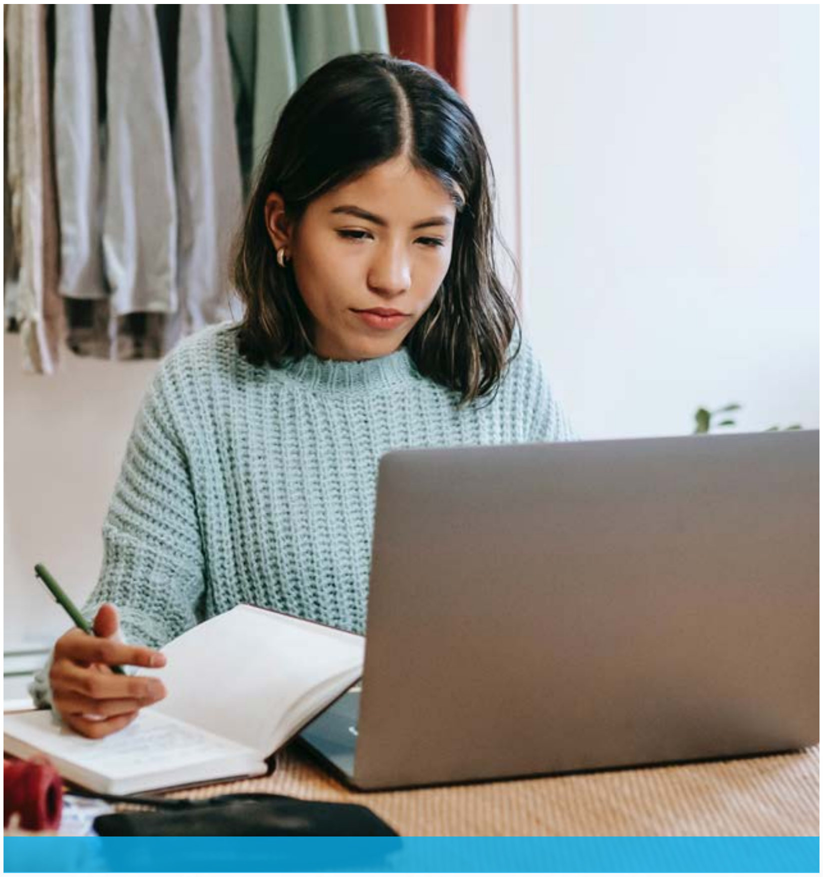
iv. Managing Web Security

When it comes to securing the digital retail ecosystem, it makes sense to begin safeguarding the Internet and everything else Web-related. Given the amount of Web-based activity conducted by retail employees, which can include the entering of personal and business information online, Internet browsing, and social media interactions it's best that management take a holistic approach toward safeguarding assets within the organization.

Protecting Personal and Business Information

There are a number of different situations within a retail organization that might necessitate an employee to enter personal and/or business information online, including everything from work being conducted with clients and partners, to the filling out of newsletter and magazine subscription forms and office supply order forms. This information could include details, both private and confidential, revealing full names, social insurance numbers, email addresses, phone numbers, physical addresses, and banking information, as well as details related to a number of other assets and entities. And, every time this type of information is entered, there are distinct cyber threats and associated risks involved.

In order to properly and effectively safeguard any retail organization against the range of threats posed by cybercriminals, it's imperative that management ensure that employees possess a deep understanding of the importance of Web security and the significance it represents for everyone involved. Cybercriminals prey on the vulnerable, and build their attacks on a foundation of personal and business information that they've collected by gaining illegal access to computers or systems. However, their potential impacts can be minimized if management ensure that all employees within the organization adhere to a handful of simple best practices:



Legitimate and trusted – Ensure that all employees using company computers and devices understand the importance of only visiting and sharing information with legitimate and trusted websites.

Source verification – Before sharing any personal or business information with anyone, employees should first verify that the entity asking for it is a trusted and verified source.

Ask questions – Whenever anyone is asking for personal or business information, employees should ask plenty of questions as to the reasons why the information is needed. And, if the response provided does not suffice, employees should be empowered to refuse providing the requested information until further details are received.

Maintain safeguards – Despite the reasons that might be given, none can justify the removal or disabling of security measures or safeguards, such as anti-virus and malware protection software, that have been put in place on computers and networks by the organization.

Ensuring Safe and Secure Internet Practices

The extent to which retail organizations rely on the Internet and its capabilities to undergo routine day-to-day tasks is immense. From mundane emails and research to common purchasing activities, there are a number of reasons that require a retail organization and its employees to browse the Internet. Although the use of the Internet is inherent and widespread today, and is a part of the everyday operations of just about every retailer, it's an excellent idea for management to ensure that everyone within the organization is exercising the right precautions when perusing the Web.

Policies and protocols – It's a very good idea for management to outline their expectations of employees when it comes to Internet browsing activities and behaviour. To do this, managers should develop their own internal Internet Usage Policy for the organization that clearly explains for employees the 'do's and don'ts' with respect to connecting to the Internet via the organizations' systems and devices.

Employee training – Once Internet policies have been developed for employees to follow, it's imperative that management provide them with ample training related to the Internet Usage Policy.

Promote awareness – In addition to the amount of training that employees receive from retail organizations around their Internet Usage Policy, it should also be administered frequently by management in order to promote continuous awareness and understanding.

Implement site-rating tools – As an added precaution, management can easily work with IT to equip employees' Internet browsers with a site-rating identification tool extension.

Ensure safe searches – As part of their ongoing training, employees should be shown how to properly confirm that the URLs of the websites that they're visiting are safe and secure by using an Internet site-rating identification tool.

Establishing Social Media Protocols

Among all of the channels that have cropped up over the course of the past number of years, social networking websites such as Facebook, X, Instagram, Pinterest, and more, have perhaps proven to be the most influential, providing retail organizations with a range of customer engagement and marketing opportunities to build stronger relationships and a more robust brand. However, given the popularity of these sites, they're increasingly becoming targets for cybercriminals looking to take advantage of online vulnerabilities in order to pilfer personal and business information from computers and systems.

In light of this threat, it's incredibly important that management include social networking protocols and best practices within their Internet usage policy, outlining for employees the proper conduct that should be followed on these sites.

Designate social networking individuals – It's a good idea to identify and designate a small handful of individuals who will be responsible for the organization's social media activity. Activity should be limited to these authorized individuals.

Identify information to be shared – Management should clearly define the type of information that can be shared on social networking sites. This can be included within the Internet Usage Policy.

Do not include sensitive information – Managers should ensure that employees never include sensitive personal or business information within the organizations' social media posts.

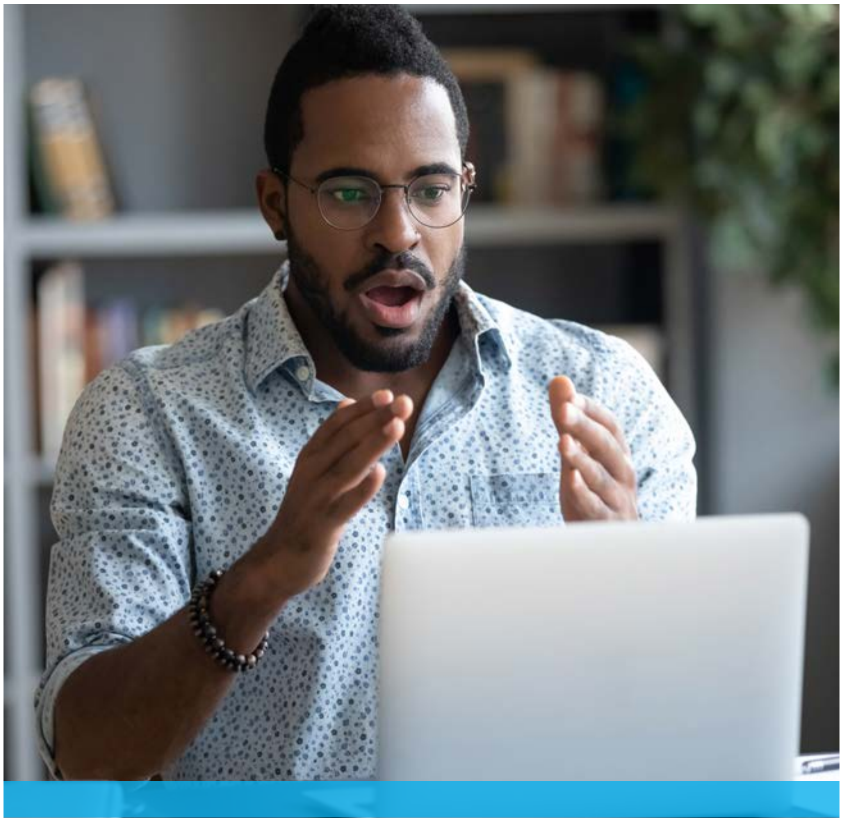
Be wary of social networking apps – It's wise to avoid using social networking apps, which are often developed and managed by third-party technology providers and may not be as secure as their websites.

Practice cautious communication – Whenever engaging with anyone on social networking sites, managers should ensure that their employees exercise caution, especially when being asked to share or provide information about the business or any of its employees.

Review information before posting – It's always a great idea to be thorough when communicating on social networking sites. And that means reviewing information before its posted.

It's also the policy of many retail organizations to allow their employees to check their own personal social media accounts while at work. If this is the case, management should advise them to follow the very same guides and best practices.

Protecting Against Social Engineering



As the means by which cyberattacks can be perpetrated increase, so too does the level of manipulation with which they are deployed. And, as manipulative tactics go, social engineering is one of the most effective ways that information is obtained by cybercriminals. By tricking employees within the organization, cybercriminals are able to gain access to computers, systems and information.

Leveraging what little information they might already have at their disposal, they'll communicate with employees, either online, by email or over the phone, gaining their trust through seemingly honest behaviour. They'll often claim to be a client or partner of the company or close associates with one of the employees' colleagues. They may even attempt to offer manufactured "proof" of their "legitimate" connection to the business. Some may go as far as to impersonate a government official or other figure of authority, requesting information such as phone numbers or account information. In some instances, they may instruct individuals to open emails and attachments or to visit particular websites.

Because manipulation is the tactic, most victims are unsuspecting of the incident until it's far too late, and only then begin to realize the very real fallout. In order to avoid these scenarios, and to properly protect the organization, its assets and people, management should ensure that their employees are aware of such scams and to be vigilant concerning these types of communications with outside sources.

Be on guard – It's a good idea to advise all employees of the organization that they should be wary of any and all emails, phone calls and visits that they receive from individuals claiming to be connected in some way to the business or anyone working within it.

Ask for verification – Managers should ensure that their employees ask every individual requesting any type of information to verify their identity with official documentation.

Follow Web security best practices – Whenever in any kind of doubt with respect to proper protocol, managers should let employees know to refer to all other best practices for conduct related to email, social networking, Internet activity, and other Web activity.

Ensuring Software Security

Despite the amount of best practices that management develops, or the level of training and education that they provide for their employees, any cyber security program is only as good as the software that's used to protect the organization. In fact, strong features and safeguards that ensure the security of software deployed within an organization can actually serve to mitigate and eliminate a number of different cyber threats altogether.

However, software, most commonly found within desktop and mobile device apps, Web servers and operating systems, can often contain or develop "bugs" that can create vulnerabilities, making them less secure and open to the exploitation and attacks of cybercriminals. In addition, software can, at times, become infected with malware.

In order to avoid security lapses related to the software that your organization is using, management should work with IT to ensure that software security is maintained by doing the following:

Use legitimate software – It's critically important that management ensures that the organization uses only legitimate software. In addition, they should make sure that it's been tested and used by others prior to use within the organization. And, **DO NOT** use unauthorized versions of software – these versions are often corrupted and/or infected and can cause serious harm to your organization's systems.

Limit access – Management should limit access to shared applications to those who require it in order to perform their jobs and execute on their responsibilities. And, the number of employees granted administrative privileges should be managed as well, ensuring that the organization's vulnerabilities are minimized and targets for potential cyberattacks reduced.

Apply regular updates – It's important to make sure that any and all software updates, often referred to as "patches", are applied as soon as they become available.

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'shosting preference, there are some recommendations to follow.

Hosted on internal servers:

Restrict access – Allow only authorized employees to gain access.

Apply upgrades – It's important to work with IT to make sure that all available upgrades have been applied to operating systems in order to avoid issues and vulnerabilities.

Back up regularly – Managers should make sure that business systems are backed up regularly, preferably to a server housed at a separate location.

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 – Management 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 management are 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. Managers 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.

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.

What is Malware?

Malware, or malicious software, is any nefarious software designed, developed and deployed with the intent to damage a system and/or illegally obtain information. And, because malware is meant not to be seen, it's often able to reside among the operating systems of desktop computers, laptops, smartphones and tablets, without being detected or removed by security safeguards.

What Types of Malware Exist?

There are a number of different types of malware. The most common, and arguably the most effective, is the 'virus', which is capable of infecting operating systems before making a copy of itself and infiltrating another device. However, there are a number of other types of malware that retail businesses and their employees should be aware of. They include:

Worms – Similar to viruses, worms spread independently, without the need to attach to other files or programs.

Trojans – Disguised as legitimate software, trojans trick users into installing them.

Ransomware – Encrypting files on a victim's computer allows attackers to demand a ransom in order to grant access back.

Spyware – Designed to secretly collect information about a user's activities, typically without their knowledge or consent, spyware can capture keystrokes, monitor browsing habits, and collect personal information from the unsuspecting.

Adware – Displaying unwanted advertisements on a user's device, while not always malicious, adware can be intrusive and negatively impact system performance.

What's Malware's Purpose?

Most commonly originating as email attachments or website downloads, malware is designed to infiltrate operating systems within digital devices, infecting files, corrupting or deleting them altogether, allowing for the illegal capture of sensitive information.

What Can Retail Managers Do?

Although malware is often incredibly effective in serving its purpose, there are a number of things that management, in conjunction with IT, can do in order to safeguard their business, systems and digital information.

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, many firewalls are also able to prevent many types of malware from even entering the system

Provide employee training – Along with the implementation of anti-malware software and firewalls, all employees within the organization should receive ongoing security awareness training and education.

Heed warnings – All employees within the organization should be made aware of warnings on websites and emails of potentially malicious content, and heed those warnings fully.

Report alerts – If a report or warning is received by an employee from the anti-malware software implemented on a retail organization's computer or device, it should be immediately reported to management.

Isolate suspicious emails and files – Employees should be advised to never open, forward or share suspicious emails or attachments with others.

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 management.

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 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, some retail managers might want to suggest the use of any one of a number of free online 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 managers 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.*

v. Managing a Secure 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 retail managers to work with IT in order to ensure the utmost in payments security for their customers.

To enhance the security of POS systems, retail managers will want to work with IT to ensure that they do the following:

Firewall is in place – Placing your POS system behind a security firewall is a must, and the only way in which to restrict the number 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.

Create 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 to.

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.

vi. Managing Secure Digital Communications

Most, if not all, communication between colleagues, associates and business partners today is conducted via email. However, as mentioned, email is increasingly being 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 ensure the utmost in protection and security when working with email, management should make all employees aware of the most common ways by which cybercriminals attempt to leverage email to their advantage.

Spam

Representing the vast majority of email communication that's sent over the Internet, Spam is email that has been sent unsolicited and without the recipient's permission, and is often disguised as product or service promotion or an offer that can be redeemed by clicking a link or visiting a website. By proxy, spam is incredibly intrusive and annoying to receive. However, if links are clicked or attachments are opened, malware is often downloaded onto the computer that it was accessed on, slowing down networks and servers, resulting in increased costs and a downturn in productivity.

Management will want to ensure that their employees are mindful of the messages and emails that they're receiving and that they are cautious to identify possible spam messages.

Sender recognition – Employees should treat any communication that comes from an unknown sender with caution.

Spelling mistakes – In order to circumvent spam filters and other security features, cybercriminals will intentionally misspell words in the subject line of the email. Employees should not ignore this obvious flag.

Awkward phrasing – In addition to misspelled words, the body of the email communication will often contain awkward or unusual phrasing, indicating that the sender is perhaps not legitimate.

Be wary – If the email promises offers that seem too good to be true, requests that links within the message be clicked on, or asks for personal or business information, it's likely spam.

In order to protect against the negative impacts of spam, management will also want to keep all employee email lists secure and confidential. And, they should consider developing a fundamental set of rules and guidelines for employees to follow with respect to email, advising them of the following:

Never click on links – Managers should make sure that employees know not to click on any links or open any attachments within the spam email

Never respond to sender – Employees should be advised to, no matter what, refrain from responding to the sender of spam, which would ultimately confirm that the address, or target, is real and active.

Delete – If employees are certain that an email is spam, they should go ahead and delete it. If they're uncertain, they should be advised to bring the matter to IT or management.

Phishing

An extremely pointed and specialized type of spam, phishing email communications are designed to look exactly like a legitimate message, and are often disguised as communication from a government agency, banking institution or other official organization. Often, these types of spam communication are painstakingly developed, sometimes using real logos, fonts, colour palettes, and imagery, and are indistinguishable from legitimate communication.

The purpose of phishing emails are similar to that of spam. However, their tactics are a little different. Rather than promote a service or product, phishing emails typically use either a helpful tone to engender trust, or intimidating messaging to create fear, each with the objective of eliciting a response or the clicking of a link.

The scope of phishing attacks is constantly expanding, but frequent attackers tend to utilize one of these four tactics:

Embedding links into emails that redirect users to an unsecured website requesting sensitive information.

Installing Trojans via a malicious email attachment or posing ads on a website that allow intruders to exploit loopholes and obtain sensitive information.

Spoofing the sender address in an email to appear as a reputable source and requesting sensitive information.

Attempting to obtain company information over the phone by impersonating a known company vendor or IT department.

Ways to Block Phishing Attacks

Employees should always be suspicious of potential phishing attacks, particularly when they don't know the sender. Here are five best practices for management to enforce in order to help make sure employees don't become helpless victims:

1. Don't reveal personal or financial information in an email – Make sure employees know not to respond to email solicitations for this information, including clicking on links sent in the emails.

2. Check the security of websites – This is a key precaution to take before sending sensitive information over the Internet. <http> indicates that the website has not applied any security measures, while <https> indicates that it has. With this in mind, employees should practice safe browsing habits while also understanding that websites that do not serve a legitimate business purpose are also more likely to contain harmful links.

3. Pay attention to website URLs – Not all emails or email links seem like phishing attacks, so employees may at times be lured into a false sense of security. Many malicious websites trick end users by mimicking legitimate websites. One way to figure out whether or not the website is legitimate is to look at the URL (if it's not hidden behind non-descript text). Employees may also be able to detect and evade the scheme by finding variations in spellings or a different domain (e.g.,.com versus .net).

4. Verify suspicious email requests – Contact the company the emails are believed to be from directly. If an employee receives an email that seems suspicious from a well-known company, such as a bank, reach out to the bank using means other than responding to the suspicious email address. It's best to contact the company using information provided on an account statement—NOT the information provided in the email.

5. Keep a clean machine – Ensuring the utilization of the latest operating system, software and Web browser, as well as antivirus and malware protection, is the best defense against viruses, malware and other online threats. IT and management should work together to develop a list of approved and safe Web browsers.

What to Do with Phishing Emails?

It's important to make employees aware of the prevalence of phishing scams and protocol concerning the way in which they report a suspicious communication. In most cases, employees should be instructed to avoid sending and sharing the message with anyone else, and instead save it in order to show a supervisor or manager and wait for further instructions.

Management should contact IT to inform them of the phishing email. IT will want a copy of the email so that they can investigate and block the source. They will provide instructions for you to follow.

Ensuring Secure Email Communication

Just as important as safeguarding against spam and phishing is, management also need to educate employees concerning the safe and secure sending of email communication, ensuring the following:

Authorized emails only – Ensure that only authorized employees send emails from the organization.

Maintain confidentiality – It's important to instruct all employees to maintain the confidentiality of their email messages and contained attachments until sent.

Archive sent emails – It's important to ensure that employees archive all sent email in the event that they are required for future reference for any reason.

vii. Managing 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 – Employees should be instructed by management to 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.

viii. Managing Secure 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.

The Basics of Remote Computing

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 policies.

As a result, it's a good idea for management to work with 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's advised by most to combine the use of a VPN with other safeguards and layers of protection mentioned throughout this guidebook, and that management ensure that employees follow a set of best practices related to the security of remote access working.

Limit access – Management should limit remote access 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.

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

Adjusting access – It's important to allow for the adjustment of remote access privileges in the event that responsibilities of individuals within the company change.

Assigned computers – It's a very good idea to provide employees with remote access 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 – Before assigning business computers and other devices to employees with remote access, they should all be labelled by management, with serial numbers recorded, in order to help track their configurations or with their recovery if they are ever lost or stolen.

Working From Home

The most common remote access arrangement is work-from-home. It's a simple and convenient way for employees to connect with their employer. However, if using a personal computer to do so, additional risks could be exposed, providing management with a few requirements to take care of in order to increase the security of work-from-home.

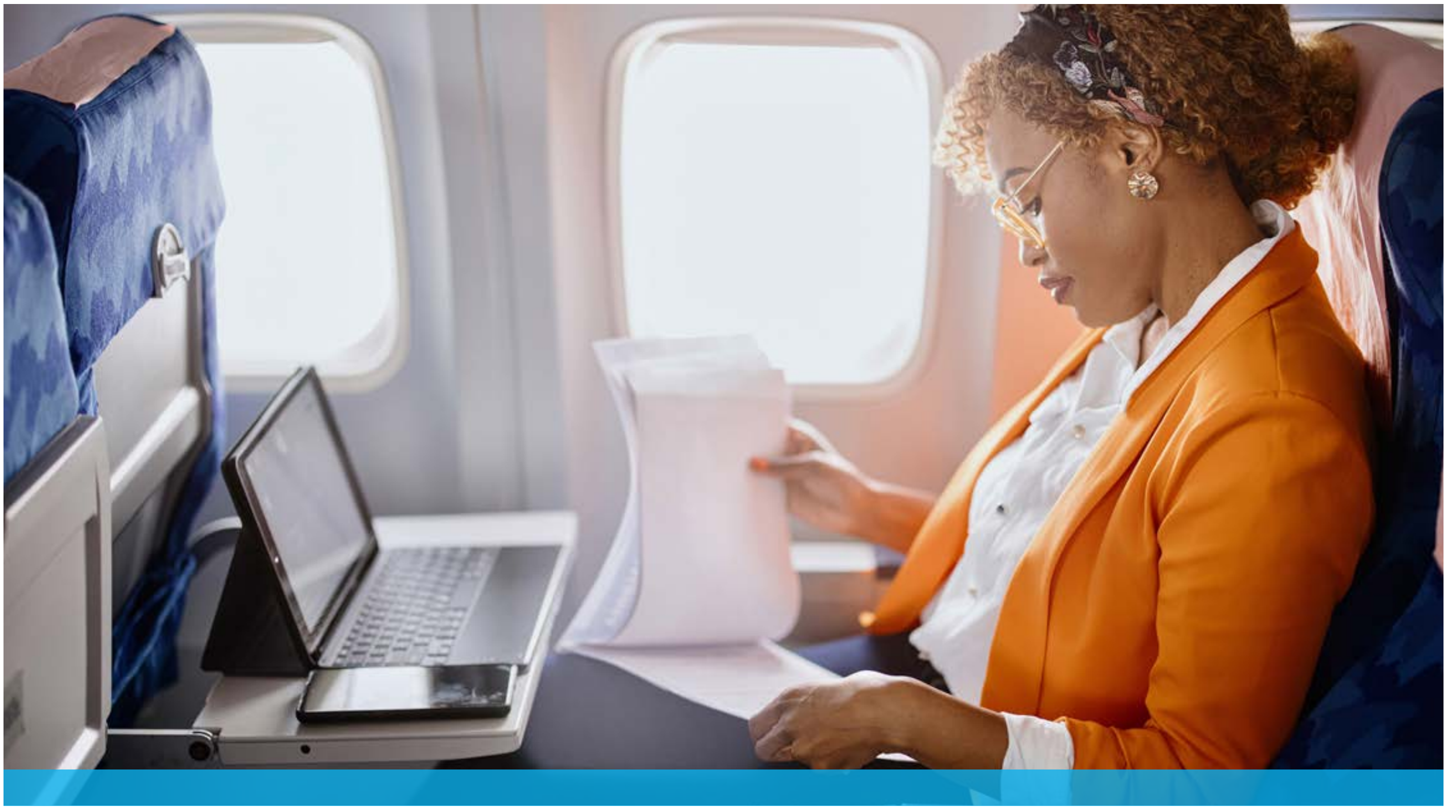
Restricting wireless access – All employees, when working from home on personal computers, should be advised to connect their computer directly to a router using an Ethernet cable, and to connect the Ethernet cable to the modem, in order to prevent anyone outside of the network from listening to, or intercepting, communication.

Secure Wi-Fi – Employees should be advised to secure their Wi-Fi connection in order to prevent cybercriminals from gaining access to sensitive business information.

Change default network name – Employees working from home should change the default Wi-Fi network name and the router access password on the network router. This will allow for a more secure connection.

Network encryption – Management should ensure that network encryption is turned on by IT, preventing any intercepted communications and sensitive information from being used by cybercriminals.

Limited access – In addition to digital safeguards and security features, employees working from home on their personal computers should also be advised by management to be vigilant in taking physical precautions, limiting access to the computer that they do their work on.



Working While Travelling

The digitization of the world around us, combined with a new working reality, means that today's retail business is very much a portable one, allowing employees to work wherever and whenever they want, including while travelling and on the go from one destination to another. As a result, data and information housed within a retailers' digital ecosystem becomes that much more exposed to risk, requiring management to advise employees to exercise caution and to follow best practices when working while travelling.

Avoid questionable connections – When on the road, working from a hotel or airport, or anywhere in between, employees of retail businesses should always avoid using unknown or questionable Wi-Fi connections. Although they may be free, they are often not very secure.

Keep your devices close – Employees should be advised to never, ever leave their work devices, whether laptop, tablet or smartphone, unattended while working in a public workspace or anywhere else while on the road.

Protect confidential information – It's always a good idea for employees to protect any confidential or sensitive business information from being seen by those around them while working in public workspaces. Managers should suggest that in these cases screens should be dimmed and that employees sit in an area where the screen cannot be viewed from any angle.

Note: All organizations should have a mandatory policy in place for the reporting of lost or stolen devices which all employees need to review and sign off on. The policy should provide various means for employees to contact the company's IT support or help desk at any time.

ix. Managing Digital Device Security

Some of the more significant and important components and 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 finding a breach. Therefor, it's becoming incredibly important for retail managers to properly oversee the use of these devices that are mobile and in frequent use.

As part of management'sresponsibility concerning the supervision of the use of digital devices, and in an effort to alleviate security risks and concerns, the following considerations should be made:

Pros and cons – In order to understand which devices are must-haves for use within the organization, it's a good idea to make a simple pros and cons list for each.

Approved devices – Based on the pros and cons list, a collection of devices that will be permitted for use within the organization can be developed.

Is it personal? – It's important to determine whether or not personally-owned mobile devices will be allowed for business use within the organization.

Develop rules – Despite the device, specific rules should be developed and applied to all, incorporating these rules into the standard operating procedures within your organization's cyber security plan.

Develop a plan – The development of a mobile device plan, which includes all of the do's and don'ts concerning mobile device use, is a good idea and allows retail managers to effectively safeguard against threats and associated risks.

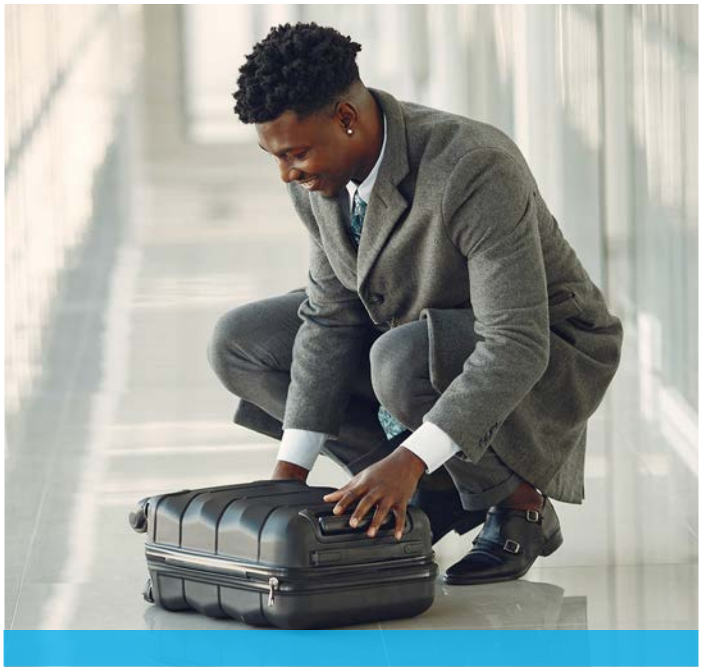
Record serial numbers – It's a really good idea to record the serial numbers of all mobile devices being used by employees within the organization in case of loss or theft.

In order to maintain consistency, and to enhance the level of cyber security within an organization, management should develop specific rules that cover the use of each type of device.

Tablets and Smartphones

Some of the most common devices used by retail businesses and their employees, tablets and smartphones are unfortunately also some of the most targeted items for theft. And, if a tablet or smartphone issued by a retail business goes missing, it's 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, there are a few considerations that retail managers need to make their employees aware of.

Take precautions – It's important to ensure that employees understand that they should treat their tablets and smartphones with the same care and security precautions as they apply to other tools, like laptops and personal computers.



Systems access – Employee devices should be locked when not in use, and set up within the retailer's system to be accessed by password only, thereby protecting sensitive information, data, and network tools.

Safe and secure – While travelling, or en route from one destination to another, employees should ensure that proper safeguards are in place in order to protect the security of sensitive information contained within communications.

Frequent back up – Managers must ensure that employees are regularly backing up the contents on their devices.

Use security apps – Managers should work with IT to ensure that any appropriate and effective security apps are installed, leveraging encryption, locators for lost devices and anti-malware.

Reporting loss – *A policy should exist that prescribes the procedure* for employees to promptly report the loss of a business tablet or smartphone as soon as the loss occurs so law enforcement can be notified and efforts can be made to recover the device.

Portable Data Storage

Many retail businesses leverage the use of portable data storage devices, including portable hard drives and portable flash drives. They present a quick and easy way to transport large files and documents from one device to another. However, these devices also represent, yet again, another potential way by which cybercriminals can infiltrate a business' systems or networks. As a result, retail managers need to ensure that their employees exercise precaution when using portable data storage devices.

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.

Identify rules – Management is responsible for identifying the rules of use for each device that's used by employees within the organization. It should be made clear what information can and cannot be stored on a portable device.

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.

Train employees – It's paramount that management ensure that all employees are trained concerning the safe handling of portable storage devices.

x. Managing a Secure Physical Space

Although the safeguards and layers of protection that will be put into place in order to secure the digital retail landscape, like authentication and encryption, are obviously necessary, the critical physical aspects of security can not be forgotten in order to ensure the utmost effectiveness of a retailer's cyber security efforts.

Ensuring Employee Security

In order to ensure the safety and security of the physical retail space, the role and responsibilities of management are significant, from the hiring of employees through to the execution of their day-to-day tasks.

In order to ensure that your retail organization hires employees who exemplify honesty and trustworthiness, it's important that management be thorough throughout the hiring and onboarding process and that they maintain consistent focus concerning the practices and behaviour of employees. Here are some specific recommendations for management to ensure that employees understand their roles within your organization's cyber security efforts:

Develop a security policy – It's of paramount importance that management play a key role in developing, publishing and maintaining an organization-wide security policy that clearly defines rules and proper business conduct, in addition to any discipline that might occur, up to an including termination, if a security breach were to happen as a result of employee negligence.

Perform background checks – It's imperative that retail managers conduct comprehensive and thorough background checks on all potential employees of the brand. And, be aware that simply checking references may not suffice given the sophistication of most cybercriminal activity.

Define non-competition rules – At the onset of employment, management should be clear concerning all non-competition, non-disclosure, intellectual property rules and contractual obligations that might be relevant within the context of the organization. For instance, management should let all new hires know that sharing confidential information outside of the organization is not permitted.

Communicate responsibilities – Management should make security training, including the clear communication of security responsibilities to newly hired employees, an integral part of the employee onboarding process. In addition, this is a great time to introduce the organization's security policy and a thorough review of its contents.

Terminate access – If an employee within the organization is leaving, either as a result of termination or resignation, it's critical that management ensure that the departing employees' access to business computers, systems, email accounts, and any other digital touchpoint, be terminated immediately to avoid any possible security lapse.

Managing Employee Practices

It's important to note that any retail organization's best security efforts can be severely limited if its employees aren't fully educated and invested in ensuring a safe and secure environment in which to work. In light of this, it's important for management to be aware of the common "messy desk" mistakes that everyone is prone to occasionally make, ensuring that their employees avoid the following:

Leaving computer screens on without password protection – Anyone passing by has easy access to all of the information on the open device. Employees must be sure to lock down screen settings.

Placing documents on the desk that could contain sensitive information – It's best to keep these types of documents locked up in drawers and file cabinets.

Forgetting to shred documents before they go into the trash or recycling bin – Any document may contain sensitive information. It's best to shred everything rather than taking a risk.

Failing to close file cabinets – This makes it easy for someone to steal sensitive information and more difficult to realize a theft has occurred.

Leaving mobile phones and USB drives out in the open – These types of devices likely contain sensitive business or personal information and are easy to pick up quickly without being noticed.

Neglecting to erase notes on whiteboards – They often display confidential information concerning products, new ideas and proprietary business processes.

Leaving backpacks out in the open – There's often at least one device or folder with sensitive information inside everyone's backpack or bag.

Writing usernames and passwords on slips of paper or post-its – It's especially important to avoid doing this given the fact that usernames and passwords are typically used to log into more than one site.

Leaving behind a key to a locked drawer – This makes it far too easy for someone to come back later, perhaps after hours when no one is around, and access confidential files.

Displaying calendars in the open or on the screen for all to see – Calendars often contain sensitive dates and/or information about customers, prospects and/or new products. Managers should make sure that employees keep them filed away or hidden from view.

Leaving wallets and credit cards out on the desk – This is more likely to impact the employee, but wallets may also possess corporate credit cards and security badges that should be kept safe and secure.

In addition, managers should ensure that when their employees are not at their workstations, that they are following best practices, which include the following:

Out of sight – When employees are not at their physical work stations, any files, documents, CDs, USB memory sticks, or anything else that contains sensitive or confidential data and information, should be put away and out of sight, including information about the business, personal information, and customer information.

Lock up – Employees should always disable their computers whenever they leave their work stations. This can be done within most systems by entering a combination of keys. The computer can then be accessed again by its user by entering their password.

Limited Access

Further, it’s important that management within the organization limit access to certain parts of the physical space, granting it only to employees who need access in order to perform their jobs and fulfill their responsibilities. For instance, employees outside of the IT department rarely need access to the servers. These areas should be locked and monitored at all times to avoid security mistakes.

xi. When Support is Needed

Managing 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, retail managers 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.*

xii. Cyber Security Self-Assessment

In order to help you and your staff 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 retail managers 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')

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.

0-7: 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.

8-14: 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.

15-23: 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.

xiii. Resources for Retailers

In order to assist retail managers in their efforts to protect their employees and 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