Cyber™

PREPARE | PREVENT | MITIGATE | RESTORE

TRAVELERS INSTITUTE®

TRAVELERS

Empowering Canadian organizations to tackle evolving cyber threats.

A CYBERSECURITY GUIDE

FOR SMALL AND MIDSIZED BUSINESSES

TABLE OF CONTENTS

EVOLVING CYBER THREATS IMPACT BUSINESSES AND ORGANIZATIONS OF ALL SIZES, SECTORS AND INDUSTRIES.

INTRODUCTION

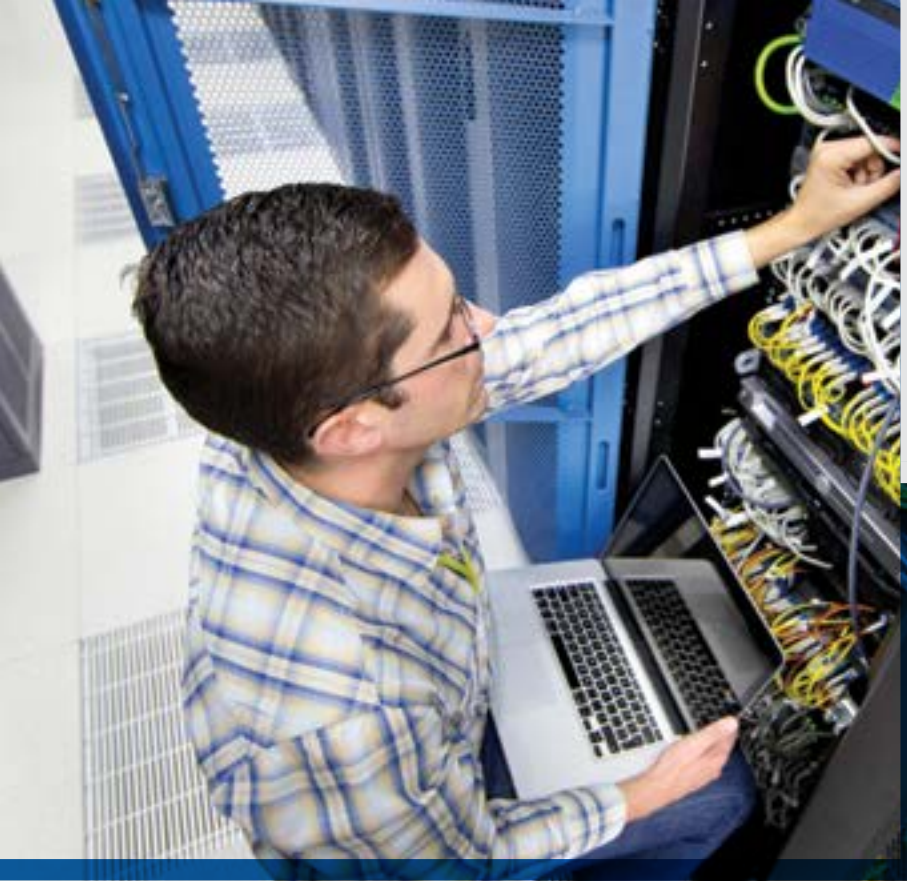
News headlines routinely feature high-profile data breaches and computer intrusions, with large corporations working around the clock to contain the damage to their business, their customers and their reputations. But research shows that cyber criminals are also attacking smaller "Main Street" businesses and organizations that are often less prepared to prevent and respond to an attack. In fact, evolving cyber threats impact businesses and organizations of all sizes, sectors and industries. There has been a steady increase during the past five years in attacks targeting businesses with fewer than 250 employees; now, over 60 percent of all targeted attacks strike small to midsized entities.[1]

Experts believe it is not a question of "if" your organization will suffer a breach, but "when." Just one resourceful hacker, one disgruntled employee or even lost physical records of customer data or your own organization's proprietary information can cause enormous financial and reputational damage. The costs of a data breach can be staggering, averaging $211 per compromised record and $4.98 million per data breach in Canada in 2015 and 2016.[2] Combined with a damaged reputation, these losses can devastate an unprepared organization.

With this in mind, the Travelers Institute, the public policy division of The Travelers Companies, Inc., launched its *Cyber: Prepare, Prevent, Mitigate, Restore*™ educational initiative, convening the business community with cyber thought leaders from the public and private sectors. Working with cybersecurity experts, government agencies and insurance industry professionals, the *Cyber: Prepare, Prevent, Mitigate, Restore* series provides business owners with the information and resources needed to meet the challenge of cybersecurity.

In this guide, we offer fundamental safeguards that can be used by small and midsized organizations to improve their cybersecurity. These safeguards, identified by Travelers Canada cyber risk professionals in the course of helping policyholders manage their cybersecurity risks, can help any organization be more prepared, and better able to prevent intrusions, mitigate damage and restore normal operations when the hackers come to call.

IN THIS GUIDE, WE OFFER FUNDAMENTAL SAFEGUARDS THAT CAN BE USED BY SMALL AND MIDSIZED ORGANIZATIONS TO IMPROVE THEIR CYBERSECURITY.



Preparation is critical.

BE PREPARED:

- KNOW YOUR DATA, SYSTEMS AND NETWORK
- FOCUS YOUR CYBERSECURITY EFFORTS
- VALIDATE YOUR BACKUP STRATEGY
- PLAN FOR INCIDENT RESPONSE

PREPARE – PREVENT – MITIGATE – RESTORE

One of the cornerstones of cybersecurity is preparation. In a world where resources are limited, you must know what systems you are running, what data you are storing and how your network is structured to allocate your cybersecurity resources effectively.

Implementing strong security controls is not enough, however, as we all know that organizations with strong security can be compromised. Accordingly, it is important to maintain regular backups of important data and to have an incident response plan in place to rely on when an incident occurs.

Know your data, systems and network

Businesses and organizations typically store many kinds of data, using a variety of computer systems, on networks that may be local, global or somewhere in between. So, the first principle of cybersecurity is "know thyself." Know what (and where) data are being created, collected and stored; maintain an accurate inventory of computer systems and software; and understand your network infrastructure.

This enables you to better:

- Identify and prioritize appropriate security controls.
- Remove unauthorized systems and software from your network.
- Patch and maintain existing systems and software.
- Recognize new vulnerabilities in existing systems and software.
- Respond more effectively when an incident occurs.

There are many kinds of data that can be found on a system or network, including the following:

Protected
Health
Information

PHI

such as health or medical records of patients or employees.

Payment
Card
Information

PCI

such as credit or debit card account numbers.

Personally
Identifiable
Information

PII

such as names, addresses, telephone numbers, Social Insurance Numbers or other identifying information.

Intellectual property

such as manufacturing processes, marketing strategies and other trade secrets.

Other proprietary information

including confidential information shared by a business partner.

In many cases, it may be appropriate for your organization to adopt a data classification scheme. A certain kind of data may warrant stronger security controls if it is particularly valuable to the organization, if its loss would be particularly damaging or if it merits special treatment in light of legal or contractual obligations.

Next, a systems and software inventory should be maintained to identify every device that has access to the network, including desktops, laptops, mobile devices, servers, network equipment and printers. The inventory should identify a specific person responsible for each device (by name and job title), as well as the device's network address and physical location.

Organizations should also maintain an inventory of software applications, identifying the systems (including servers, workstations and laptops) on which they reside.

Any systems or applications that are not authorized should be investigated and removed.

Finally, it is important to maintain accurate information about the structure and topology of an organization's network. This information can be used during the normal course of business to ensure that changes to the network are consistent with existing network security controls. It will also be invaluable in the course of responding to a cybersecurity incident.

Focus your cybersecurity efforts

Once you understand the data, systems and network that you are trying to protect, you can focus on implementing (or improving) the security controls that would be most effective in light of your specific needs and resources. (You will also be better prepared to work with a cybersecurity consultant, if you choose to do that.)

Consider the following:

What are your "crown jewels"?

If you have adopted a data classification scheme, you will want to implement stronger security controls for the storage and transmission of data that are classified as more sensitive.

What are your vulnerabilities?

A vulnerability assessment can help identify weak spots in your cybersecurity that deserve greater attention. If your organization permits systems or network access to outside parties, such as contractors or vendors, understand that their vulnerabilities become your vulnerabilities.

What are the most likely threat scenarios?

If you understand the threats that are most likely to impact your business or organization, you can focus on minimizing those threats.

COMPLIANCE WITH A PARTICULAR CYBERSECURITY STANDARD IS NOT A PREREQUISITE TO GOOD CYBERSECURITY, BUT IT CAN BE IMPORTANT IN DETERMINING WHICH SECURITY CONTROLS TO IMPLEMENT. BUSINESSES THAT HANDLE PAYMENT CARD INFORMATION, FOR EXAMPLE, MUST COMPLY WITH THE PCI DATA SECURITY STANDARD.

Extensive information about computer and network security controls is freely available online, including comprehensive taxonomies of security controls that can help ensure that you are not omitting one that would be valuable to your organization.[3]

Here, we highlight a few fundamental security controls:

Strong passwords: Almost all systems can be configured to require users to select passwords that would be difficult for an intruder to compromise. Users should be instructed not to use passwords (or variants of passwords) that they use elsewhere (e.g., to control access to personal email or other internet accounts).

Firewalls: Firewalls are used to permit only appropriate traffic to enter and leave a system or network. Like any other security control, a firewall must be properly configured and maintained to be effective. Firewalls should only permit network traffic that is appropriate to the needs of the business or organization. For example, file transfer requests to a company's email server should probably be rejected.

Anti-virus: Anti-virus software is designed to defend your network against malicious software ("malware"). To maintain an effective defense, your anti-virus software should run in the background at all times and be continually updated. The ability to quickly install anti-virus updates on all systems is critical.

Content filtering: Content-filtering controls restrict material delivered over the internet via the Web, email or other means. They enable a company or organization to block attachments in emails or material from websites that are likely to include spyware, viruses, pornography and other objectionable content. "Spam" filters, in particular, should be used to block email messages that are unsolicited or potentially dangerous.

Encryption: Encryption can be employed to protect any data that your organization considers sensitive. Encryption should be considered both for data being stored ("data at rest") as well as data being moved or sent somewhere ("data in motion"). Many security experts believe that data are most at risk when on the move. Whenever sensitive data are transmitted externally, consider using encryption. Additionally, if sensitive data are being transmitted internally over less secure networks, consider using encryption. For laptops and mobile devices, the use of whole-disk encryption can significantly reduce the risks associated with lost or stolen devices.

Multifactor (or Two-factor) authentication: An authentication factor is an independent category of credential used for identity verification. The three most common authentication factors are often described as something you know (e.g., a password), something you have (e.g., a smartphone or access card), and something you are (e.g., biometrics such as fingerprints). Some technologies are also using location (e.g., GPS coordinates) and time of day as additional authentication factors. Multifactor authentication is often used to secure control of sensitive data or to secure remote access to a network.

Virtual private network (VPN): A VPN is a secured network that is built on a larger, underlying network. In one common scenario, a company may provide remote access to the company's network through a VPN, allowing its employees to access the company's network securely over the public internet. A VPN can also be used to provide limited access to part of a network. For example, a company might use a VPN to permit third-party vendors to access certain systems or services on its network, without providing access to the entire network.

Network and application logging: Many systems, applications and network devices have a built-in capability to generate log files that reflect user access and activity. These log files can be very helpful in the event of a cybersecurity incident, particularly for systems and applications that store and manipulate sensitive information.

Intrusion detection system (IDS): An IDS can work together with firewalls to analyze network traffic and to block traffic that matches a known or suspected attack pattern.

After deciding which security controls to focus on and implement, an organization should document its reasons as part of an overall cybersecurity plan or strategy. An organization cannot be expected to implement every possible security control, but it should have a reasonable, documented plan in place for how it is protecting its data, systems and network.

AN ORGANIZATION RUNNING AN OBSOLETE VERSION OF AN OPERATING SYSTEM OR APPLICATION (I.E., A VERSION FOR WHICH PATCHES AND SECURITY UPDATES ARE NO LONGER BEING RELEASED), SHOULD TRANSITION TO A SUPPORTED VERSION. OTHERWISE, THE VULNERABLE SYSTEM OR APPLICATION SHOULD BE CAREFULLY PROTECTED AND/OR QUARANTINED.

Validate your backup strategy

One of the most important steps that an organization can take to protect against cyber risks is to maintain regular, systematic backup copies of important data. A well-designed backup strategy will protect against system and storage failure, as well as fire or flood. In addition, ransomware is on the rise – cybercriminals are using encryption to "lock" data found on compromised computers and demanding payment to decrypt the data. Maintaining good backups can protect you from falling victim to the latest ransomware.

In evaluating your backup strategy, you will want to consider what data need to be backed up, how frequently to perform backups and where the backups should be stored. For example, maintaining remote backups in "the cloud" may be simple and cost-effective, but the backup copies may not be immediately available to you if your internet connection is down. The cost of any particular backup strategy will have to be weighed against how quickly and reliably data must be recovered if damaged or destroyed.

It will often make sense to implement a "tiered" backup strategy in which data are backed up frequently to one location, and maybe less frequently to a second location. For example, a remote backup service could be used for nightly backups, with an additional backup copy made on a local storage device every week and stored in a separate, secure location. With the growth of ransomware, at least one backup copy should be stored offline or on a more tightly secured part of your network.

Backup copies of data should be encrypted if the original data warranted encryption. The backup copies should also be tested periodically to ensure that data can, in fact, be restored if the original data have been damaged or destroyed.

Plan for incident response

Every organization should plan for the unexpected – including a data breach or cyber incident. In fact, without an incident response plan, there is a greater likelihood of making mistakes in responding to the breach or incident – for example, by failing to comply with applicable laws and regulations. Such mistakes can cause damage to the business or organization that goes beyond the damage directly caused by the attack. A well-designed incident response plan will make it easier for your organization to launch a rapid and coordinated response.

IN MORE THAN **90%** OF BREACHES, THE COMPROMISE TAKES ONLY MINUTES OR LESS

AND **99.6%** OF THE TIME, DATA ARE EXFILTRATED WITHIN DAYS.[4]

IN GENERAL, AN INCIDENT RESPONSE PLAN SHOULD INCLUDE AT LEAST THE FOLLOWING COMPONENTS:

1. INFORMATION ABOUT THE PEOPLE INSIDE THE ORGANIZATION WHO WILL FORM THE INCIDENT RESPONSE TEAM;

2. GUIDELINES AND PROCEDURES TO ASSIST THE TEAM; AND

3. INFORMATION ABOUT EXTERNAL RESOURCES THAT ARE AVAILABLE TO SUPPORT THE TEAM.

The incident response team

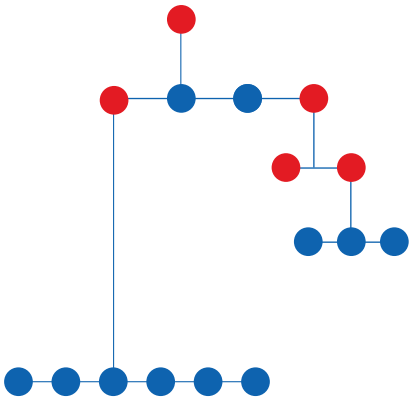
Identify team members by name and job title, together with a description of roles and responsibilities. An experienced manager, such as the Chief Information Security Officer, should serve as the team leader to help coordinate the overall response effort. Other members should include representatives from management, information technology, legal, compliance and public affairs/media relations.

Procedures and guidelines for incident response

An incident response plan should provide a framework for action so that important decisions have been considered ahead of time and are not made under pressure. In particular, it is important for the incident response plan to provide procedures and guidelines on difficult issues including identifying lines of authority and internal reporting obligations. The team should be focused on making the best possible decisions, not on figuring out how and by whom the decisions need to be made.

Clear procedures and guidelines on the following questions can greatly facilitate an incident response effort:

- Does the incident response plan even apply? Not every security incident will require invoking the plan.
- Is the business or organization insured for the incident? If so, when should the insurer be notified?
- Should the team bring in external resources? Should law enforcement authorities be notified? Who will have primary responsibility for coordinating with them?
- When should certain services or parts of the network be shut down or transitioned to backup systems, if available? There probably should be different criteria for shutting down an email server than a customer-facing website server, for example.
- What data, if lost or exposed, are subject to data breach notification laws? If notification is required, when and how should notification be made?
- What data, if lost or exposed, must be reported to government regulators? To business partners?
- Should information about the incident be communicated to employees of the organization? To the public?
- How should the team document the incident response effort, and how should it preserve records or evidence that it collects during the investigation?



It will not be possible, of course, for an incident response plan to provide detailed procedures and guidelines to cover every possible issue or scenario. The procedures and guidelines should be flexible enough to apply to a range of different cyber incidents, while providing more concrete guidance for those incidents that are considered the most likely to arise.

External resources

Depending on the nature and scope of the incident, it may be appropriate for the incident response team to seek assistance from external resources, such as a "breach coach," a computer and network forensics expert or a crisis management consultant. Most companies do not have employees with both the experience and time to handle an incident response effort.

In the course of developing an incident response plan, it is important to identify external resources and to establish relationships with them before an incident occurs, so that they will be ready to assist when needed. It will also be more cost-effective to negotiate for these services before an incident, rather than waiting until your organization is in dire need of them.

If your organization outsources any part of its IT function, the incident response plan should also provide contact information for your IT providers. It will often be necessary to work with your IT providers to investigate and secure evidence after a cybersecurity incident.

Once you have an incident response plan in place, it is important to test it regularly — annually, if possible.

Testing the incident response plan

These "tabletop" exercises should involve the full incident response team, and the results of the exercises should be made available to senior management. It is better to address issues that might be raised by senior management about the incident response plan in connection with a tabletop exercise — not in the midst of an actual incident response effort.

Helping prevent damaging cyber incidents.

PREVENT INCIDENTS:

- STRENGTHEN ACCESS CONTROLS
- PATCH KNOWN VULNERABILITIES
- EDUCATE YOUR EMPLOYEES
- ADOPT SECURITY-CONSCIOUS POLICIES AND PROCEDURES

PREPARE – **PREVENT** – MITIGATE – RESTORE

Security controls and incident response plans are necessary, but not necessarily sufficient, for good cybersecurity. Implementing the next four guidelines will go a long way toward helping your organization effectively prevent damaging cyber incidents:

1. Strengthen your access controls;
2. Promptly patch system and application vulnerabilities;
3. Educate your employees about cyber risks and security practices; and
4. Adopt policies and procedures that integrate good security practices into your business operations.

Strengthen access controls

We are all familiar with passwords, which are among the most fundamental types of access controls. More sophisticated access controls are becoming commonplace. For example, many banks and financial institutions have begun requiring two-factor authentication for online account access, and many smartphones and computers can be unlocked using biometric identifiers, such as fingerprints. Judiciously implementing stronger access controls, like limiting the number of employees with remote network access, can be a cost-effective way to improve the cybersecurity of your organization.

Even without adopting new access control technologies, businesses and organizations can benefit if they adhere to the principle of least privilege: that is, access to data, systems and the network should be permitted only to the extent necessary for the smooth and continued operation of the enterprise. Some information may be accessible to everyone; some information may be restricted to a specific department; and some information should be accessible only by a set of key personnel.

The principle of least privilege should be applied to all users, including system administrators and other members of an IT department. Inappropriate use of administrative privileges is often found to be a major contributing factor in data breaches and other cyber incidents.

In many growing organizations, system administrators assume numerous job functions and have access to multiple systems or applications. This can present a security risk if administrative privileges are not properly controlled, making it easier for an attacker to gain full control of a compromised system. To minimize this risk, the following controls should be considered:

- Users should not be allowed local administrative privileges, even on computers provided for their exclusive use.
- Members of the IT staff should have administrative privileges only for specific systems or applications, and only to the extent necessary for the performance of their duties.
- Members of the IT staff with administrative privileges should maintain separate accounts for daily use and for use as a system administrator. The administrator account should not be used for routine access to email or the internet. The password for the administrator account should not be shared, even with other members of the IT staff, and should be different from the password for the user account.
- When wider privileges must be granted to a user or system administrator to perform a specific task, grant the privileges only for a limited time.

Finally, it is important to include physical access controls for sensitive data and systems. Providing physical security to the building exterior can be a first step to protecting against unauthorized system and network access. Protect areas such as server rooms, computer rooms and telephone equipment rooms by appropriate security measures, such as locked doors and entry controls.

NEARLY 60 PERCENT OF CANADIAN ORGANIZATIONS REPORTED USING MULTIFACTOR AUTHENTICATION IN 2016 TO IMPROVE TRUST AMONG CUSTOMERS AND BUSINESS PARTNERS.[5]

Patch known vulnerabilities

This guideline is simple: patch your systems and software. An unpatched vulnerability is one of the easiest and most common methods of compromising a computer system or network.

Unfortunately, there can be significant obstacles to ensuring that all computer systems and software applications on a network are fully patched. First, on most corporate networks, there are a multitude of applications running on a variety of different systems. All of these applications and systems may require patches, provided by a host of third-party vendors. Second, it is a good practice to test patches before they are deployed, particularly for systems or software that are considered mission critical — introducing delay. Finally, patches are not always applied successfully, particularly to laptop computers and other mobile devices that are frequently disconnected from the network.

These difficulties can be addressed in part through the use of a patch management system. Whether using a commercial patch management system or tools that have been developed in-house, the system should:

- **Help track, obtain and validate available patches.**

  As different vendors release patches for their products, the system should identify which patches are needed in your particular environment and make them available to the IT staff for testing and evaluation.

- **Permit priority-based patching.**

  Routine patches can be applied on a predetermined schedule, but critical patches should be applied as soon as possible.

- **Perform reporting and auditing.**

  If the deployment of a patch fails anywhere on your network, information about the failure should be easily available to members of the IT staff.

PATCHES ARE NOT ALWAYS APPLIED SUCCESSFULLY, PARTICULARLY TO LAPTOP COMPUTERS AND OTHER MOBILE DEVICES THAT ARE FREQUENTLY DISCONNECTED FROM THE NETWORK.

It is also good practice for an organization to scan its systems and network regularly for vulnerabilities that may have been missed by the patch management system.

In some instances, it may be necessary to continue using a system or application with known vulnerabilities — for example, a legacy system with a vulnerability for which no patch is available. In that case, the vulnerable system should be carefully protected using other means, such as firewalls and strict access controls.

Educate your employees

Many cybersecurity incidents can be directly attributed to inadequate security awareness training. A training program designed to empower employees to recognize common cyber threats and to notify the IT staff is a cost-effective way to reduce these threats.

A comprehensive training program should:

- **Emphasize the importance of cybersecurity to the organization's success.** Employees should understand why data, systems and network security matter. A security breach can allow attackers to drain an organization's bank account; other financial and legal repercussions may follow, such as incident response costs, data breach notification expenses and loss of reputation and goodwill. If applicable, legal and regulatory requirements to protect certain kinds of data, such as personal health information (PHI), should be highlighted. The training should address each employee's responsibility to protect the organization's data, systems and network.
- **Train employees to avoid information security risks.** Risks can include phishing and other forms of social engineering, as well as improper password management, unsafe internet browsing and using unauthorized software.
- **Explain how to protect laptops, mobile devices and digital storage media.** Employees should be reminded to physically safeguard data and devices, as well as when and how to use encryption. Computers and other physical assets are lost more than 100 times more frequently than they are stolen.[6]
- **Encourage employees to report suspicious activity.** Employees should be aware of your incident response procedures and should know how to report suspicious activity, including questionable phone calls, to IT or security personnel.

Finally, employees should also receive training on policies and procedures that relate to cybersecurity. In many instances, explaining the rationale for restrictive "system use" policies will help to promote greater compliance.

The number of spear-phishing campaigns targeting employees increased by 55% in 2015.[7]

Adopt security-conscious policies and procedures

Good cybersecurity will be hard to achieve if a company's policies or procedures are haphazard — a skilled hacker can compromise an entire corporate network from a foothold obtained on one vulnerable computer.

There are several areas in particular where formal policies or procedures can substantially improve cybersecurity:

WHEN NEW DEVICES ARE ADDED TO A NETWORK, THERE SHOULD BE PROCEDURES TO ENSURE THAT DEFAULT PASSWORDS ARE CHANGED; PATCHES AND UPDATES ARE APPLIED; AND UNNECESSARY SERVICES, APPLICATIONS AND NETWORK PORTS ARE REMOVED OR DISABLED.

- A "system use" policy should be in place to govern the use of the business or organization's computers and network, including appropriate restrictions on the use of electronic mail, social media, the internet, external storage devices and unauthorized systems and software.
- There should also be procedures on disposal requirements for sensitive information and data, including computer systems and storage devices that store or process such data.
- Inadequate control of changes to network equipment and systems can be a common cause of systems and security failures. Lack of a written procedure creates the risk that changes could be made without proper preparation or testing. Establish written procedures that govern and coordinate all changes to existing configurations.
- There should be a process for promptly revoking system and network access when an employee leaves a company or organization, and for changing passwords and other controls to shared accounts, if any, that the employee may have known or accessed. It may also be advisable to have employees sign a confidentiality or non-disclosure agreement, as well as a representation upon leaving the business or organization that no sensitive, proprietary or other confidential data have been taken.

Vendor management

Businesses and organizations must pay special attention to policies and procedures relating to their vendors — IT or otherwise. The cybersecurity of an organization will be seriously jeopardized if a vendor with poor cybersecurity is given access to the organization's systems or network.

In accordance with the principle of least privilege, an organization should only give a vendor the level of systems or network access that is necessary for the performance of the vendor's responsibilities. Vendors should be subject to the same password requirements as other users (or system administrators, if appropriate), and should not use the same password across different client sites. Once the organization is no longer using the vendor, policies and procedures should be in place to ensure that access credentials and privileges are promptly revoked.

The policies and procedures of the organization should also ensure that the vendor has adopted sound cybersecurity practices, commensurate with the level of data, systems and network access given to the vendor. It may be appropriate, for example, to include contract provisions that set forth cybersecurity requirements, agreements to assist with investigations, insurance obligations, indemnification provisions, etc. If the vendor is given access to sensitive data, such as personally identifiable information, additional controls may be appropriate, such as requiring third-party assessments of the vendor's cybersecurity practices.

Attackers are increasingly taking advantage of outsourcing relationships to gain access to sensitive information.[8]

Cyber incidents need not be catastrophic if properly managed.

MITIGATE DAMAGE:

- DETECT INCIDENTS EARLY
- EXECUTE YOUR RESPONSE PLAN
- GET HELP WHEN NEEDED
- DOCUMENT YOUR RESPONSE EFFORT

PREPARE – PREVENT – **MITIGATE** – RESTORE

Cyber incidents may be inevitable but need not be catastrophic if properly managed. Early detection is crucial, so organizations should review network and security logs as frequently as possible — indeed, continuous monitoring is a worthy goal.

When an incident does occur, a well-designed incident response plan will be invaluable in guiding the company or organization from the initial stages of incident response — investigate, assess and mediate — through to the eventual restoration of normal operations. It will often make sense for an organization to seek outside expertise, to contain the damage from an incident; it will always make sense to document the actions taken during the entire incident response process (as well as the reasons for doing so).

Detect incidents early

Even an organization with strong cybersecurity cannot assume that its network is impenetrable. Therefore, it is critically important to detect incidents early to minimize the damage in the event of a compromise.

Fortunately, most systems (and many applications) include some logging or monitoring capability. Network firewalls can be configured to log suspicious traffic and to issue alerts under specified conditions. Almost all computers can be configured to track unsuccessful login attempts, which are an early indicator of a potential attack. Businesses and organizations should be aware of the logging and monitoring capabilities that are already available to them; in addition, there are special-purpose network monitoring systems that can be implemented to allow for closer monitoring of network traffic.

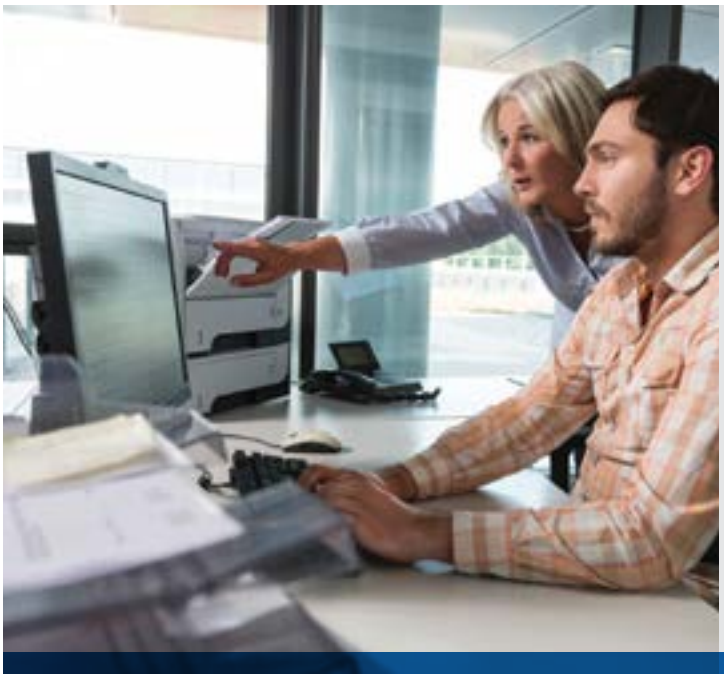
It is usually not practical, however, to have all systems and applications configured to log as much data as possible. Instead, organizations should focus their logging and monitoring capabilities on protecting their most valuable assets. For example, unsuccessful login attempts to a central database server should likely be investigated more promptly and thoroughly than unsuccessful login attempts to an average employee's laptop.

For many organizations, it will make sense to use a security incident event management system (SIEM), whether implemented in-house or provided by a vendor. Such a system operates as a centralized resource for collecting, monitoring and analyzing network logs and other security-related information. By using a SIEM, organizations can greatly reduce the risk that early indicators of a compromise will be missed.

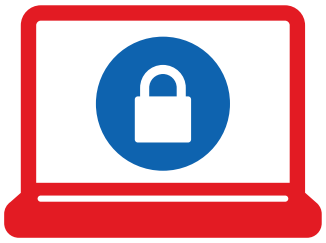
Execute your response plan

When an organization is impacted by a cyber incident, there are often a multitude of unanswered questions about what happened, what the impact will be and what to do next.

In order to answer those questions, your incident response team should initially focus on the following: investigating the incident, assessing its impact and mitigating any damage. These tasks must often be undertaken concurrently, in the middle of a situation that is rapidly changing, with information that is incomplete and sometimes inaccurate. In such trying circumstances, a well-designed incident response plan will help the team succeed by delineating areas of responsibility, facilitating information sharing and identifying pertinent guidelines or procedures — for example, when deciding whether to use a computer and network forensics consultant during the investigation.



NOTIFY YOUR INSURANCE CARRIER PROMPTLY AFTER AN INCIDENT IS DISCOVERED. CYBER INSURANCE CAN HELP COMPANIES BY PROVIDING ACCESS TO A BREACH COACH, FORENSICS CONSULTANTS AND OTHER PROFESSIONALS IN THE DATA SECURITY COMMUNITY.



Investigate the incident

The investigation of a substantial cyber incident — at a minimum, determining how the attack was conducted, which systems were compromised and what data have been lost or exposed — is likely to require substantial time and expertise. Such investigations typically involve:

- Preserving, collecting and analyzing application, system and network logs that may have evidence relating to the attack.
- Identifying any software or hardware vulnerabilities that were used to facilitate the attack.
- Identifying unauthorized changes to systems on the network, including the installation of malicious software ("malware") such as keyloggers or remote-access Trojans.
- Determining what data, if any, were stolen or exposed, including any passwords or other security controls that may have been compromised.

The investigation may have to include network devices such as firewalls and routers, not just the computers and servers that are on the network. Any significant evidence obtained during the investigation should be properly preserved, preferably in consultation with legal counsel.

The investigation may also involve interviews of employees, contractors or other third parties who may have been impacted by, or otherwise involved in, the incident. Information obtained through such interviews should be memorialized in writing, and interviews of third parties should preferably be conducted only in consultation with legal counsel.

Assess the impact

The impact of a cyber incident will typically be assessed in many dimensions: the number of impacted systems; the amount of data lost (whether measured by the volume of the data or the number of victims whose data were stolen); the magnitude of financial loss; the effect on a business or organization's operations; and the anticipated difficulty in recovering from the incident, to mention a few.

These assessments will be needed by senior management and will also be needed by the incident response team in order to make sound decisions at critical junctures. For example, the incident response plan may specify that a computer and network forensics consultant should be retained if the number of impacted systems exceeds a certain threshold, or if certain kinds of data (such as payment card information) have been stolen or exposed.

In particular, the impact of a cyber incident that involves the loss of data will be greatly affected by the kind of data involved. The loss of customer account data, for example, will likely result in a different response effort than the loss of the company or organization's own data. Whenever a cyber incident involves the loss or even potential loss of data, legal counsel should be closely involved in the incident response effort.

Mitigate any damage

Once the nature and the scope of the attack are understood, the incident response team can move toward the recovery and restoration of lost or damaged data and systems. However, if the attack is causing ongoing damage to the organization, it may be necessary to take steps to mitigate that damage even before the incident investigation and the impact assessment are complete.

The immediate impulse may be to "pull the plug" — that is, to do everything possible to disrupt the attack, such as disconnecting all systems known to have been compromised. In some cases, this can be an appropriate response.

However, other factors should be considered before deciding to "pull the plug."

First, the tactic may be ineffective. It is well known that attackers will seek to embed themselves into a compromised network, so that disabling one, or a few, compromised computers will simply cause the attackers to move elsewhere on the network. Pursuing a "whack-a-mole" mitigation effort can distract the incident response team from executing a more comprehensive recovery and restoration plan.

Second, pulling the plug may impede the investigation. If the attackers have compromised a system where encrypted data are stored, it may be more important to monitor their activities to learn if the attackers have been able to decrypt the data than to shut down the system immediately.

Finally, a mitigation effort undertaken in haste, without sufficient planning and consideration, might itself cause damage to a business or organization. It may not make sense, for example, to shut down a company's email server, if a hacker has only obtained limited access to the server without yet obtaining access to the emails.

Instead of pulling the plug, it may be preferable to mitigate damage by pursuing a strategy of containment — locking down portions of the network that the attackers have not yet compromised, or blocking egress points by re-configuring firewalls to strictly limit outbound traffic.

It can be challenging for an incident response team to investigate, assess and mitigate the damage from a significant cyber incident. Therefore, it is often appropriate for the organization to support the team with external resources.

Get help when needed

There are many outside experts and consultants who can help a business or organization respond effectively to a cyber incident. A list of these external resources should be included in the incident response plan, together with guidelines and policies that will assist the incident response team in determining when outside resources should be brought to bear.

These resources include:

A "breach coach" or other outside legal counsel. An experienced breach coach can provide guidance throughout the incident response effort, particularly on issues relating to privacy, notification requirements and regulatory compliance. In addition, aspects of the incident response effort conducted under the direction of a breach coach may be protected by privilege in the event of future litigation.

A computer and network forensics expert. Use of an outside forensics expert is necessary if internal IT personnel do not have the capacity or expertise to investigate the incident, which may require analyzing malware or examining detailed logs of network traffic. It may also be advisable to use an outside forensics expert if the incident might give rise to litigation.

A crisis management consultant. An experienced crisis management consultant can help the organization minimize any reputational injury that could result from the incident.

Law enforcement. If there is reason to believe that a crime has been committed, it may be appropriate to refer the matter to law enforcement authorities. Few cyber attacks occur in isolation; from investigating similar or related incidents, law enforcement authorities may be able to provide information about the tools and techniques that were used to conduct the attack. If the attack was financially motivated, law enforcement may be better positioned to trace the money that was stolen, if any.

Document your response effort

Throughout the incident response effort, it is important to document the steps taken by the incident response team. This will help ensure that your organization is better able to identify lessons learned, to respond to any future legal or regulatory inquiries, and to reconcile any changes made to your systems or networks after the urgency of the incident response effort has passed. The incident response plan should include forms or other guidance that will help to ensure adequate recordkeeping.

Sometimes, it may be appropriate for an attorney to be involved in documenting the incident response effort, as this may allow the organization to assert a claim of privilege over the materials in the event of future litigation.

Complete the road to recovery.

RESTORE NORMAL OPERATIONS:

- REMEDIATE, RESTORE AND REPLACE
- CONTINUE MONITORING
- COMMUNICATE EFFECTIVELY
- IMPLEMENT LESSONS LEARNED

PREPARE – PREVENT – MITIGATE – **RESTORE**

After assessing the situation, your organization will be ready to complete the road to recovery: remediating vulnerabilities; restoring lost or damaged systems and data; and replacing passwords, encryption keys and other compromised controls.

Along the way, it will be important to continue monitoring your systems and networks for signs that the attackers may have evaded your efforts to eliminate them. It will also be important to provide accurate information about the incident, if and when appropriate, to interested stakeholders, whether employees, business partners, regulators or others.

Finally, your organization can benefit from the incident by identifying and applying lessons learned from a careful examination of the incident and the incident response effort.

Remediate, restore and replace

Ultimately, the goal of your incident response effort is to remove the attackers from your network and to return to normal operations. To do so, you must:

- **Remediate vulnerabilities.** In most cases, the incident response team will have been attempting to eliminate vulnerabilities as they have been discovered over the course of the investigation. Any remaining vulnerabilities that compromise the security of the network should be addressed at this stage, whether through patching or other methods. If it has not been possible to identify the vulnerabilities used by the attackers and to remediate them, the recovery effort may well prove futile.

- **Restore lost or damaged systems and data.** It will be much easier to restore data from a backup copy than to re-create lost or damaged data. When restoring a compromised system, the preferred method is to re-image the operating system and applications from a clean image. If this is not possible, care must be taken to ensure that all unwanted changes to the system have been identified and repaired. Otherwise, a “back door” installed by the attackers could be used to reinfect the system and the network.

- **Replace compromised controls.** This final step is crucial, but often overlooked. When attackers have compromised a system or network, they are often able to obtain information about security controls, such as passwords and encryption keys, which can be used in later attacks. The incident response team should give thought to security controls that may have been compromised, not only security controls that have been compromised.

Continue monitoring

It is important to monitor the network closely throughout the entire incident response effort. It is equally important that monitoring continue for a time even after the recovery effort is thought to be complete. Attackers will often react to steps taken by the incident response team, and close monitoring of the network can provide insight into the attackers' goals and how they operate.

More importantly, continued monitoring of the network will help to ensure that the recovery effort was successful. It should be assumed that attackers, having once gained a foothold on a network, will have taken steps to embed themselves further in order to ensure access to the network even after the initial point of compromise has been denied to them.

Depending on the scope and duration of the incident, it may be advisable to conduct a vulnerability scan of the business or organization's systems and network. This can serve to ensure that any changes made during the incident response effort did not introduce new vulnerabilities, and can also provide added reassurance that the response effort was, in fact, successful.

Communicate effectively

When responding to a cyber incident, it can be very difficult to determine what information should be communicated both internally and externally, because the information available about the incident may be incomplete and unreliable. Providing information that later turns out to be inaccurate can significantly impair the organization's reputation in the eyes of its customers and shareholders, and can also invite the scrutiny of government regulators. Therefore, it is critical for the organization to have formulated an effective communications strategy before a cyber incident occurs.

When communicating with senior management, it is important for the incident response team to provide as much reliable information as possible about the scope of the incident, its potential impact on the organization and the anticipated duration of the response effort. It is preferable for that information to be conveyed through one or more designated points of contact, hopefully identified in the incident response plan, and not through ad hoc, informal communications with different members of the response team.

When deciding whether, when and what information should be communicated to third parties, including the public, consider the following:

Factors to consider:

Has information about the incident already been made public or is it about to be?
If so, it is probably in the best interests of the organization to make a public statement in order to maintain the trust of its customers and business partners, and to position itself as the authoritative source of information. If information about the incident is likely to become public — for example, if the incident involved the loss of data that must be reported under a data breach notification law — it is important to make a public statement.

What reliable information, if any, is available?
During the early stages of an incident response effort, there may not be much reliable information at all. In that case, if a public statement must be made, hopefully the organization can disclose when the incident was first discovered, demonstrate that it has promptly begun to investigate — including cooperating with law enforcement agencies or involving outside investigators — and describe remedial measures for affected third parties, such as credit monitoring services.

Data breach reporting, notification and recordkeeping obligations

Whenever data have been lost as a result of the incident, it will be necessary to determine whether notification to affected individuals or reporting to responsible authorities is required by law. This may be a challenging task, because it can be difficult to determine what data have been compromised and what laws apply. Moreover, data breach laws continue to evolve. For instance, Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) mandates data breach notification to the Office of the Privacy Commissioner, affected individuals and, in some cases, other third parties, but these provisions will be brought into force only after more specific regulations are developed and in place, later in 2017. Both reporting and notification obligations will be triggered where there is a "real risk of significant harm," which may include bodily harm, damage to reputation or relationships, identify theft, financial loss, or loss of employment, business or professional opportunities. Assessing whether a real risk of significant harm exists will involve weighing the sensitivity of the information involved and the probability that the information was or will be misused. Organizations will also be required to keep a record of every breach of safeguards involving personal information, whether or not reporting or notification requirements are engaged. The new obligations under PIPEDA are similar to those already in place in Alberta, but will apply to a wider range of organizations across the country. Provincial health privacy laws in Ontario, New Brunswick and Newfoundland and Labrador also contain reporting requirements for the healthcare sector.

In the United States, 48 out of 50 states have data breach notification statutes, and there are other federal laws and regulations which can mandate notifications to affected individuals. In addition, you will be required to report breaches in certain sectors, such as healthcare and defense, to various state and federal authorities.

Consult with legal counsel, even if the investigation of the incident is still incomplete, to evaluate your reporting obligations and notification strategy. Any notification required by law should be timely and comprehensive. Keep copies of all notifications that are sent out, as well as any responses that are received. It is equally important to demonstrate that you understand your reporting obligations and are taking prompt and appropriate measures to respond to the incident.

Implement lessons learned

After recovering from a cyber incident, it is important to identify and apply any lessons that can be learned. By examining both the incident and the incident response effort, an organization has an invaluable opportunity to improve its ability to protect against and respond to future cyber incidents.

The review process should include members of the incident response team as well as personnel – employees or outside consultants – who were not involved in the incident response effort. It can be very helpful for the review process to be facilitated by an experienced manager who was not directly involved in the response effort.

REVIEW THE FOLLOWING QUESTIONS AFTER A CYBER INCIDENT:

- Are any additional changes needed to the organization's security controls, beyond those already made by the incident response team? Do remedial measures that were implemented under time pressure need to be changed or modified in the future?
- Would any changes to the organization's cybersecurity policies reduce the likelihood or severity of future cyber incidents? Would any changes to the organization's business practices as a whole (e.g., concerning what information is collected or stored) reduce the likelihood or severity of future cyber incidents?
- Would any changes to the organization's incident response plan enable the incident response team to respond more quickly and effectively in the future?
- Were outside resources used and managed well?
- Was appropriate information communicated in a timely fashion to senior management?

LEARN MORE

There is always room for a business or organization to improve its cybersecurity. Indeed, as the threat landscape evolves, organizations must pursue continuous improvement, or else risk becoming the next victim of cybercrime.

The Travelers Institute looks forward to working with businesses and organizations to help make our digital world a source of great opportunity, not unmanageable risks.

For more information about the ***Cyber: Prepare, Prevent, Mitigate, Restore*** initiative, visit travelersinstitute.org/cyber or contact institute@travelers.com. Additional cyber resources can be found at travelers.com/cyber.

ABOUT THE TRAVELERS INSTITUTE

Travelers established the Travelers Institute as a means of participating in the public policy dialogue on matters of interest to the property casualty insurance sector, as well as the financial services industry more broadly. The Travelers Institute draws upon the industry expertise of Travelers' senior management and the technical expertise of its risk professionals, and other experts to provide information, analysis and recommendations to public policymakers and regulators.

NOTES

[1] Symantec Corp., 2016 Internet Security Threat Report, April 2016, Volume 21. https://resource.elq.symantec.com/LP=2899

[2] Ponemon Institute, 2016 Cost of Data Breach Study: Global Analysis. Research sponsored by IBM. https://securityintelligence.com/cost-of-a-data-breach-2016/

[3] National Institute of Standards and Technology, Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53 Rev. 4 (April 2013). http://www.nist.gov/manuscript-publication-search.cfm?pub_id=917904

[4] Verizon, 2016 Data Breach Investigations Report. http://news.verizonenterprise.com/2016/04/2016-data-breach-report-info/

[5] PWC, Turnaround and transformation in cybersecurity: How Canadian businesses are responding to rising cyber-risks. Key Findings from The Global State of Information Security Survey 2016 (Canadian Insights). https://www.pwc.com/ca/en/technology-consulting/publications/pwc-gsiss-2016-canadian-insights-2015-11-en.pdf

[6] Verizon, 2016 Data Breach Investigations Report. http://news.verizonenterprise.com/2016/04/2016-data-breach-report-info/

[7] Symantec Corp., 2016 Internet Security Threat Report, April 2016, Volume 21. https://resource.elq.symantec.com/LP=2899

[8] M-Trends 2016, Mandiant, a FireEye Company, February 2016. https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html

TRAVELERS INSTITUTE® | TRAVELERS

travelersinstitute.org

The Travelers Institute, 700 13th Street NW, Suite 1180, Washington, DC 20005

Cyber™

PRÉPARER | PRÉVENIR | ATTÉNUER | RESTAURER

TRAVELERS INSTITUTE®

TRAVELERS

Habiliter les organisations canadiennes à réagir aux cybermenaces en constante évolution

UN GUIDE EN CYBERSÉCURITÉ

POUR LES PETITES ET MOYENNES ENTREPRISES

TABLE DES MATIÈRES

LES CYBERMENACES EN CONSTANTE ÉVOLUTION AFFECTENT LES ENTREPRISES ET LES ORGANISATIONS DE TOUTES TAILLES, DE TOUS SECTEURS ET DE TOUTES INDUSTRIES.

INTRODUCTION

Les atteintes à la protection des données et les intrusions informatiques font souvent la une de l'actualité et les grandes entreprises travaillent sans relâche afin de limiter les dommages occasionnés à leurs activités, leurs clients et leur réputation. Les recherches démontrent que les cybercriminels attaquent également les petites entreprises et organisations générales ('Main Street') qui sont souvent moins bien préparées pour prévenir une attaque et y répondre. En fait, les cybermenaces en constante évolution affectent les entreprises et les organisations de toutes tailles, de tous secteurs et de toutes industries. Au cours des cinq dernières années, il y eu une augmentation régulière des attaques ciblant les entreprises de moins de 250 employés; aujourd'hui, plus de 60 % de l'ensemble des attaques ciblées frappent les petites à moyennes entités.[1]

Les experts estiment qu'il ne s'agit pas de « si » votre organisation se fera attaquer, mais plutôt de « quand ». Un pirate débrouillard, un employé mécontent ou même des dossiers physiquement perdus renfermant des données sur les clients ou des renseignements exclusifs sur votre propre entreprise peut occasionner d'énormes pertes financières et une atteinte à la réputation. Les coûts liés à une atteinte à la protection des données peuvent être gigantesques, avec une moyenne de 211 $ par dossier compromis et de 4 980 000 $ par atteinte à la protection des données au Canada, en 2015 et 2016.[2] Conjuguées à une réputation endommagée, ces pertes peuvent ravager une organisation non préparée.

En ayant ceci à l'esprit, la Travelers Institute, le service des politiques publiques de The Travelers Companies, Inc., a lancé son initiative éducative *Cyber : Préparer, Prévenir, Atténuer, Restaurer* (Cyber : Prepare, Prevent, Mitigate, Restore) qui réunit les entreprises et des leaders en matière de cyberrisques des secteurs privés et publics. En travaillant avec des experts en cybersécurité, des agences gouvernementales et des professionnels en assurance, la série *Cyber : Préparer, Prévenir, Atténuer, Restaurer* offre aux propriétaires d'entreprises les renseignements et ressources nécessaires pour répondre au défi que présente la cybersécurité.

Dans le présent guide, nous offrons des mécanismes de protection fondamentaux qui peuvent être utilisés par des petites et moyennes organisations afin d'améliorer leur cybersécurité. Ces mécanismes de protection, identifiés par les professionnels en cyberrisques de Travelers Canada afin d'aider les titulaires de polices à gérer leurs cyberrisques, peuvent aider toute organisation à être mieux préparée, à mieux prévenir des intrusions, à atténuer des dommages et à restaurer les activités habituelles lorsque les pirates débarquent.

DANS LE PRÉSENT GUIDE, NOUS OFFRONS DES MÉCANISMES DE PROTECTION FONDAMENTAUX QUI PEUVENT ÊTRE UTILISÉS PAR DES PETITES ET MOYENNES ORGANISATIONS AFIN D'AMÉLIORER LEUR CYBERSÉCURITÉ.

La préparation est essentielle.

SOYEZ PRÊTS À :

- **CONNAÎTRE VOS DONNÉES, SYSTÈMES ET RÉSEAUX**
- **CONCENTRER VOS EFFORTS EN CYBERSÉCURITÉ**
- **VALIDER VOTRE STRATÉGIE DE SAUVEGARDE**
- **PLANIFIER UNE INTERVENTION EN CAS D'INCIDENT**

PRÉPARER – PRÉVENIR – ATTÉNUER – RESTAURER

Une des pierres angulaires de la cybersécurité est la préparation. Dans un monde où les ressources sont limitées, vous devez savoir quels systèmes vous exploitez, quelles données vous stockez et comment votre réseau est structuré afin de répartir efficacement vos ressources en cybersécurité.

La mise en place de mécanismes de contrôle de la sécurité puissants n'est pas suffisante, toutefois, puisque nous savons que les organisations avec une sécurité élevée peuvent être compromises. Par conséquent, il est important de sauvegarder régulièrement les données importantes et d'avoir un plan d'intervention en cas d'incident sur lequel se fier lorsque survient un incident.

Connaître vos données, systèmes et réseaux

Les entreprises et organisations stockent habituellement plusieurs types de données, en utilisant divers systèmes informatiques sur des réseaux locaux, internationaux ou quelque part entre les deux. Le premier principe en matière de cybersécurité est « Connais-toi toi-même ». Sachez quelles données sont créées, recueillies et stockées (et où elles le sont); maintenez un inventaire exact des systèmes et logiciels informatiques; et comprenez votre infrastructure de réseaux.

Ceci vous permet de mieux:

- Identifier et prioriser les mécanismes de contrôle de la sécurité appropriés.
- Retirer des systèmes et logiciels non autorisés de votre réseau.
- Corriger et maintenir des systèmes et logiciels existants.
- Reconnaître des nouvelles vulnérabilités dans les systèmes et logiciels existants.
- Intervenir plus efficacement lorsque survient un incident.

Plusieurs types de données peuvent se trouver sur un système ou réseau, y compris les données suivantes:

Renseignements personnels sur la santé

RPS (*PHI*)

comme les dossiers de santé ou médicaux des patients ou des employés.

Renseignements relatifs aux cartes de paiement

RCP (*PCI*)

comme les numéros de comptes de cartes de crédit ou de débit.

Renseignements personnels permettant de vous identifier

RPI (*PII*)

comme les noms, adresses, numéros de téléphone, numéros d'assurance sociale ou autres renseignements permettant l'identification.

Propriété intellectuelle

comme les procédés de fabrication, les stratégies de marketing et les secrets commerciaux.

Autres renseignements exclusifs

y compris les renseignements confidentiels partagés par un partenaire d'affaires.

Dans de nombreux cas, il peut être approprié pour votre organisation d'adopter un plan de classification des données. Certains types de données peuvent justifier que des mécanismes de contrôle de la sécurité plus puissants soient imposés, notamment si les données sont précieuses pour l'organisation, si leur perte peut occasionner des dommages importants ou si elles méritent un traitement spécial en raison d'obligations juridiques ou contractuelles.

Aussi, un inventaire des systèmes et des logiciels devrait être maintenu pour identifier chaque appareil qui a un accès au réseau, y compris les ordinateurs de bureau, les ordinateurs portables, les appareils sans fil, les serveurs, le matériel de réseau et les imprimantes. L'inventaire devrait identifier une personne spécifique comme étant responsable de chaque appareil (avec son nom et son titre), ainsi que l'adresse du réseau de l'appareil et son emplacement physique. Les organisations devraient également maintenir un inventaire des applications logicielles, qui identifie les systèmes (y compris les serveurs, les postes de travail et les ordinateurs portables) sur lesquels elles se trouvent.

Tout système ou toute application non autorisée devrait faire l'objet d'une enquête et être retirée.

Finalement, il est important de maintenir des renseignements exacts concernant la structure et la topologie du réseau d'une organisation. Ces renseignements peuvent être utilisés dans le cours normal des affaires pour assurer que les changements au réseau soient conformes aux mécanismes de contrôle de la sécurité du réseau existants. Ces renseignements seront également précieux en cas d'intervention à la suite d'un cyberincident.

Concentrer vos efforts en cybersécurité

Une fois que vous comprenez les données, systèmes et réseaux que vous cherchez à protéger, vous pouvez vous concentrer sur la mise en place (ou l'amélioration) des mécanismes de contrôle de la sécurité qui seraient les plus efficaces en regard de vos besoins et ressources spécifiques. (Vous serez également mieux préparés pour travailler avec un consultant en cybersécurité, si vous choisissez cette option.)

Considérez ce qui suit:

Quelles sont vos données les plus importantes (crown jewels)?

Si vous avez adopté un plan de classification des données, vous voudrez mettre en place des mécanismes de contrôle de la sécurité plus puissants en ce qui concerne le stockage et la transmission des données considérées plus sensibles.

Quelles sont vos vulnérabilités?

Une évaluation de la vulnérabilité peut aider à identifier les points faibles au niveau de vos mesures de cybersécurité qui nécessitent plus d'attention. Si votre organisation permet à des tiers, notamment les entrepreneurs ou fournisseurs, d'accéder aux systèmes ou aux réseaux, il faut comprendre que leurs vulnérabilités deviennent également les vôtres.

Quels sont les scénarios de menaces les plus probables?

Si vous comprenez les menaces les plus probables pouvant affecter votre entreprise ou votre organisation, vous pouvez concentrer vos efforts afin de réduire ces menaces.

LA CONFORMITÉ À UNE NORME PARTICULIÈRE EN MATIÈRE DE CYBERSÉCURITÉ N'EST PAS UN PRÉREQUIS POUR ASSURER UNE BONNE CYBERSÉCURITÉ, MAIS ELLE PEUT ÊTRE IMPORTANTE AFIN DE DÉTERMINER QUELS MÉCANISMES DE CONTRÔLE DE LA SÉCURITÉ DOIVENT ÊTRE MIS EN PLACE. LES ENTREPRISES QUI TRAITENT LES RENSEIGNEMENTS CONCERNANT LES CARTES DE PAIEMENT, PAR EXEMPLE, DOIVENT SE CONFORMER À LA NORME DE SÉCURITÉ DES DONNÉES DES RCP.

De nombreux renseignements sur les mécanismes de contrôle de la sécurité informatique et des réseaux sont disponibles en ligne, y compris des taxonomies globales sur les mécanismes de contrôle de la sécurité pouvant aider à vous assurer que vous n'oubliez aucun mécanisme qui pourrait être précieux pour votre organisation.[3]

Ici, nous soulignons certains mécanismes de contrôle de la sécurité fondamentaux :

Mots de passe robustes : Presque tous les systèmes peuvent être configurés afin d'exiger des utilisateurs qu'ils choisissent des mots de passe qu'un intrus aurait de la misère à compromettre. On devrait dire aux utilisateurs de ne pas utiliser des mots de passe (ou des variations de mots de passe) qu'ils utilisent ailleurs (p. ex., pour contrôler l'accès à leurs comptes de courriel personnel ou autres comptes en ligne).

Pare-feu : Les protections pare-feu sont utilisées afin de permettre uniquement l'entrée et la sortie d'un trafic approprié dans un système ou un réseau. Comme tout autre mécanisme de contrôle de la sécurité, un pare-feu doit être configuré adéquatement et maintenu afin d'être efficace. Les protections pare-feu devraient uniquement permettre un trafic dans le réseau qui est approprié en regard des besoins de l'entreprise ou de l'organisation. Par exemple, les demandes de transfert de dossiers sur le serveur de messagerie d'une entreprise devraient probablement être refusées.

Anti-virus : Les logiciels antivirus sont conçus pour défendre votre réseau à l'encontre des logiciels malveillants (« maliciels »). Afin de maintenir une défense efficace, votre logiciel antivirus devrait fonctionner en arrière-plan en tout temps et être continuellement mis à jour. La capacité d'installer rapidement des mises à jour antivirus sur tous les systèmes est cruciale.

Filtrage du contenu : Les mécanismes de contrôle qui filtrent le contenu restreignent le matériel qui est diffusé sur Internet, par courriel ou par d'autres moyens. Ils permettent à une entreprise ou une organisation de bloquer les pièces jointes dans des courriels ou du matériel provenant de sites Web qui pourraient probablement contenir des logiciels espions, des virus, de la pornographie et d'autres contenus discutables. Les filtres de pourriels, notamment, devraient être utilisés afin de bloquer les courriels non sollicités ou potentiellement dangereux.

Cryptage : Les mécanismes de contrôle qui filtrent le contenu restreignent le matériel qui est diffusé sur Internet, par courriel ou par d'autres moyens. Ils permettent à une entreprise ou une organisation de bloquer les pièces jointes dans des courriels ou du matériel provenant de sites Web qui pourraient probablement contenir des logiciels espions, des virus, de la pornographie et d'autres contenus discutables. Les filtres de pourriels, notamment, devraient être utilisés afin de bloquer les courriels non sollicités ou potentiellement dangereux.

Authentification multifactorielle (ou à deux facteurs) : Un facteur d'authentification est un identifiant indépendant utilisé à des fins de vérification de l'identité. Les trois facteurs d'authentification les plus souvent utilisés sont ceux qui sont souvent décrits comme quelque chose que vous connaissez (p. ex., un mot de passe), quelque chose que vous avez (p. ex., un téléphone intelligent ou une carte d'accès) et quelque chose que vous êtes (p. ex., des biométriques comme les empreintes digitales). Certaines technologies utilisent aussi l'emplacement (p. ex., les coordonnés par GPS) et le moment de la journée à titre de facteurs d'authentification supplémentaires. L'authentification multifactorielle est souvent utilisée pour sécuriser le contrôle des données sensibles ou l'accès à distance à un réseau.

Réseau privé virtuel (RPV) : Un RPV est un réseau sécurisé bâti sur un réseau sous-jacent plus large. Un scénario courant serait celui où une entreprise fournit un accès à distance à son réseau au moyen d'un RPV, permettant ainsi à ses employés d'accéder au réseau de l'entreprise en toute sécurité par Internet. Un RPV peut également être utilisé pour fournir un accès limité à une partie d'un réseau. Par exemple, une entreprise peut utiliser un RPV pour permettre à des tiers fournisseurs d'accéder à certains systèmes ou services sur son réseau, sans donner accès à tout le réseau.

Connexion aux réseaux et aux applications : Plusieurs systèmes, applications et réseaux ont la capacité intégrée de générer des registres qui font état de l'accès et des activités des utilisateurs. Ces registres peuvent être très utiles en cas d'incident en cybersécurité, notamment pour les systèmes et applications qui stockent et manipulent des renseignements sensibles.

Système de détection d'intrusion (SDI) : Un SDI peut travailler avec les protections pare-feu afin d'analyser le trafic sur le réseau et de bloquer celui-ci lorsqu'il ressemble à un modèle d'attaque connue ou soupçonnée.

Après avoir décidé sur quels mécanismes de contrôle de la sécurité se concentrer et mettre en place, une organisation devrait documenter ses raisons dans le cadre d'un plan ou d'une stratégie globale de cybersécurité. On ne peut s'attendre à ce qu'une organisation mette en place tous les mécanismes de contrôle de la sécurité possibles, mais elle devrait avoir en place un plan raisonnable et documenté afin de protéger ses données, systèmes et réseaux.

UNE ORGANISATION QUI UTILISE UNE VERSION DÉSUÈTE D'UN SYSTÈME D'EXPLOITATION OU D'UNE APPLICATION (C.-À.D. UNE VERSION QUI NE GÉNÈRE PLUS DE CORRECTIFS ET NE MET PLUS À JOUR DES RUSTINES DE SÉCURITÉ) DEVRAIT FAIRE LA TRANSITION VERS UNE VERSION PRISE EN CHARGE. AUTREMENT, LE SYSTÈME OU L'APPLICATION VULNÉRABLE DEVRAIT ÊTRE ATTENTIVEMENT PROTÉGÉ ET/OU MIS EN QUARANTAINE.

Valider votre stratégie de sauvegarde

Une des mesures les plus importantes qu'une organisation peut prendre afin de se protéger contre les cyberrisques est de maintenir des copies régulières et systématiques de sauvegardes de données importantes. Une stratégie de sauvegarde bien conçue assurera une protection à l'encontre des défaillances de systèmes et de stockage, ainsi que des incendies ou inondations. En outre, les rançongiciels (*ransomware*) sont de plus en plus courants et les cybercriminels utilisent le cryptage pour « bloquer » des données trouvées sur des ordinateurs compromis et demander le paiement de rançons pour déchiffrer les données. Le maintien de bonnes sauvegardes peut vous protéger afin d'éviter d'être la victime des derniers rançongiciels.

Dans le cadre de l'évaluation de votre stratégie de sauvegarde, vous devriez considérer quelles données doivent être sauvegardées, à quelle fréquence les sauvegarder et où les stocker. Par exemple, maintenir des sauvegardes à distance dans « les nuages » peut être simple et rentable, mais les copies de sauvegarde pourraient ne pas être disponibles immédiatement si votre connexion Internet ne fonctionne pas. Il faudra tenir compte du coût associé à toute stratégie de sauvegarde particulière en regard de la rapidité et de la fiabilité du recouvrement des données si elles sont endommagées ou détruites.

Il sera souvent judicieux de mettre en place une stratégie de sauvegarde « graduelle » en vertu de laquelle les données sont sauvegardées fréquemment à un même emplacement, et moins fréquemment à un second emplacement. Par exemple, un service de sauvegarde à distance pourrait être utilisé pour les sauvegardes de nuit, avec une copie additionnelle de sauvegarde faite sur un appareil de stockage local à chaque semaine et stocké dans un emplacement distinct et sécurisé. Avec la croissance des rançongiciels, au moins une copie de sauvegarde devrait être conservée hors ligne ou sur une partie plus sécurisée de votre réseau.

Les copies de sauvegarde de données devraient être cryptées si les données originales nécessitaient un cryptage. Les copies de sauvegarde devraient aussi faire l'objet d'examens périodiques pour assurer que les données peuvent, dans les faits, être restaurées si les données originales sont endommagées ou détruites.

Planifier une intervention en cas d'incident

Chaque organisation devrait se préparer pour les imprévus – y compris les atteintes à la protection des données ou les cyberincidents. D'ailleurs, sans plan d'intervention en cas d'incident, il y a une plus grande chance de faire des erreurs lors de l'intervention en cas de violation ou d'atteinte – par exemple, en omettant de se conformer aux lois et règlements applicables. De telles erreurs peuvent causer des dommages à l'entreprise ou l'organisation qui sont encore plus importants que les dommages directement causés par l'attaque. Un plan d'intervention en cas d'incident bien conçu permettra à votre organisation de lancer plus facilement une intervention rapide et coordonnée.

DANS PLUS DE **90%** DES ATTEINTES, LE COMPROMIS NE DURE QUE QUELQUES MINUTES OU MOINS.

ET **99.6%** DU TEMPS, LES DONNÉES SONT EXFILTRÉES DANS LES JOURS QUI SUIVENT.[4]

HABITUELLEMENT, UN PLAN D'INTERVENTION EN CAS D'INCIDENT DEVRAIT INCLURE AU MOINS LES COMPOSANTES SUIVANTES :

1. DES RENSEIGNEMENTS SUR LES PERSONNES AU SEIN DE L'ORGANISATION QUI FORMERONT L'ÉQUIPE D'INTERVENTION EN CAS D'INCIDENT;

2. DES DIRECTIVES ET PROCÉDURES POUR AIDER L'ÉQUIPE; ET

3. DES RENSEIGNEMENTS CONCERNANT LES RESSOURCES EXTERNES QUI SONT DISPONIBLES POUR APPUYER L'ÉQUIPE.

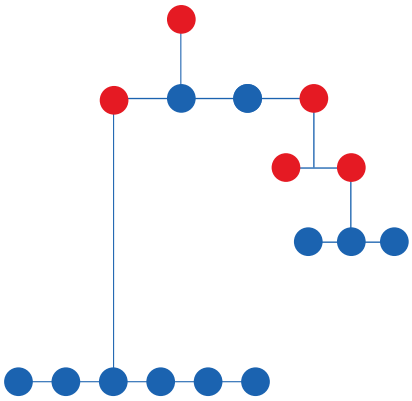
Équipe d'intervention en cas d'incident

Identifiez les membres de l'équipe par leur nom et titre, ainsi que par une description de leurs rôles et responsabilités. Un directeur qualifié, comme le Responsable de la sécurité de l'information, devrait agir à titre de chef d'équipe afin d'aider à coordonner l'effort global d'intervention. Les autres membres devraient inclure les représentants de la direction, du service des technologies de l'information, des services juridiques, de la conformité et des affaires publiques/relations avec les médias.

Procédures et directives – intervention en cas d'incident

Un plan d'intervention en cas d'incident devrait fournir un cadre afin que les décisions importantes puissent être considérées à l'avance et non prises sous pression. Il est d'ailleurs important qu'un plan d'intervention en cas d'incident fournisse des procédures et directives sur la façon de traiter les questions importantes, notamment en identifiant les pouvoirs hiérarchiques et les obligations internes en matière de signalement. L'équipe devrait se concentrer à prendre les meilleures décisions possibles et non à se demander comment et par qui ces décisions doivent être prises

Des procédures et directives claires concernant les questions suivantes peuvent grandement faciliter un effort d'intervention en cas d'incident :



- S'agit-il d'un cas où le plan d'intervention en cas d'incident s'applique? Ce ne sont pas tous les incidents en matière de sécurité qui nécessiteront l'application du plan.
- L'entreprise ou l'organisation est-elle assurée pour l'incident? Si oui, quand est-ce que l'assureur devrait être avisé?
- L'équipe devrait-elle apporter des ressources externes? Les autorités chargées de l'application de la loi devraient-elles être avisées? Qui aura la responsabilité principale de tout coordonner avec elles?
- Quand est-ce que certains services ou certaines parties du réseau devraient être éteintes ou transférées vers des systèmes de sauvegarde, le cas échéant? Les critères pour éteindre un serveur de messagerie par rapport à ceux pour éteindre un serveur de sites Web avec le client devraient probablement être différents, par exemple.
- Quelles données, si perdues ou exposées, sont assujetties à des lois visant la notification en cas d'atteinte à la protection des données? Si la notification est requise, quand et comment devrait-elle être faite?
- Quelles données, si perdues ou exposées, doivent être signalées aux organismes gouvernementaux chargés de la réglementation? Aux partenaires d'affaires?
- Les renseignements concernant l'incident devraient-ils être communiqués aux employés de l'organisation? Au public?
- Comment est-ce que l'équipe devrait documenter l'effort d'intervention en cas d'incident et comment devrait-elle conserver les dossiers ou la preuve recueillie au cours de l'enquête?

Un plan d'intervention en cas d'incident ne pourra évidemment pas prévoir des procédures et directives pour couvrir toutes les questions et tous les scénarios possibles. Les procédures et directives devraient être assez flexibles pour s'appliquer à une variété de cyberincidents différents, tout en fournissant des directives plus concrètes en regard des incidents qui surviendront plus probablement.

Ressources externes

Dépendant de la nature et de l'étendue de l'incident, il peut être approprié pour l'équipe d'intervention en cas d'incident de demander de l'aide auprès de ressources externes, notamment un « coach en cas d'atteinte », un expert judiciaire en informatique et en réseaux ou un consultant en gestion de crises. La plupart des entreprises n'ont pas d'employés qui ont en même temps l'expérience et le temps de gérer un effort d'intervention en cas d'incident.

Dans le cadre de l'élaboration d'un plan d'intervention en cas d'incident, il est important d'identifier des ressources externes et d'établir des liens avec elles avant qu'un incident ne survienne, afin que ces ressources soient prêtes à vous aider en cas de besoin. Il sera aussi plus rentable de négocier ces services avant la survenance d'un incident, au lieu d'attendre jusqu'à ce que votre organisation ait un besoin urgent de ceux-ci.

Si votre organisation sous-traite toute partie de ses fonctions en TI, le plan d'intervention en cas d'incident devrait aussi fournir les coordonnées de vos fournisseurs en TI. Il sera souvent nécessaire de travailler de concert avec vos fournisseurs en TI pour faire enquête et sécuriser la preuve après la survenance d'un incident de cybersécurité.

Une fois votre plan d'intervention en cas d'incident mis en place, il est important de le tester régulièrement – à chaque année si possible.

Tester le plan d'intervention en cas d'incident

Ces « exercices de simulation » devraient impliquer toute l'équipe d'intervention en cas d'incident et les résultats de ces tests devraient être mis à disposition de la haute direction. Mieux vaut traiter les questions qui peuvent être soulevées par la haute direction concernant le plan d'intervention en cas d'incident dans le cadre d'un exercice de simulation que lors d'un effort d'intervention en cas d'incident réel.

Aider à prévenir les cyberincidents qui occasionnent des dommages

PRÉVENEZ DES INCIDENTS :

- RENFORCER LES MÉCANISMES DE CONTRÔLE D'ACCÈS
- CORRIGER LES VULNÉRABILITÉS CONNUES
- FORMER VOS EMPLOYÉS
- ADOPTER DES POLITIQUES ET PROCÉDURES AXÉES SUR LA SÉCURITÉ

PRÉPARER – **PRÉVENIR** – ATTÉNUER – RESTAURER

Les mécanismes de contrôle de la sécurité et les plans d'intervention en cas d'incident sont nécessaires, mais ne sont pas nécessairement suffisants pour assurer une bonne cybersécurité. La mise en place des quatre directives suivantes aidera beaucoup votre organisation à prévenir efficacement des cyberincidents qui occasionnent des dommages :

1. Renforcez vos mécanismes de contrôle d'accès;
2. Corrigez sans délai les vulnérabilités au niveau des systèmes et des applications;
3. Formez vos employés en leur parlant des cyberrisques et des pratiques en matière de sécurité; et
4. Adoptez des politiques et procédures qui intègrent des bonnes pratiques en matière de sécurité dans le cadre des activités de votre entreprise.

Renforcer les mécanismes de contrôle d'accès

Nous sommes tous familiers avec les mots de passe, qui sont les types de mécanismes de contrôle d'accès les plus importants. Il existe de plus en plus de mécanismes de contrôle d'accès plus sophistiqués. Par exemple, de nombreuses banques et institutions financières ont commencé à exiger l'authentification à deux facteurs pour avoir un accès en ligne aux comptes bancaires et de nombreux téléphones intelligents et ordinateurs peuvent être débloqués au moyen d'identifiants biométriques, comme les empreintes digitales. La mise en place judicieuse de mécanismes de contrôle d'accès plus puissants, notamment en limitant le nombre d'employés ayant un accès à distance au réseau, peut constituer une façon rentable d'améliorer la cybersécurité de votre organisation.

Même sans adopter des nouvelles technologies de contrôle d'accès, les entreprises et organisations peuvent en profiter si elles adoptent le principe du moindre privilège : c'est-à-dire, l'accès aux données, systèmes et réseaux devrait uniquement être permis dans la mesure où cet accès est nécessaire pour assurer le bon fonctionnement continu des activités de l'entreprise. Certains renseignements peuvent être accessibles à tous; certains peuvent être restreints à un département spécifique; et d'autres devraient uniquement être accessibles par certains membres importants du personnel.

Le principe du moindre privilège devrait s'appliquer à tous les utilisateurs, y compris les administrateurs de systèmes et autres membres d'un département de TI. On considère souvent que l'utilisation inappropriée de privilèges administratifs constitue un facteur déterminant au niveau des atteintes à la protection de données et autres cyberincidents.

Dans de nombreuses organisations en pleine croissance, les administrateurs de systèmes assument plusieurs fonctions et ont accès à une multitude de systèmes et d'applications. Ceci peut entraîner un risque d'atteinte à la sécurité si les privilèges administratifs ne sont pas adéquatement contrôlés, facilitant ainsi la possibilité pour un pirate de contrôler entièrement un système compromis. Pour minimiser ce risque, les mécanismes de contrôle suivants devraient être considérés :

- Les utilisateurs ne devraient pas pouvoir obtenir des privilèges administratifs locaux, même sur des ordinateurs qui leur sont fournis à des fins d'utilisation exclusive.
- Les membres du personnel des TI devraient avoir des privilèges administratifs uniquement pour des systèmes ou applications spécifiques, et seulement dans la mesure où ces privilèges sont nécessaires dans le cadre de l'exécution de leurs fonctions.
- Les membres du personnel des TI qui ont des privilèges administratifs devraient maintenir des comptes distincts en ce qui concerne les utilisations quotidiennes et l'utilisation à titre d'administrateur des systèmes. Le compte de l'administrateur ne devrait pas être utilisé pour les accès de routine aux courriels ou à Internet. Le mot de passe relatif au compte de l'administrateur ne devrait pas être partagé, même avec les autres membres du personnel des TI, et devrait être différent du mot de passe du compte de l'utilisateur.
- Lorsque des privilèges plus larges doivent être accordés à un utilisateur ou un administrateur de système pour effectuer une tâche précise, ces privilèges peuvent être accordés mais uniquement pendant une période de temps limitée.

Finalement, il est important d'inclure des mécanismes de contrôle d'accès physiques pour les données et systèmes sensibles. Le fait d'assurer la sécurité physique de l'extérieur du bâtiment peut constituer la première étape de la protection visant l'accès non autorisé à un système ou un réseau. Il faut aussi protéger certaines zones, comme les salles de serveurs, les salles d'ordinateurs et les salles dotées de l'équipement téléphonique en adoptant des mesures de sécurité appropriées, notamment des portes verrouillées et des mécanismes de contrôle des entrées.

PRÈS DE 60 POUR CENT DES ORGANISATIONS CANADIENNES ONT SIGNALÉ AVOIR UTILISÉ UNE AUTHENTIFICATION MULTIFACTORIELLE EN 2016 AFIN D'AMÉLIORER LA CONFIANCE PARMI LES CLIENTS ET LES PARTENAIRES D'AFFAIRES.[5]

Corriger les vulnérabilités connues

Cette directive est simple : corrigez vos systèmes et logiciels. Une vulnérabilité qui n'est pas corrigée est l'une des méthodes les plus faciles et courantes de compromettre un système ou un réseau informatique.

Malheureusement, des obstacles importants peuvent empêcher d'assurer que tous les systèmes informatiques et applications de logiciels sont entièrement corrigés. Tout d'abord, sur la plupart des réseaux d'affaires, plusieurs applications fonctionnent sur divers systèmes différents. Toutes ces applications et tous ces systèmes peuvent exiger des correctifs, qui sont fournis par un flot de tiers fournisseurs. Deuxièmement, une bonne pratique est de tester les correctifs avant de les déployer, notamment en ce qui concerne les systèmes ou logiciels considérés critiques – pour éviter des délais. Finalement, les correctifs ne sont pas toujours appliqués avec succès, particulièrement sur les ordinateurs portables et autres appareils sans fil qui sont souvent déconnectés du réseau.

Ces difficultés peuvent être traitées en partie en utilisant un système de gestion des correctifs. Que ce soit en utilisant un système commercial de gestion des correctifs ou des outils élaborés à l'interne, le système devrait :

- **Aider à assurer le suivi des correctifs disponibles, les obtenir et les valider.**

  Pendant que les différents fournisseurs lancent des correctifs pour leurs produits, le système devrait identifier quels correctifs sont nécessaires au sein de votre environnement particulier et les mettre à la disposition du personnel des TI à des fins d'examen et d'évaluation.

- **Permettre les corrections sur une base prioritaire.**

  Les correctifs de routine peuvent être appliqués selon un échéancier prédéterminé, mais les correctifs urgents devraient être appliqués dès que possible.

- **Prévoir le signalement et la vérification.**

  Si le déploiement d'un correctif échoue à quelque endroit que ce soit sur votre réseau, le personnel des TI devrait facilement avoir accès aux renseignements concernant cette défaillance.

Une autre bonne pratique à suivre par les organisations est de scanner ses systèmes et réseaux régulièrement afin de détecter des vulnérabilités que le système de gestion des correctifs pourrait avoir manqué.

Dans certains cas, il peut être nécessaire de continuer d'utiliser un système ou une application qui a des vulnérabilités connues – par exemple, un ancien système qui a des vulnérabilités pour lesquelles il n'existe aucun correctif disponible. Dans ce cas, le système de vulnérabilités devrait être protégé attentivement en utilisant d'autres moyens, comme des pare-feu et des mécanismes de contrôle d'accès stricts.

Former vos employés

De nombreux incidents de cybersécurité peuvent être directement attribués au fait que la formation sur la sensibilisation aux questions de sécurité est défaillante. Un programme de formation conçu pour permettre aux employés de reconnaître des menaces courantes d'atteintes à la cybersécurité et d'aviser le personnel des TI constitue une façon rentable de réduire ces menaces.

Un programme de formation globale devrait :

- **Mettre l'emphase sur l'importance de la cybersécurité pour la réussite de l'organisation.** Les employés devraient comprendre pourquoi la sécurité des données, systèmes et réseaux est importante. Une atteinte à la sécurité peut permettre aux pirates de vider le compte bancaire d'une organisation; d'autres répercussions financières et juridiques peuvent s'ensuivre, comme des frais d'intervention en cas d'incident, des frais de notification en cas d'atteintes à la protection des données, une atteinte à la réputation et la perte de clientèle. Le cas échéant, des exigences légales et réglementaires pour protéger certains types de données, comme les renseignements personnels sur la santé, devraient être soulignées. La formation devrait traiter de la responsabilité de chacun des employés de protéger les données, systèmes et réseaux de l'organisation.
- **Former les employés pour éviter des risques d'atteintes à la sécurité des renseignements.** Les risques peuvent inclure l'hameçonnage et d'autres formes d'ingénierie sociale, ainsi que la mauvaise gestion des mots de passe, la navigation non sécuritaire sur Internet et l'utilisation non autorisée de logiciels.
- **Expliquer comment protéger des ordinateurs portables, des appareils sans fil et des supports de stockage numérique.** On devrait rappeler aux employés de protéger physiquement les données et appareils et leur expliquer quand et comment utiliser le cryptage. Les ordinateurs et autres biens matériels sont perdus au moins 100 fois plus souvent qu'ils ne sont volés.[6]
- **Encourager les employés à signaler les activités suspectes.** Les employés devraient connaître vos procédures d'intervention en cas d'incident et savoir comment signaler une activité suspecte, y compris des appels téléphoniques douteux, au personnel des TI ou chargé de la sécurité.

Finalement, les employés devraient aussi recevoir une formation sur les politiques et procédures liées à la cybersécurité. Dans plusieurs cas, le fait d'expliquer la raison d'être des politiques restrictives en matière d'« utilisation des systèmes » contribuera à favoriser un meilleur respect de celles-ci.

Le nombre de campagnes de harponnage ciblant employés a augmenté de 55 % en 2015.[7]

Adopter des politiques et procédures axées sur la sécurité

Une bonne cybersécurité sera difficile à atteindre si les politiques ou procédures de l'entreprise sont aléatoires – un pirate compétent peut compromettre le réseau complet d'une entreprise à partir d'un accès obtenu sur un ordinateur vulnérable.

Des politiques et procédures formelles peuvent améliorer grandement la cybersécurité au niveau de certains domaines particuliers :

LORSQUE DES NOUVEAUX APPAREILS SONT AJOUTÉS À UN RÉSEAU, IL DEVRAIT Y AVOIR DES PROCÉDURES POUR ASSURER QUE LES MOTS DE PASSE PAR DÉFAUT SOIENT CHANGÉS; QUE LES CORRECTIFS ET MISES À JOUR SOIENT MIS EN PLACE; ET QUE LES SERVICES, APPLICATIONS ET PORTS RÉSEAUX NON NÉCESSAIRES SOIENT RETIRÉS OU DÉSACTIVÉS.

- Une politique visant l'« utilisation des systèmes » devrait être mise en place pour régir l'utilisation des ordinateurs et réseaux de l'entreprise ou l'organisation, notamment avec des restrictions appropriées au niveau de l'utilisation des courriels, des médias sociaux, d'Internet, des appareils de stockage externe et des systèmes et logiciels non autorisés.
- Il devrait également y avoir des procédures visant les exigences relatives à l'élimination des renseignements et données sensibles, notamment les systèmes informatiques et appareils de stockage qui stockent ou traitent de telles données.
- Le contrôle inadéquat des changements visant l'équipement et les systèmes réseau peut constituer une cause courante des défaillances au niveau des systèmes et de la sécurité. L'absence de procédure écrite crée le risque que des changements soient apportés sans une préparation ou des essais adéquats. Il faut établir des procédures écrites qui régissent et coordonnent tous les changements au niveau des configurations existantes.
- Il devrait y avoir un processus qui permet de révoquer l'accès aux systèmes et réseaux sans délai lorsqu'un employé quitte l'entreprise ou l'organisation, et de changer les mots de passe et autres mécanismes de contrôle visant les comptes partagés, le cas échéant, que l'employé peut avoir connu ou auxquels il peut avoir eu accès. Il est aussi recommandé de faire signer une entente de confidentialité ou de non divulgation à l'employé, ainsi qu'une déclaration à l'effet qu'au moment de quitter l'entreprise ou l'organisation, il n'est parti avec aucune donnée sensible, exclusive ou autrement confidentielle.

Gestion des fournisseurs

Les entreprises et organisations doivent faire particulièrement attention aux politiques et procédures visant leurs fournisseurs – en TI ou autrement. La cybersécurité d'une organisation sera sérieusement mise en péril si un fournisseur dont la cybersécurité est faible obtient l'accès aux systèmes ou réseaux de l'organisation.

Conformément au principe du moindre privilège, une organisation devrait uniquement remettre à un fournisseur le niveau d'accès aux systèmes ou réseaux qui est nécessaire dans le cadre de l'exécution de ses responsabilités. Les fournisseurs devraient être assujettis aux mêmes exigences relatives aux mots de passe que les autres utilisateurs (ou administrateurs de systèmes, le cas échéant) et ne devraient pas utiliser le même mot de passe sur différents sites de clients. Une fois que l'organisation ne fait plus affaires avec le fournisseur, des politiques et procédures devraient être mises en place pour assurer que les références et privilèges d'accès soient immédiatement révoqués.

Les politiques et procédures de l'organisation devraient également assurer que le fournisseur a adopté des bonnes pratiques en matière de cybersécurité, qui sont appropriées eût égard au niveau de l'accès aux données, systèmes et réseaux fourni au fournisseur. Il pourrait être approprié, par exemple, d'inclure des dispositions dans le contrat qui prévoient des exigences en matière de cybersécurité, des ententes pour aider au niveau des enquêtes, des obligations en matière d'assurance, des dispositions visant l'indemnisation, etc. Si le fournisseur obtient l'accès à des données sensibles, notamment des renseignements personnels permettant l'identification, des mécanismes de contrôle supplémentaires pourraient être appropriés, comme par exemple d'exiger des évaluations préparées par des tiers sur les pratiques relatives à la cybersécurité du fournisseur.

Les pirates profitent de plus en plus des relations de sous-traitance pour avoir accès à des renseignements sensibles.[8]

Les cyberincidents ne sont pas nécessairement catastrophiques s'ils sont bien gérés.

ATTÉNUEZ LES DOMMAGES :

- DÉTECTER LES INCIDENTS RAPIDEMENT
- METTRE EN ŒUVRE VOTRE PLAN D'INTERVENTION
- OBTENIR DE L'AIDE LORSQUE NÉCESSAIRE
- DOCUMENTER VOTRE EFFORT D'INTERVENTION

PRÉPARER – PRÉVENIR – **ATTÉNUER** – RESTAURER

Les cyberincidents peuvent être inévitables mais ils ne sont pas nécessairement catastrophiques s'ils sont bien gérés. Une détection rapide est essentielle, de sorte que les organisations devraient examiner leurs réseaux et registres de sécurité aussi souvent que possible – en effet, une surveillance continue est un objectif louable.

Lorsqu'un incident survient, un plan d'intervention en cas d'incident bien conçu sera précieux pour aider l'entreprise ou l'organisation à partir des premiers stades d'intervention en cas d'incident – faire enquête, évaluer et atténuer – et ce, jusqu'à la restauration éventuelle des activités normales. Il sera souvent logique pour une organisation de faire appel à de l'aide extérieure afin de contenir les dommages occasionnés par un incident; il sera toujours logique de documenter les mesures prises durant le processus complet d'intervention en cas d'incident (ainsi que les raisons d'être de ces mesures).

Détecter les incidents rapidement

Même une organisation qui a une cybersécurité élevée ne peut pas assumer que son réseau est impénétrable. Par conséquent, il est essentiel de détecter rapidement les incidents afin d'atténuer les dommages en cas de compromis.

Heureusement, la plupart des systèmes (et de nombreuses applications) comprennent certaines capacités d'enregistrement ou de surveillance. Des pare-feu de réseaux peuvent être configurés pour enregistrer du trafic suspect et pour émettre des alertes selon des conditions déterminées. Presque tous les ordinateurs peuvent être configurés afin de faire le suivi de toutes les tentatives d'accès qui ont échoué, lesquelles constituent un indicateur rapide d'une attaque potentielle. Les entreprises et organisations devraient avoir connaissance des capacités d'enregistrement et de surveillance qui leur sont déjà disponibles; de plus, il existe des systèmes de surveillance du réseau pour des fins spéciales qui peuvent être mis en place pour permettre une surveillance plus accrue du trafic sur le réseau.

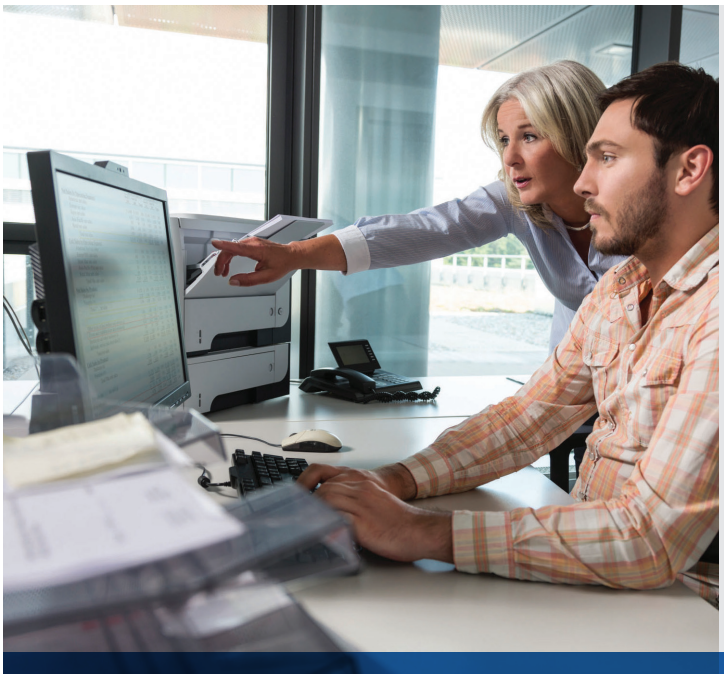
Habituellement, ce n'est toutefois pas pratique d'avoir tous les systèmes et applications configurés de façon à enregistrer le plus de données possibles. Les organisations devraient plutôt axer leurs capacités d'enregistrement et de surveillance sur la protection de leurs biens les plus précieux. Par exemple, les tentatives d'accès à une base de données centrale qui ont échoué devraient probablement faire l'objet d'une enquête approfondie plus rapidement que les tentatives d'accès à l'ordinateur d'un employé qui ont échoué.

Pour de nombreuses organisations, il sera logique d'utiliser un système de gestion des incidents liés à la sécurité, peu importe qu'ils soient mis en place à l'interne ou fourni par un fournisseur. Un tel système agit à titre de ressource centralisée afin de recueillir, de surveiller et d'analyser les registres de réseaux et autres renseignements liés à la sécurité. En utilisant un tel système, les organisations peuvent grandement réduire le risque de manquer les indicateurs précoces d'un compromis.

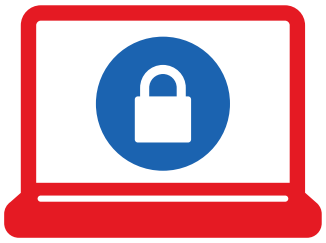
Mettre en œuvre votre plan d'intervention

Lorsqu'une organisation est affectée par un cyberincident, de nombreuses questions sans réponses surviennent pour savoir ce qui est arrivé, quelle en sera la conséquence et quoi faire par la suite.

Afin de répondre à ces questions, votre équipe d'intervention en cas d'incident devrait initialement se concentrer sur ce qui suit : faire enquête sur l'incident, évaluer ses effets et atténuer les dommages. Ces tâches doivent souvent être effectuées simultanément, en plein milieu d'une situation qui évolue rapidement, avec des renseignements incomplets et quelques fois inexacts. Dans de telles circonstances compliquées, un plan d'intervention en cas d'incident bien conçu aidera l'équipe à s'en sortir en délimitant les responsabilités de chacun, en facilitant le partage des renseignements et en identifiant les lignes directrices ou procédures pertinentes – par exemple, en décidant s'il faut utiliser ou non un expert judiciaire en informatique et en réseaux au cours de l'enquête.



AVISEZ VOTRE ASSUREUR SANS DÉLAI APRÈS LA DÉCOUVERTE D'UN INCIDENT. L'ASSURANCE VISANT LES CYBERRISQUES PEUT AIDER LES ENTREPRISES EN FOURNISSANT UN COACH EN CAS D'ATTEINTE, DES EXPERTS JUDICIAIRES ET D'AUTRES PROFESSIONNELS DU SECTEUR DE LA SÉCURITÉ DES DONNÉES.



Faire enquête sur l'incident

L'enquête sur un cyberincident important – au minimum, la détermination de la façon dont l'attaque a été effectuée, quels systèmes ont été compromis et quelles données ont été perdues ou exposées – prendra probablement beaucoup de temps et d'expertise. Une telle enquête implique habituellement ce qui suit :

- Conserver, recueillir et analyser les registres d'applications, de systèmes et de réseaux qui peuvent renfermer une preuve liée à l'attaque.
- Identifier les vulnérabilités au niveau des logiciels ou du matériel informatique utilisées pour faciliter l'attaque.
- Identifier les changements non autorisés affectant les systèmes sur le réseau, y compris l'installation de logiciels malveillants (« maliciels ») comme les enregistreurs de frappe (*keyloggers*) ou les chevaux de Troie.
- Déterminer quelles données, le cas échéant, ont été volées ou exposées, y compris les mots de passe ou autres mécanismes de contrôle de la sécurité qui ont pu avoir été compromis.

L'enquête pourrait avoir à inclure des appareils de réseau comme des pare-feu et des routeurs, et non seulement des ordinateurs et serveurs qui sont sur le réseau. Toute preuve importante obtenue au cours de l'enquête devrait être conservée adéquatement, de préférence après avoir consulté un conseiller juridique.

L'enquête peut également nécessiter que des employés, entrepreneurs ou autres tiers affectés par l'incident, ou autrement impliqués dans celui-ci, fassent l'objet d'entrevues. Les renseignements obtenus dans le cadre de telles entrevues devraient être constatés par écrit et les entrevues de tiers devraient préférablement être menées avec des conseillers juridiques.

Évaluer l'impact

L'impact d'un cyberincident sera habituellement évalué en fonction de différents facteurs : le nombre de systèmes affectés; la quantité de données perdues (qu'elle soit mesurée en fonction du volume des données ou du nombre de victimes dont les données ont été volées); l'ampleur de la perte financière; l'effet sur les activités d'une entreprise ou d'une organisation; et les difficultés anticipées pour se remettre sur pieds suite à l'incident, pour en nommer quelques-uns.

Ces évaluations seront nécessaires pour la haute direction et l'équipe d'intervention en cas d'incident afin de prendre des bonnes décisions à des moments critiques. Par exemple, le plan d'intervention en cas d'incident pourrait préciser qu'on devrait retenir les services d'un expert judiciaire en informatique et en réseaux si le nombre de systèmes affectés dépasse un certain seuil, ou si certains types de données (comme les renseignements sur les cartes de paiement) ont été volés ou exposés.

D'ailleurs, l'impact d'un cyberincident qui implique la perte de données sera grandement affecté selon le type de données en question. La perte de données sur le compte d'un client, par exemple, occasionnera probablement un effort d'intervention différent de celui qui surviendrait à la suite d'une perte des propres données de l'entreprise ou de l'organisation. À chaque fois qu'un cyberincident implique la perte réelle ou potentielle de données, un conseiller juridique devrait être étroitement impliqué au niveau de l'effort d'intervention en cas d'incident.

Atténuer les dommages

Une fois que la nature et l'étendue de l'attaque sont compris, l'équipe d'intervention en cas d'incident peut débuter le rétablissement et la restauration des données et systèmes perdus ou endommagés. Toutefois, si l'attaque cause des dommages courants à l'organisation, il peut être nécessaire de prendre des mesures pour atténuer les dommages avant même que l'enquête sur l'incident et l'évaluation de l'impact ne soient finalisées.

Nous pourrions décider de « tout fermer » sur un coup de tête – c'est-à-dire, tout faire pour interrompre l'attaque, comme déconnecter tous les systèmes qu'on sait avoir été compromis. Dans certains cas, ceci peut être la réponse appropriée.

Toutefois, on devrait tenir compte de d'autres facteurs avant de décider de « tout fermer ».

Premièrement, cette tactique pourrait ne pas fonctionner. On sait bien que les pirates tenteront de s'intégrer dans un réseau compromis, de sorte que désactiver un ou plusieurs ordinateurs compromis fera juste en sorte que le pirate ira ailleurs sur le réseau pour l'attaquer. L'effort d'atténuation visant à taper sur une taupe (*whack-a-mole*) peut distraire l'équipe d'intervention en cas d'incident et l'empêcher de se concentrer sur un plan de rétablissement et de restauration plus global.

Deuxièmement, tout fermer peut faire entrave à l'enquête. Si les pirates ont compromis un système dans lequel des données cryptées sont stockées, il pourrait être plus important de surveiller leurs activités pour savoir si les pirates ont été capables de déchiffrer les données que de fermer le système immédiatement.

Finalement, un effort d'atténuation entrepris trop rapidement, sans planification et considération suffisantes, peut lui-même causer des dommages à une entreprise ou une organisation. Il pourrait ne pas être utile, par exemple, de fermer le serveur de courriels d'une entreprise si un pirate a uniquement obtenu un accès limité au serveur sans avoir encore obtenu un accès aux courriels.

Au lieu de tout fermer, il pourrait être préférable d'atténuer les dommages en adoptant une stratégie de confinement – en fermant certaines portions du réseau que les pirates n'ont pas encore compromises ou en bloquant des points de sortie en reconfigurant les pare-feu afin de strictement limiter le trafic sortant.

Il peut être difficile pour une équipe d'intervention en cas d'incident de faire enquête, d'évaluer et d'atténuer les dommages découlant d'un cyberincident important. Par conséquent, il est souvent approprié pour l'organisation de soutenir l'équipe avec des ressources externes.

Obtenir de l'aide lorsque nécessaire

Il existe de nombreux experts et consultants externes qui peuvent aider une entreprise ou une organisation à intervenir efficacement lors d'un cyberincident. Une liste de ces ressources externes devrait être incluse dans le plan d'intervention en cas d'incident, ainsi que des lignes directrices et politiques qui aideront l'équipe d'intervention en cas d'incident à déterminer lorsqu'il faut faire appel à des ressources externes.

Ces ressources incluent :

Un « coach en cas d'atteinte » ou autre conseiller juridique externe. Un coach en cas d'atteinte qualifié peut donner des directives tout au long de l'effort d'intervention en cas d'incident, notamment sur des questions concernant la protection des renseignements personnels, les exigences relatives à la notification et la conformité à la réglementation. En outre, certains aspects de l'effort d'intervention en cas d'incident entrepris sous la direction d'un coach en cas d'atteinte peuvent être protégés par un privilège en cas de litige éventuel.

Un expert judiciaire en informatique et en réseaux. L'utilisation d'un expert judiciaire externe est nécessaire si le personnel des TI à l'interne n'a pas la capacité ou l'expertise requise pour faire enquête sur l'incident, laquelle pourrait nécessiter l'analyse de maliciels ou l'examen des registres détaillés du trafic sur le réseau. Il pourrait également être souhaitable d'utiliser un expert judiciaire externe si l'incident peut donner lieu à un litige.

Un consultant en gestion de crise. Un consultant en gestion de crise qualifié peut aider l'organisation à atténuer toute atteinte à la réputation pouvant résulter de l'incident.

Application de la loi. S'il existe une raison de croire qu'un crime a été commis, il peut être approprié de soumettre le dossier aux autorités chargées de l'application de la loi. Peu de cyberattaques surviennent de façon isolée; en faisant enquête sur des incidents similaires ou liés, les autorités chargées de l'application de la loi peuvent être en mesure de fournir des renseignements concernant les outils et techniques utilisés pour entreprendre l'attaque. Si l'attaque était à motivation financière, les autorités chargées de l'application de la loi peuvent être plus à même de retracer les fonds volés, le cas échéant.

Documenter votre effort d'intervention

Tout au long de l'effort d'intervention en cas d'incident, il est important de documenter les mesures prises par l'équipe d'intervention en cas d'incident. Ceci aidera votre organisation à mieux identifier les leçons tirées de l'incident, répondre à toute enquête judiciaire ou réglementaire future et réconcilier tout changement effectué sur vos systèmes et réseaux après que l'urgence de l'effort d'intervention se soit estompée. Le plan d'intervention en cas d'incident devrait inclure des formulaires ou autres directives qui aideront à assurer une tenue adéquate des dossiers.

Quelques fois, il peut être approprié pour un avocat d'être impliqué au niveau du travail de documentation de l'effort d'intervention en cas d'incident, car cela peut permettre à l'organisation de revendiquer un privilège sur les documents en cas de litige éventuel.

Compléter le chemin de la reprise.

RÉTABLIR LES ACTIVITÉS HABITUELLES :

- REMÉDIER, RESTAURER ET REMPLACER
- CONTINUER LA SURVEILLANCE
- COMMUNIQUER EFFICACEMENT
- METTRE EN ŒUVRE LES LEÇONS APPRISES

PRÉPARER – PRÉVENIR – ATTÉNUER – **RESTAURER**

Après avoir évalué la situation, votre organisation sera prête à compléter le chemin de la reprise : en corrigeant les vulnérabilités, en restaurant les systèmes et données perdus ou endommagés; et en remplaçant les mots de passe, les clés de cryptage et autres mécanismes de contrôle compromis.

Tout au long du parcours, il sera important de continuer de surveiller vos systèmes et réseaux afin de détecter des signes que les pirates ont réussi à contrer vos efforts afin de les éliminer. Il sera également important de fournir des renseignements exacts concernant l'incident, si et lorsqu'appropriés, aux personnes intéressés, peu importe qu'elles soient des employés, des partenaires d'affaires, des agents chargés de la réglementation ou autrement.

Finalement, votre organisation peut bénéficier de l'incident en identifiant et en mettant en application les leçons apprises après un examen attentif de l'incident et de l'effort d'intervention en cas d'incident.

Remédier, restaurer et remplacer

Ultimement, l'objectif visé par votre effort d'intervention en cas d'incident est d'éliminer les pirates de votre réseau et de retourner aux activités normales. Pour ce faire, vous devez :

- **Corriger les vulnérabilités.** Dans la plupart des cas, l'équipe d'intervention en cas d'incident aura tenté d'éliminer les vulnérabilités au fur et à mesure qu'elles sont découvertes au cours de l'enquête. Toute vulnérabilité restante qui compromet la sécurité des réseaux devrait être traitée à ce stade, au moyen de correctifs ou d'autres méthodes. S'il n'a pas été possible d'identifier les vulnérabilités utilisées par les pirates et de les corriger, l'effort de recouvrement pourrait être futile.
- **Restaurer les systèmes et données perdus ou endommagés.** Il sera beaucoup plus facile de restaurer des données provenant d'une copie de sauvegarde que de recréer des données perdues ou endommagées. Lorsqu'on restaure un système compromis, la méthode favorisée est de réinstaller le système d'exploitation et les applications à partir d'une image nette. Si ceci n'est pas possible, il faut s'assurer que tous les changements non voulus au système ont été identifiés et réparés. Sinon, une « porte de sortie » installée par les pirates pourrait être utilisée pour infecter à nouveau le système et le réseau.
- **Remplacer les mécanismes de contrôle compromis.** La dernière étape est cruciale, mais elle est souvent négligée. Lorsque les pirates compromettent un système ou réseau, ils sont souvent capables d'obtenir des renseignements concernant les mécanismes de contrôle de la sécurité, comme les mots de passe et clés de cryptage, qui peuvent être utilisés lors d'attaques subséquentes. L'équipe d'intervention en cas d'incident devrait porter attention aux mécanismes de contrôle de la sécurité qui pourraient avoir été compromis et non seulement aux mécanismes de contrôle de la sécurité qui ont été compromis.

Continuer la surveillance

Il est important de surveiller étroitement le réseau tout au long de l'effort d'intervention en cas d'incident. Il est également important de continuer de surveiller le réseau pendant une certaine période de temps, même après la fin de l'effort de recouvrement. Les pirates réagiront souvent aux mesures prises par l'équipe d'intervention en cas d'incident et une surveillance étroite du réseau peut permettre de saisir les objectifs visés par les pirates et leur façon de fonctionner.

Qui plus est, une surveillance continue du réseau permettra d'assurer que l'effort de recouvrement a été un succès. On devrait assumer que les pirates, une fois avoir réussi à s'implanter dans le réseau, auront pris des mesures pour s'incruster encore plus afin d'avoir accès au réseau même après que le point initial de compromis leur ait été refusé.

Dépendant de l'étendue et de la durée de l'incident, il pourrait être conseillé d'effectuer un scan des vulnérabilités contenues dans les systèmes et réseaux de l'entreprise ou de l'organisation. Ceci peut aider à assurer que tout changement effectué pendant l'effort d'intervention en cas d'incident n'a pas introduit des nouvelles vulnérabilités et peut également ajouter un réconfort à l'effet que l'effort d'intervention a, dans les faits, été une réussite.

Communiquer efficacement

Lorsque vous répondez à un cyberincident, il peut être très difficile de déterminer quels renseignements devraient être communiqués à l'interne et à l'externe, car les renseignements disponibles concernant l'incident peuvent être incomplets et non fiables. Le fait de fournir des renseignements qui s'avèrent par la suite être inexacts peut grandement porter atteinte à la réputation de l'organisation aux yeux de ses clients et actionnaires et peut aussi attirer l'attention des organismes de réglementation gouvernementaux. Par conséquent, il est essentiel pour l'organisation d'avoir établi une stratégie de communications efficace avant la survenance d'un cyberincident.

Lorsque l'on communique avec la haute direction, il est important pour l'équipe d'intervention en cas d'incident de fournir le plus de renseignements fiables possibles concernant l'étendue de l'incident, son impact potentiel sur l'organisation ainsi que la durée prévue de l'effort d'intervention. Il est préférable que ces renseignements soient fournis au moyen de l'un ou de plusieurs des points de contact désignés, préférablement identifiés dans le plan d'intervention en cas d'incident, et non au moyen de communications informelles ponctuelles avec différents membres de l'équipe d'intervention.

Lorsque vous décidez si et quand les renseignements doivent être communiqués à des tiers, y compris le public, ainsi que quels renseignements doivent être communiqués, pensez à ceci :

Facteurs à considérer :

Des renseignements concernant l'incident ont-ils déjà été rendus publics ou sont sur le point de l'être?

Si c'est le cas, il est probablement dans les meilleurs intérêts de l'organisation de faire une annonce publique afin de maintenir la confiance de ses clients et partenaires d'affaires et de se positionner comme étant la source d'autorité des renseignements. Si les renseignements concernant l'incident vont probablement devenir publics – par exemple, si l'incident impliquait une perte de données qui doit être signalée en vertu des lois sur la notification en cas d'atteintes à la protection des données – il est important de faire une annonce publique.

Quels renseignements fiables, le cas échéant, sont disponibles?

Au cours des premières phases d'un effort d'intervention en cas d'incident, il se peut qu'il n'y ait aucun renseignement fiable. Dans ce cas, si une annonce publique doit être faite, l'organisation peut, dans le mesure du possible, divulguer quand l'incident a été découvert pour la première fois, démontrer qu'elle a commencé à faire une enquête sans délai – notamment en collaborant avec les organismes chargés de l'application de la loi ou en impliquant des enquêteurs externes – et décrire les mesures correctives pour les tiers affectés, comme des services de surveillance du crédit.

Obligations de signalement des atteintes à la protection des données, de notification et de tenue des registres

À chaque fois que des données seront perdues à la suite d'un incident, il sera nécessaire de déterminer si la notification aux personnes physiques affectées ou si le signalement à des autorités responsables est requis par la loi. Cette tâche peut constituer un défi car il peut être difficile de déterminer quelles données ont été compromises et quelles lois s'appliquent. De plus, les lois sur les atteintes à la protection des données continuent d'évoluer. En effet, la *Loi sur la protection des renseignements personnels et les documents électroniques* (« LPRDE ») canadienne exige la notification des atteintes à la protection des données au Commissariat à la protection de la vie privée, aux personnes physiques affectées et dans certains cas, à d'autres tiers. Toutefois, ces dispositions entreront en vigueur uniquement après l'élaboration de règlements additionnels spécifiques qui prendront effet plus tard en 2017. Tant les obligations de signalement que les obligations de notification seront déclenchées lorsqu'il y a risque réel de préjudice important (*« real risk of significant harm »*), ce qui peut inclure un préjudice corporel, une atteinte à la réputation ou aux relations d'affaires, l'usurpation d'identité, une perte financière ou une perte d'emploi ou d'occasions d'affaires ou professionnelles. L'évaluation d'un risque réel de préjudice important nécessitera de tenir compte de la sensibilité des renseignements impliquées et de la probabilité que les renseignements aient été ou seront mal utilisés. Les organisations devront également consigner toute violation des mécanismes de protection des renseignements personnels, peu importe l'existence ou non d'exigences au niveau du signalement ou de la notification. Les nouvelles obligations aux termes de la LPRDE sont similaires à celles qui sont déjà en vigueur en Alberta, mais s'appliqueront à un éventail plus large d'organisations partout au pays. Les lois provinciales sur la protection des renseignements personnels sur la santé de l'Ontario, du Nouveau-Brunswick et de Terre-Neuve-et-Labrador renferment également des exigences en matière de signalement affectant le secteur de la santé.

Aux États-Unis, 48 des 50 États ont des lois visant la notification en cas d'atteintes à la protection des données et il existe d'autres lois fédérales et règlements fédéraux qui peuvent exiger la notification des personnes physiques affectées. En outre, vous devrez signaler les atteintes au niveau de certains secteurs, comme les secteurs de la santé et de la défense, à divers organismes étatiques et fédéraux.

Consultez des conseillers juridiques même si l'enquête sur l'incident n'est pas complétée afin d'évaluer vos obligations de signalement et votre stratégie de notification. Toute notification exigée en vertu de la loi devrait être globale et faite en temps opportun. Conservez des copies de toutes les notifications envoyées, ainsi que de toutes les réponses reçues. Il est également important de démontrer que vous comprenez vos obligations de signalement et êtes en train de prendre des mesures rapides et appropriées pour répondre à l'incident.

Mettre en œuvre les leçons apprises

Après s'en être remis d'un cyberincident, il est important d'identifier et d'appliquer toutes les leçons tirées de l'incident. En examinant l'incident et l'effort d'intervention à la suite de l'incident, une organisation a une occasion précieuse d'améliorer sa capacité de se protéger à l'encontre de cyberincidents éventuels et d'y répondre.

Le processus d'examen devrait inclure les membres de l'équipe d'intervention en cas d'incident ainsi que le personnel – les employés ou les consultants externes – qui n'étaient pas impliqués au niveau de l'effort d'intervention en cas d'incident. Le processus d'examen peut être grandement facilité avec un directeur qualifié qui n'était pas directement impliqué dans l'effort d'intervention

EXAMINEZ LES QUESTIONS SUIVANTES APRÈS UN CYBERINCIDENT :

- Des changements additionnels affectant les mécanismes de contrôle de la sécurité de l'organisation sont-ils nécessaires en plus de ceux déjà apportés par l'équipe d'intervention en cas d'incident? Les mesures correctives mises en place de façon urgente doivent-elles être changées ou modifiées pour le futur?
- Est-ce que des changements aux politiques visant la cybersécurité de l'organisation réduiraient la probabilité ou la sévérité de cyberincidents futurs? Est-ce que des changements aux pratiques commerciales globales de l'organisation (p. ex., concernant le type de renseignements recueillis ou stockés) réduiraient la probabilité ou la sévérité de cyberincidents futurs?
- Est-ce que des changements affectant le plan d'intervention en cas d'incident de l'organisation pourraient permettre à l'équipe d'intervention en cas d'incident d'intervenir plus rapidement et efficacement dans le futur?
- Est-ce que des ressources externes ont été utilisées et gérées comme il faut?
- Les renseignements appropriés ont-ils été communiqués en temps opportun à la haute direction?

EN APPRENDRE DAVANTAGE

Il y a toujours moyen d'améliorer la cybersécurité d'une entreprise ou d'une organisation. En effet, alors que l'univers des menaces est en constante évolution, les organisations doivent avoir comme objectif de continuellement s'améliorer afin d'éviter d'être la prochaine victime d'un cybercrime.

La Travelers Institute a hâte de travailler avec des entreprises et organisations afin de faire en sorte que notre monde numérique soit une source de grandes occasions et non pas de risques non gérables.

Pour obtenir plus de renseignements concernant l'initiative ***Cyber : Préparer, prévenir, atténuer et restaurer***, visitez le site travelersinstitute.org/cyber ou envoyez un courriel à institute@travelers.com. Des ressources supplémentaires en cyberrisques peuvent se trouver sur travelers.com/cyber.

À PROPOS DE LA TRAVELERS INSTITUTE

Travelers a établi la Travelers Institute comme moyen de participer au dialogue sur les politiques publiques concernant des questions d'intérêt pour le secteur de l'assurance des dommages, ainsi que de façon plus globale pour l'industrie des services financiers. La Travelers Institute s'appuie sur les connaissances de l'industrie de la haute direction de Travelers et l'expertise technique de ses professionnels des risques et autres experts pour fournir des renseignements et effectuer des analyses et recommandations aux responsables des politiques publiques et agents de la réglementation.

NOTES

[1] Symantec Corp., 2016 Internet Security Threat Report, Avril 2016, https://resource.elq.symantec.com/LP=2899

[2] Ponemon Institute, 2016 Cost of Data Breach Study: Global Analysis. Recherche commanditée par IBM. https://securityintelligence.com/cost-of-a-data-breach-2016

[3] National Institute of Standards and Technology, Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53 Rev. 4 (Avril 2013). http://www.nist.gov/manuscript-publication-search.cfm?pub_id=917904

[4] Verizon, 2016 Data Breach Investigations Report. http://news.verizonenterprise.com/2016/04/2016-data-breach-report-info

[5] PWC, Turnaround and transformation in cybersecurity: How Canadian businesses are responding to rising cyber-risks. Conclusions principales formulées dans The Global State of Information Security Survey 2016 (Canadian Insights). http://www.pwc.com/ca/en/technology-consulting/publication/pwc-gsiss-2016-canadian-insights-2015-11-en.pdf

[6] Verizon, 2016 Data Breach Investigations Report. http://news.verizonenterprise.com/2016/04/2016-data-breach-report-info

[7] Symantec Corp., 2016 Internet Security Threat Report, Avril 16, Volume 21. https://resource.elq.symantec.com/LP=2899

[8] M-Trends 2016, Mandiant, a FireEye Company, Février 2016. https://www.fireeye.com/currentthreats/annual-threat-report/mtrends.html

TRAVELERS INSTITUTE® | TRAVELERS

travelersinstitute.org

The Travelers Institute, 700 13th Street NW, Suite 1180, Washington, DC 20005