BUILDING A **SAFE** AND **RESILIENT CANADA**

Enhancing Canada's **Critical Infrastructure Resilience to Insider Risk**

Critical Infrastructure Directorate

Public Safety Canada
Sécurité publique Canada

Canada

At a Glance

What if the keys to the castle were in the hands of those that you were trying to defend against?

What if the contractor building your IT infrastructure was working for your competitor?

What if your most important asset was also your biggest vulnerability?

Insider risk relates to people working within an organization to subvert the confidentiality, integrity, and availability of the information contained within the walls of that entity. This guide establishes eight security actions that can be used to initiate or enhance an organization's approach to protecting against threats from within.

Cat. No.: PS9-12/2019E-PDF
ISBN: 978-0-660-30273-7

Table of Contents

Introduction

The purpose of this document is to provide Canadian critical infrastructure organizations with guidance on what constitutes insider risk and recommendations on how to monitor, respond to, and mitigate insider risk. This guide will assist organizations in developing their insider risk programs to defend against human and technical vulnerabilities, including those related to their partners, service providers, and associates. At the end of each security action is a list of internationally accepted and established security standards that originate from organizations such as the US National Institute of Technology (NIST), US National Insider risk Task Force (NITTF), and the International Organization for Standardization (ISO).

Many Canadian industries face challenges related to physical or computer security threats to their organizations. With increasingly diversified business processes that are connected to a cyber-centric world, owners and operators of Canada's critical infrastructure should be cognizant of their vulnerabilities towards all manners of threats, both physical and cyber.

An insider risk can be defined as anyone with knowledge or access to an organization's infrastructure (both physical and computer networks) who maliciously, or by chance, misuses their trusted access to harm the organization's employees, customers, assets, reputation or interests. As defined by Carnegie Mellon's CERT Insider Threat Centre (CERT Inside Threat Center, 2016), an insider risk is a person that works from within an organization to subvert the confidentiality, integrity, and availability of the information contained within the walls of that entity.

8 Recommended Security Actions

THEME 1
Establishing a Holistic Approach to Security

Security Action #1
Establish a Culture of Security[1]

Security is a fundamental and essential element of managing business risks, such as intentional and unintentional insiders. Organizations should develop and implement strong policies related to both physical and cyber security, with leadership coming from senior management. Organizational security policies should incorporate all areas of an organization and outline the responsibilities of all employees. The following actions highlight this holistic approach to security.

Establish Senior Management Engagement and Accountability

Strengthening an organization's security posture and building a secure environment to defend against risks is ultimately the responsibility of senior management. Cyber resilience and the management of cyber security risks are key challenges for organizations today. Organizations are rapidly recognizing the high risk of negative financial and/or reputational damage caused by security breaches. An organization where senior executives establish and support a strong security culture is crucial for obtaining employee buy-in and participation in maintaining a secure environment.

Identify a Senior Official Responsible for Managing Insider Risks

When implementing or managing insider risks, organizations should ensure that decision making responsibilities lie with a fully-accountable senior official from the organization. This official should be tasked with reporting and managing risks and should be supported by an insider risk working group with representation from various aspects of the organization, including human resources, legal, privacy, communications, technology, and security. In addition, this official and the working group should be provided with sufficient authority and resources, to fulfill their mandated duties, and should consider developing a public communications plan in advance of any insider risk issue.

Security Action #1

1) Establish Senior Management Engagement and Accountability
2) Identify a Senior Official Responsible for Managing Insider Risks
3) Build a Whole-of-Organization Commitment to Security and Emphasize Leadership at All Levels

1 Additional resources for insider risks can be found in the National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4, AT-1, AT-2 and AT-3; the Carnegie Mellon CERT Resilience Model (CERT-RMM), Organizational Training and Awareness; and ISO 27002: Information Security Awareness, Education and Training.

Build a Whole-of-Organization Commitment to Security and Emphasize Leadership at All Levels

An organization is as only as strong as its weakest link. A method to strengthen its risk posture to insider risks is by clearly communicating with all employees expected actions regarding security rules and codes of behavior for the organization. Properly designed policies regarding acceptable use of company systems, data, and other resources are instrumental in the establishment of an effective insider risk program. All applicable departments within an organization should also be involved in the development of policies regarding access to sensitive and important data and assets.

Organizational security should be championed by the executive leadership with the understanding that all levels of the company must play a role in building resilience. Ultimately a senior executive of the organization is responsible for setting security strategy and executing and fostering a strong culture of security and risk mitigation.

Organizations should:

Identify an organizational champion for managing insider risks with full accountability.

Identify a senior executive accountable for the development of a company-wide security policy and program.

Develop a governance structure, including an insider risk working group, to develop, deliver and manage an insider risk program.

Establish an organizational "pledge" to recognize the importance of security in delivering a profitable and sustainable business.

Design comprehensive physical and cyber network security policies and procedures encompassing all departments.

Promote a culture of security at all levels by linking employee and management performance to security metrics.

Security Action #2
Develop Clear Security Policies and Procedures[2]

In the current environment of inter-connectivity, risks from insiders can come from anyone, including an organization's employees, partners, associates, and third-party service providers. Any external organization or individual that has access to an organization's internal network, resources, personnel, facilities or digital assets should be considered a risk. The following actions are recommended to assist organizations in developing clear security policies and procedures to mitigate potential risks.

Define Clear Expectations and Outcomes

Security policies implemented by an organization should clearly state the rules and guidelines for employees, related to the following areas:

- Account access management;
- Password control and integrity;
- Access rights to physical and digital internal data or documents
- Personal internet use, social media access, as well as the downloading and storage of personal data to corporate networks;
- Employees participation in regular and appropriate training exercises; and
- Corrective actions and supplementary training

Identify Risk Levels of Positions in the Organization

Organizations should assign risk levels to all positions within an organization based on the access of the position to sensitive information and physical areas. This practice should apply to all employees, as well as contractors and subcontractors. It is also important to conduct periodic position assessments to identify any potential changes to position requirements, rules or responsibilities, and to adjust the risk level of the position accordingly.

Align Employee Access With Position Risk Levels

New employee screening should be commensurate with the level of risk assessed to complete the functions and tasks expected of that employee. For example, positions with greater access to sensitive information should be subject to more rigorous security checks. Other than the standard security procedures including credit and criminal checks, organizations should also investigate if necessary past performance claims, résumé information and face-to-face interviews. Reviewing and verifying all information available regarding a potential hire will facilitate in providing trusted access to organizational information and systems.

Security Action #2

1) Define Clear Expectations and Outcomes
2) Identify Risk Levels of Positions in the Organization
3) Align Employee Access with Position Risk Levels

2 Additional resources for insider risks can be found in the NIST Special Publication 800-53, Revision 4, RA-1, RA-3, PM-9; National Insider Threat Task Force, B-2 and C-6; and ISO 27002: Risks related to external parties and customers and third-party agreements.

Organizations should:

Clearly define, post, and educate employees in departmental security policies.

Conduct employee screening based on position requirements.

Assign appropriate risk levels of employees commensurate with the criticality and importance of the information, systems, and area that they access.

Security Action #3
Reduce Risks from Partners and Third Party Providers[3]

With expanded networks and increased user access, and data storage footprints, it is important to build security measures and expectations into any service agreement with third party providers. Understanding where key assets and systems are located and structured and how partners and third-parties access the organization's network and facilities is a critical step in reducing and mitigating risks. The following actions are recommended to help an organization reduce potential risks from third parties.

Understand Key Assets and Systems

Third-party organizations, contractors, consultants, and outsourced service providers that have physical access to an organization, its data, or computer systems, should be scrutinized as potential sources for insider access. This can primarily be accomplished if the organization has identified its critical assets and data, where it is located and implement controls to limit access to it. Implementation of network and data access controls and monitoring is very important in reducing any potential risks by partners and third party service providers.

Know Your Partners

Security agreements between the organization and its business partners and associates that govern such areas as data ownership, confidentiality, intellectual property, and nondisclosure agreements should be considered. The security posture of third party service providers should be the

3 Additional resources for insider risks can be found in the NIST Special Publication 800-53, Revision 4, RA-3 and PM-9; National Insider Threat Task Force, B-2 and C-6; the CERT-RMM External dependencies, human resources, and access control sections; and ISO 27002.

responsibility of the third party. However, it is important to independently verify the security processes of partners, including employee background checks, and what functions, if any, are sub-contracted to other entities. In addition, building trusted and long-term relationships and incorporating assurance language into third party contracts is important in reducing security risks in the supply chain of an organization.

Security Action #3

1) Understand Key Assets and Systems
2) Know your partners
3) Know your risks

Know Your Risks

An ideal opportunity to assess an organization's security requirements and threat environment is during a complete enterprise-wide risk assessment. Knowledge of the security environment within an organization and the identification of potential threats will assist in the development of appropriate security policies related to data access and network account management. Additionally, an internal risk assessment will identify those critical assets that are deemed most important to the organization's business operations as well as the potential threats to those assets. Asset identification is important in any decisions to identify the risks associated with providing third-party access to vital systems and key assets.

Organizations should:

Conduct an organization-wide risk assessment identifying all key assets and critical systems; Identify all security concerns related to third-party access to its networks, data and systems.

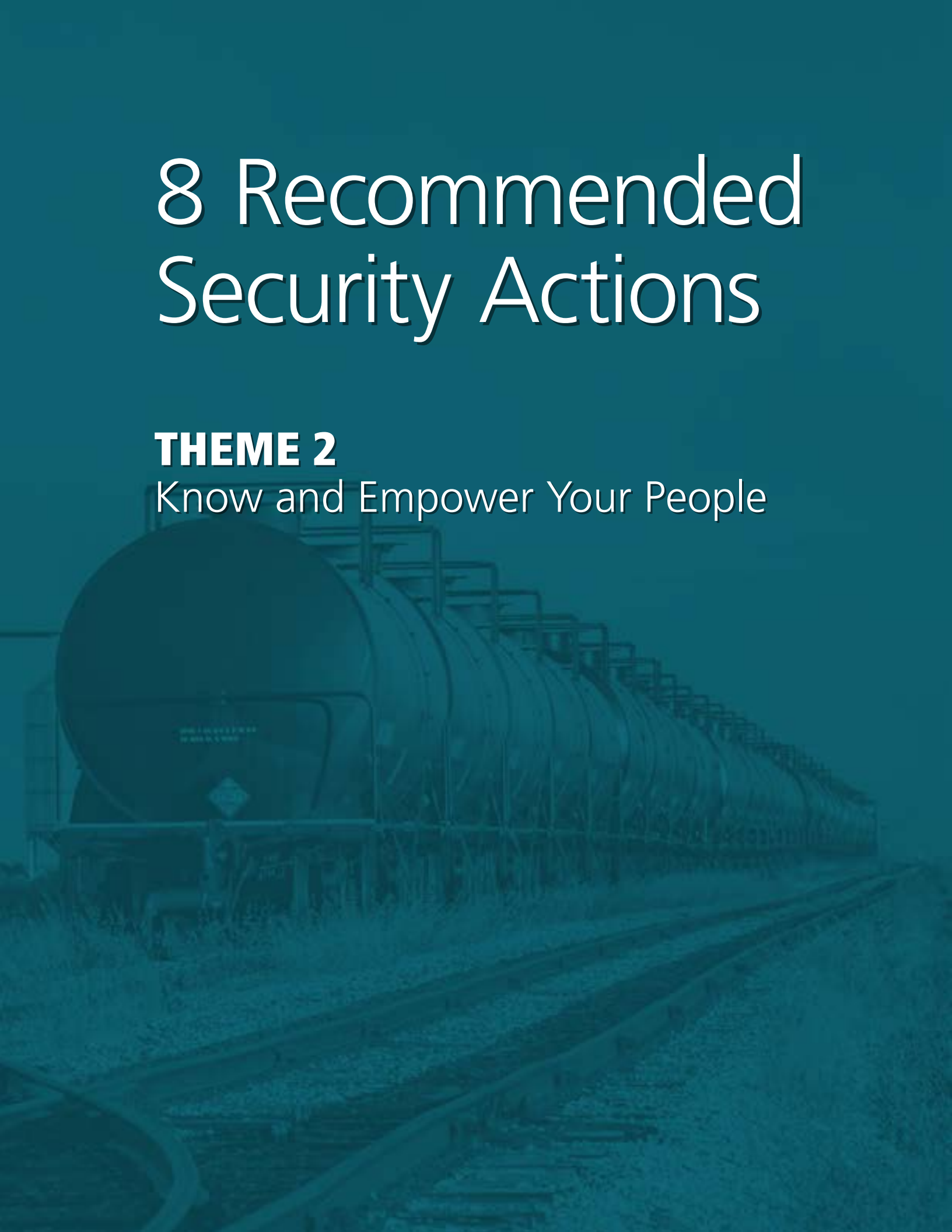
Independently verify the security posture of third party service providers, including background checks of employees with access to an organization's critical facilities or networks.

Ensure comprehensive third-party security agreements, with assurance language included in the agreements, to reduce supply chain risk.

Build long-term trusted relationships with key service providers.

8 Recommended Security Actions

THEME 2
Know and Empower Your People



Security Action #4
Implement a Personnel Screening Life-Cycle[4]

Employees are both an organization's biggest asset and its biggest vulnerability. The leadership within an organization should pursue a comprehensive approach to the management of human resources and should take steps to minimize their exposure to insider risk situations. The following actions are recommended to bolster human resource management.

Conduct Pre-employment Screening

Reducing the risk of insider risk should start at the beginning of the hiring process, as there are a number of actions that can be taken at this early stage. Criminal, credit, and reference checks should be administered to identify any potential areas or indicators of concern. Conducting preliminary research including thorough social media vetting can help in determining an employee's risk profile with regards to their access to critical, confidential, or propriety information or systems within the organization.

Implment Ongoing Employee Security Screening

Organizations should review and update their security screening of employees at periodic intervals (e.g. every 5 years) or as the situation warrants. It should be recognized that risk levels can change over time and consequently periodic background checks and credit checks comparative to the security level of any given position can identify unusual activities and behaviors that might have otherwise gone unnoticed. For instance, if an employee is taking on new responsibilities, or is moving to a position with a higher risk profile, a more thorough background check might be required.

Incorporate Departure and Internal Movement Procedures

When an employee leaves an organization, procedures and policies should be in place to ensure that their accounts are disabled and physical access to company premises and computer systems or data are rescinded. This includes having manager accountability for all termination procedures for employees departing the organization. Passwords issued to individuals should be cancelled; access passes and identity cards returned to the designated security officer; and laptops, mobile phones, or any other type of device accounted for. These procedures will reduce the risk of an individual accessing internal physical or network assets after their departure from the organization. In addition to employees departing an organization, organizations should amend access privileges for employees if they move to different functional areas within the same organization.

Security Action #4

1) Pre-employment screening
2) Ongoing employee security screening
3) Departure and internal movement procedures
4) Transparent security policies

4 Additional resources for insider risks can be found in the NIST Special Publication 800-53, Revision 4, PS-1, PS-2, PS-3, and PS-8.

Establish Transparent Security Policies

The practice of having transparent organizational-wide security policies will help reduce insider risks. Background screening policies should cover all employees, and must be non-discriminatory. Information uncovered during a background check must be properly weighed against the organization's risk tolerance and employees should be provided the opportunity to dispute any findings that might be inaccurate. In addition, an organization should have an established formal grievance process in place should employees wish to appeal a decision.

Organizations should:

Conduct thorough pre-employment and continuous screening of all personnel using all resources available, including social media.

Update security access and clearances for employees based on the roles and responsibilities of their position.

Amend access privileges for employees that have moved to new positions within the organization.

Promote a transparent security program to all employees to manage physical and network security expectations.

Security Action #5
Provide Training, Raise Awareness and Conduct Exercises[5]

Recognizing that employees are an organizations "front- line" in detecting and reporting potential insider risks, a robust training program is paramount to strengthening an organizations security posture. The following three recommendations are suggested to improve risk awareness training for employees.

Provide Regular Training to Decrease the Risk of Unintended Security Infractions

To ensure that employees understand the risk environment, it is essential to provide effective and continual security awareness training. As potential threats could manifest themselves in both the physical and cyber domains, organizations need to be comprehensive in their approach. For example, with respect to unintentional insider risks, employees should be trained on a number of areas, including recognizing phishing schemes, ensuring password integrity, use of portable media and access to social media. Employees should be made aware that social media is often used to build target profiles and to gain access to employee credentials or company information.

Raise Awareness of Potential Warning Signs

It is important for organizations to convey to employees the potential impacts that insider risks can have on an organization, and potential warning signs regarding employee behavior. While there is no particular profile established to readily identify a malicious or an unintentional insider risk, employees should be trained to recognize behaviour within the organization that could potentially lead to the manifestation of malicious insider risk activity. The following is a list of attributions and actions that could be considered when determining if someone could become an insider risk:

- Alcohol or substance abuse;
- Argumentative or combative personality at work;
- Changes in financial situation;
- Disregard for policies and procedures;
- Frequent attempts to access unauthorized files or systems;
- Termination or unexpected resignation;
- Absenteeism;

---

5 Additional resources for insider risks can be found in the NIST Special Publication 800-53, Revision 4, AT-1, AT-2, and AT-3; and ISO 27002: 8.2.2 Information awareness, education, and training

- Unauthorized travel; and
- Unauthorized contact with foreign representatives and/or competitors.

This list is not exhaustive, and individuals who exhibit any or some of these behaviours are not necessarily at risk of becoming malicious actors. The intent of awareness is to influence people to consider and identify potential threats before they materialize, and the list mentioned above identifies common characteristics found in previous insider risk cases. Organizations should also develop employee assistance mechanisms to help prevent employees from becoming at risk of compromise.

Foster a Culture of Vigilance and Empower Employees

Organizations must foster a culture of security in order for its policies and programs to be effective. To build this culture of security, it is important for employees to be part of the solution, and to recognize that a combined and organizational approach to security is of benefit to all.

The most important step for an organization is to help its employees identify the warning signs that may signal future acts of insider risk activity. For example, the philosophy of "See Something, Say Something" has been adapted by multiple countries, including Canada, and empowers all people to be vigilant in addressing potential threats. Such a call to action should be non-intrusive and an intrinsic part of corporate culture and training so as not to create an environment of mistrust. Employees and management should understand that everyone has a role to play in security and sometimes the smallest indicators could be relevant to identifying a larger threat.

Security Action #5

1) Provide Regular Training to Decrease the Risk of Unintended Security Infractions
2) Raise Awareness of Potential Warning Signs
3) Foster a Culture of Vigilance and Empower Employees

Unusual activity relating to insider risk could be any observed behavior indicating potential or perceived malicious harm to the organization. Some of these activities could be innocent; however, it is up to trained enforcement and security personal to determine whether the behavior warrants investigation. If unusual activity is observed, people should be encouraged to report it to management or senior management within the organization to take appropriate action. If unusual activity is observed it is encouraged for witnesses to provide:

- Who or what was seen;
- When was it seen;
- Where did it occur; and
- Why it is unusual.

Organizations should:

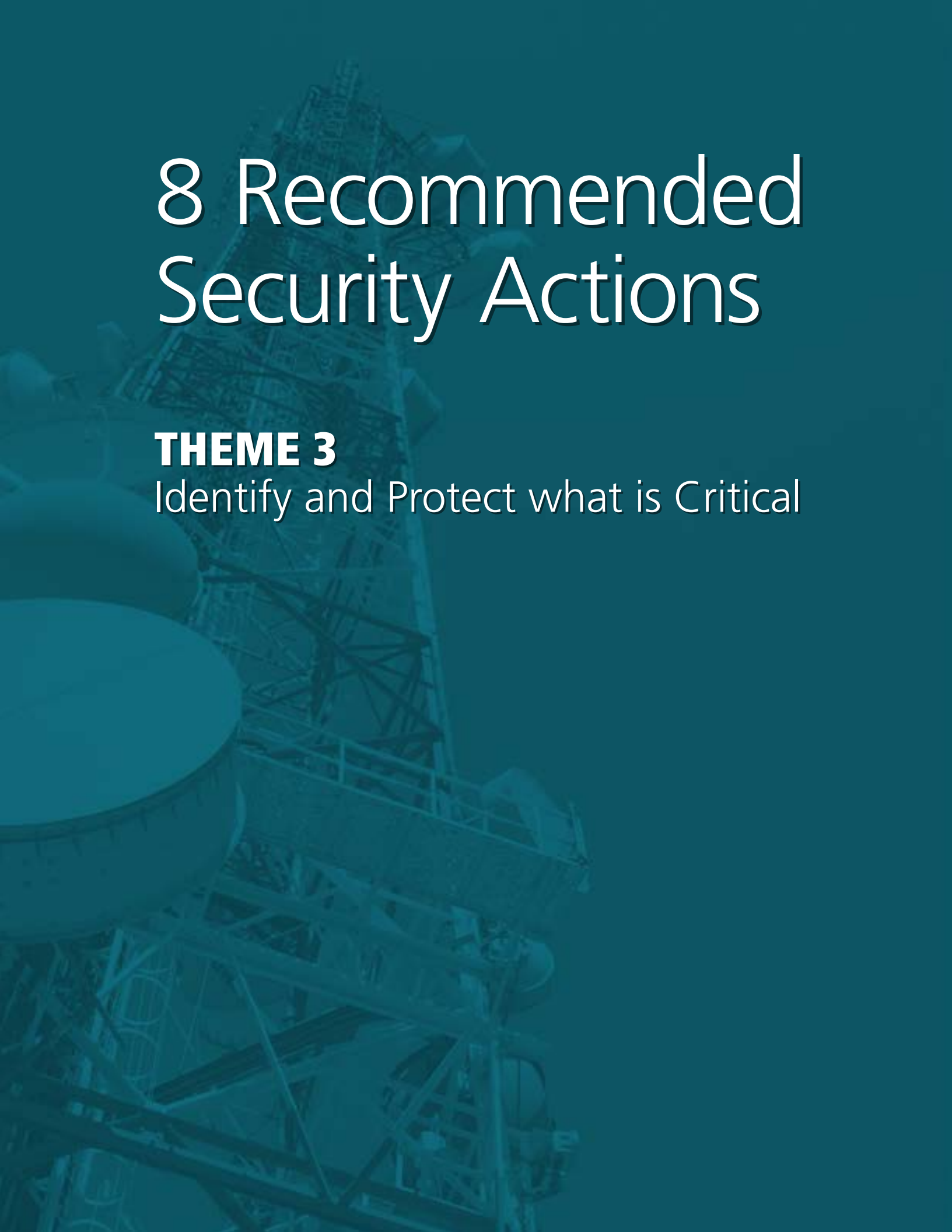
Develop a security training program for all employees.

Raise awareness of indicators of potential security concerns.

Provide access to employee assistance programs to help prevent employees from becoming at risk of compromise.

Develop and promote a culture of security vigilance by encouraging employees to say something if they see something.

Conduct periodic exercises to test the security posture within an organization.



8 Recommended Security Actions

THEME 3
Identify and Protect what is Critical

Security Action #6
Identify Critical Assets and Protect Them[6]

A critical asset can be viewed as anything, that if destroyed, altered, or otherwise degraded, would impact the confidentially, integrity, or availability of essential services. The following is a list of suggestions to improve an organization's understanding and protection of their critical assets.

Identify and Rank Key Assets and Systems

It is essential for any organization to develop effective and efficient measures of protection and deterrence to understand the breadth, complexity, and depth of the assets that compose their systems and infrastructure. Critical assets include, but are not limited to, facilities, systems, equipment, technology, and intellectual property. Organizations should include the identification and ranking of critical assets and systems as a key part of business continuity planning.

There are a number of methods or techniques available to identify and rank assets. For example, one method for an organization to identify its critical assets is to conduct a risk assessment. A risk assessment will help identify the organization's critical assets, to discuss systems process, data and their current risk profile. For an assessment of this nature, organizations will be able to rank and accurately score their critical assets and subsequently develop a mitigation strategy to protect them. When integrated into business continuity planning for the organization, asset criticality can be assessed and the appropriate security measures implemented.

Secure Key Assets and Systems

Organizations should also implement security procedures that guard against both physical and computer-based access. Such procedures can include security checkpoints, two factor authentications for accessing computer networks, firewalls, network monitoring, or any other methods that are designed for restricting access to authorized users. In addition, organizations should develop an approach to monitoring system usage by authorized and unauthorized users as well as access to physical premises during off-hours. Architecture documents should also outline how/what data is being sent to 3rd parties and the sensitivity of the data, as data deemed to be critical or sensitive should be masked or encrypted. Further, it is essential to have both visually recognizable and inherent security defences in place to guard assets, with the level of protection being associated with the criticality of the asset.

---

6 Additional resources for insider risks can be found in the NIST Special Publication 800-53, Revision 4, CP-2(8), CM-2, CM-8, PM-5, PM-8, and RA-2; and ISO 27002 – 7.1.1 Inventory of Assets.

Leverage Signage and Visible Deterrents to Access

A holistic approach to asset protection must include visible protection measures for employees to reduce the chances of unintended access. The proper use of signs and other visible deterrents can provide clear instructions to reduce unintended access by employees. These can be prominent measures such as security guards, fences, and traffic check points, to more subtle tactics such as warning signs indicating restricted access, document labelling, or posted policies and regulations.

Areas where there is a need for physical control of access should be clearly identified and demarcated to assist in unintended and accidental access. Warning signs are a common but clear way to identify restricted areas and manage the flow of personnel. From an information protection perspective, the proper labeling of information should be done in such a way that personnel can immediately recognize sensitive data and apply the correct handling, storage or destruction protocols.

Apply the Principle of Least Privilege

The principle of least privileged should be applied to restrict users a minimal level of access required to perform their duties effectively. Restricting access to an organization's networks and infrastructure using this principle can be instrumental to mitigate insider risk. For example, a user who is responsible for processing invoices to pay suppliers most likely does not need access to personnel files. Similarly, a heavy machinery operator most likely does not need to access a control room. The fundamental objective of this principle is to take a strategic approach to access control within an organization.

Security Action #6

1) Identify and Rank Key Assets and Systems
2) Secure Key Assets and Systems
3) Signage and Visible Deterrents to Access
4) Principle of Least Privilege
5) Separation of Duties

Separate Duties

Organizations should consider dividing key functions among a number of people to ensure that a single individual cannot misuse sensitive information or sabotage key assets. If responsibilities are shared among trusted employees, the risk of insider malicious activities against an organization is reduced through the mutual sharing of responsibility and accountability. Sharing of responsibilities also provides continuity should someone leave a critical position. However, there is an associated cost with the training that may be required for responsibility sharing, and it becomes the responsibility of an organization to find the balance that works best for their environment.

Organizations should:

Conduct an organization-wide assessment to identify and rank critical assets and systems and security measures to protect them.

Monitor system usage by authorized and unauthorized users as well as physical premises access.

Outline how/what data is being sent to 3rd parties and the sensitivity of the data, as protect data appropriately.

Consider the principle of least privilege and separation of duties for critical systems and data.

Leverage visible deterrents to decrease the likelihood of unintended access to facilities, networks and systems.

Security Action #7
Monitor, Respond to and Mitigate Unusual Behaviour[7]

The establishment of a security program within an organization should include procedures to monitor both physical and network behaviour and a plan for responding to any incident. Appropriate physical security controls and a means of tracking access along with effective employee awareness and vigilance should help reduce insider risk. The following are some recommended actions that could reduce organizational risks of insiders.

Track Remote Access and Monitor Device Endpoints

Organizations should be aware of the remote access technologies used by employees and the potential risks to their organization's systems and data. Motivated attackers often enter organizations remotely, either while employed or after termination, using legitimate access provided by the organization. This type of access can be prevented, or at the very least

7 Additional resources for insider risks can be found in the NIST Special Publication 800-53, Revision 4, AC-2, AC-17, and AC-19; and ISO 27002: 11.4.2.

monitored, through organizational policy and technology solutions. It is recommended that where possible, access to critical data only be granted to employees who are physically located in the workplace, and not those who work remotely.

Organizations have been increasingly adopting policies that encourage teleworking or some other form of mobile work arrangement. As such, remote access to corporate networks via smartphones, laptops, and tablets has become the new norm. Remote access to an organization's computer systems provides an ideal opportunity for malicious actors to attack and/or gain access to systems. While remote access can enhance employee productivity, remote access to critical data, processes, and information systems must be granted with caution and documented by the organization.

Organizations should also consider capturing full packet content or network flow data at its network perimeter. Anomalies such as large amounts of digital information leaving the network may indicate possible compromise or unauthorized access. Organizations should also consider monitoring the use of printers, scanners, copiers, and fax machines to mitigate data exfiltration against large volumes of information being copied, downloaded, and faxed.

Establish Effective Incident Reporting, Tracking, and Response Measures

Organizations should establish a process where unusual behaviour or potential incidents can be reported and tracked in a confidential manner. Management should consider the most appropriate action to take when an incident is reported, including senior management accountability for mitigating any possible insider risk activity. This could include a personal employee interview, regular network monitoring, and employee termination or law enforcement intervention depending on the severity of the event.

Security Action #7

1) Track Remote Access and Monitor Device Endpoints
2) Establish Effective Incident Reporting, Tracking, and Response Measures
3) Awareness and Implications of Social Networking Sites

Raise Awareness of best practices regarding the use of Social Networking Sites

Organizations should develop transparent policies and procedures on the appropriate use of social networking sites (SNS) in the workplace to ensure that employees are not posting information that could make them susceptible to unintentional information disclosure or deliberate disclosure. The use of SNS in the workplace raises privacy implications for both employees and employers and increases the overall risk for opportunistic insiders. Employees should be aware that any of the information or communications posted on their SNS can potentially be accessed by everyone, including the organization itself. It should also be noted that SNS can also be used as an early warning platform for individuals who may have become potential insider threats.

Organizations should:

Establish a means of monitoring physical and network access from all endpoints and remote devices.

Develop a culture that enhances employee awareness of security and reporting unusual activity or abnormal behaviour.

Raise awareness of the potential risks associated with social media sites.

Limit remote access to non-critical assets and systems where possible.

Establish protocols to report, track and respond to unusual incidents.

Consider engaging the security and intelligence community, including the RCMP or CSIS.

Security Action #8
Protect Your Data[8]

Prevention is a first line of defence against internal threats. Organizations should ensure their critical systems and data are not only protected, but also backed-up with a recovery plan in place to minimize interruption if a compromise occurs. Having effective backup and recovery mechanisms in place can significantly reduce the amount of time needed to restore a system following an incident. Data and systems backup, recovery and monitoring procedures should include the following considerations.

Establish and Test Business Continuity Plans and Procedures.

When possible, organizations should have multiple copies of data backups, stored in a secure, offsite location. This includes controlling access to physical backup documentation and data, with no single individual having access to both online data and the physical backup media. In addition, organizations should require full disclosure of any third party vendors sub-contracted to provide backup services, including offsite storage. Organizations should

8 Additional resources for insider risks can be found in the NIST Special Publication 800-53, Revision 4, CP-2, CP-3, CP-4, CP-6, CP-9, and CP-10; and ISO 27002: 10.5.1.

also test their backup and recovery processes on a regular basis as part of their disaster recovery and continuity planning.

Implement Procedures to Limit Information Exit Points

One of the challenges for organizations is to ensure that they not only are aware where their data resides, but through which routes and by what methods it can exit their networks and systems. Policies should be established within an organization to define acceptable rules and guidelines for downloading and storing large amounts of data or sensitive files. Policies for the use of portable storage devices (thumb drives, hard disk devices, and mobile devices) should also be implemented, particularly if they are connected or have access to the organization's computer network. In addition to limiting sources of potential information exfiltration points, organizations can consolidate the access points to the internet so as to provide maximum monitoring and detection at limited egress and ingress locations. Lastly, organizations can implement segregated systems that prevent data loss through isolated devices with limited to no network connectivity. For example, an organization could provide employee access to the internet via a separate computer that is not connected to the corporate network in any way.

Security Action #8

1) Establishing and Testing Business Continuity Plans and Procedures.
2) Implementing Procedures to Limit Information Exit Points

Organizations should:

Backup and protect all organizational data and essential systems on a regular basis.

Develop policies for downloading large amounts of data or sensitive files.

Consolidate access points to the internet.

Implement segregated systems to prevent data loss.

Limit or restrict portable storage devices.

Conclusion

The threat from within can originate from any person at any time, and there is no one solution to either identify or prevent this type of activity. The insider risk, however, is fundamentally another type of organizational risk that can be properly mitigated though a holistic approach to measures and tactics designed to limit exposure and reduce risk. An organizational approach to reducing insider risk should start at the beginning of the hiring process and continue throughout the lifecycle of employment. Organizations should also proactively and immediately deal with employees displaying unusual behaviours. Criminal and credit background checks, as well as discussions with previous employers about a prospective hire, should be administered. Organizations should also have policies and procedures for employees to report concerning or disruptive behaviour by co-workers as well as a robust employee assistance program to aid those in times of hardship or stress.

Technology also plays an important role in the detection and mitigation of insider risks. Adequate monitoring of all digital assets of the organization is essential, including its critical data and the information stored on its network. Access to information and corporate systems should be risk-managed depending on the sensitivity of the data being accessed. In addition, movement of sensitive information, large data files, and network activity should be monitored, and all relevant data should be backed-up and verified on a regular basis.

An organization's people can be its biggest strength, or their biggest vulnerability, with motivated and accidental insiders possessing the power to cause potentially crippling effects to any organization. Organizations must therefore be vigilant and resilient; continuously monitor the threat landscape; meticulously plan for response and recovery activities; and implement measures to protect against incidents. An insider risk can be a risk to all organizations no matter the industry, geography, and type of target. By following the eight security actions recommended in this guide, organizations can develop or improve upon their own insider risk programs.

While it is recommended that all of these actions be taken, it is recognized that given finite resources, this may not be possible for any given organization. However, any one of the security actions identified throughout this document would positively impact an organization's security posture to insider risks.

ANNEX A
Insider Risk Scenarios

The following two insider risk scenarios are hypothetical and incorporate elements of the eight security actions outlined earlier in this guide. Both scenarios demonstrate the importance of implementing proper security actions and can be used as a learning opportunity to mitigate insider risk.

Scenario #1
Intentional Insider risk

Within many organizations there are people with access to, and control over, sensitive information. The question to be asked is, "What if one of these individuals becomes motivated to harm that organization, and what would be the impacts to an organization?" As an example, imagine an informatics employee who has administrator level privileges within an organization and who is slated to be laid off. Such an event could motivate the employee to access the systems either directly or remotely and cause undue hardships for users by deleting their user privileges or login information. Should the individual be motivated to cause more substantial damage, he or she could either affect critical systems or remove proprietary information that are crucial to the organization's business. To complicate the situation, the individual could also take measures to prevent recovery, such as deleting or preventing access to backups. This combination of actions could cripple any organization that is subjected to such an attack. This is a typical insider risk situation and a demonstration of 6 of the security actions presented above, namely:

- **Security Action #1: Establish a Culture of Security:** Security is a fundamental and essential element of managing business risks, such as intentional and unintentional insiders. Organizational security policies should incorporate all areas of an organization and outline the responsibilities of all employees.
- **Security Action #5: Provide Training, Raise Awareness and Conduct Exercises:** Closer attention and monitoring should have been placed on the individual closer to his termination date.
- **Security Action #6: Identify Critical Assets and Protect Them:** This situation could have been prevented if key functions within the organization were divided, so that a single individual could not steal or modify data.
- **Security Action #7 Monitor, Respond to and Mitigate Unusual Behaviour:** By granting remote access to only email and non-critical data, the organization would have prevented the data exfiltration.
- **Security Action #8 Protect Your Data:** Capturing full packet content at the perimeter or at minimum, capturing network flow data and sending an alert to senior management on anomalies at these exit points, may have prevented the breach.
- **Security Action #8 Protect Your Data:** This could have been prevented by controlling access to the physical media, meaning no one individual should have access to both the online data and the physical backup media. The two person rule could also be applied where no one individual has full access, but requires the passcode or approval of a second administrator.

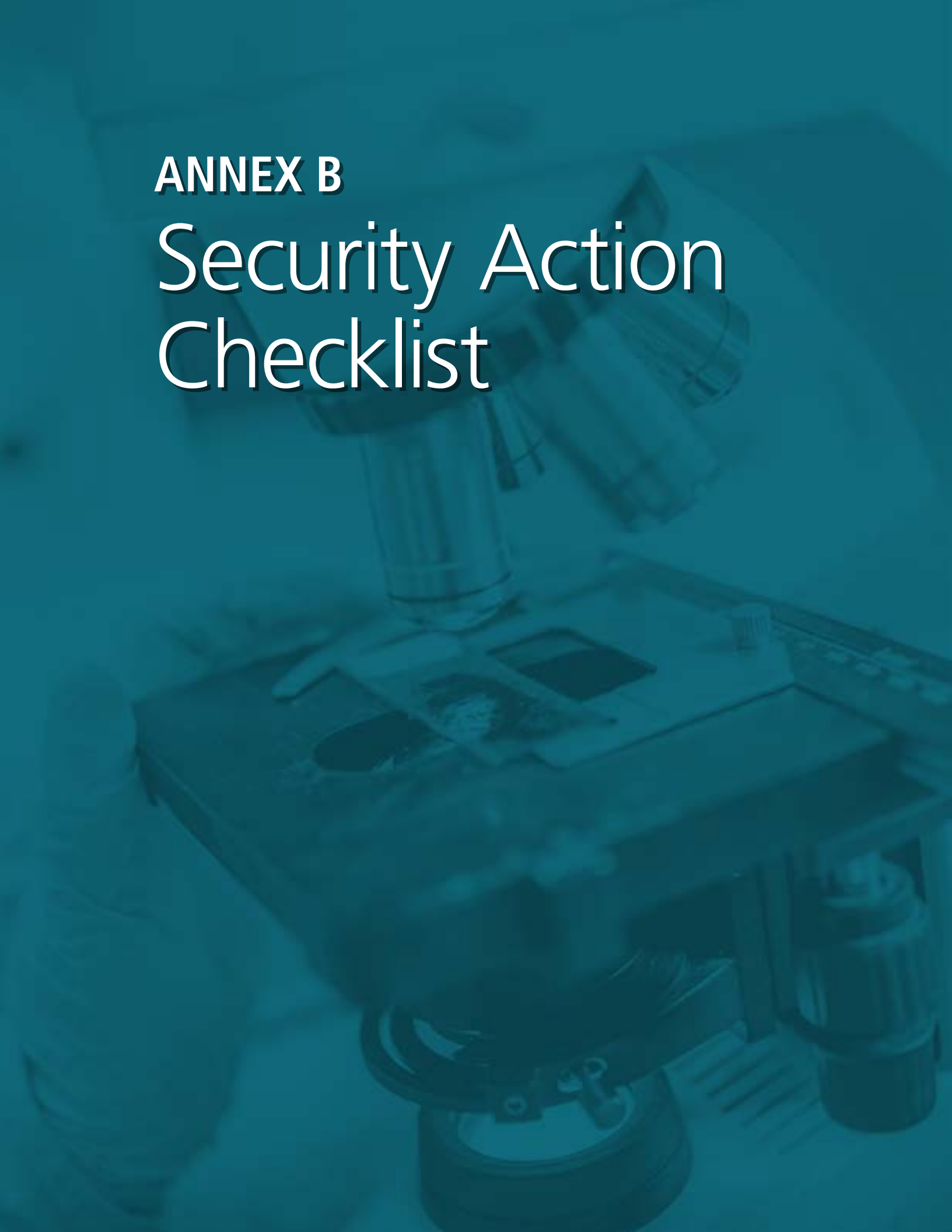
Scenario #2
Unintentional Insider risk

Company A has an ongoing working relationship with Company B. The nature of their relationship requires shared access to common networks. Within the confines of normal business activity, an employee at Company A receives an unsolicited email containing a malicious attachment. Perceiving the email as legitimate, the user opens the infected email attachment and unwittingly infects his computer. The malicious software installs various programs designed to compromise the user's computer and harvest available information such as user identification and network accessibility. The user having access to both company networks, soon spreads that infection to other connected networks, thus allowing the software and person responsible unauthorized access to any information that can be found on the associated networks. This can range from critical proprietary information from both companies such as financial records, personal data on company employees, as well as user names and passwords for company executives. Once access is gained to a system, an attacker is only limited by their own capabilities and the effectiveness of the system to defend and protect that system. It is not uncommon for this type of unauthorized presence to exist for weeks, months, and even years. The following 5 security actions should be noted in relation to this scenario:

- **Security Action #2 Develop Clear Security Policies and Procedures:** An internet usage policy of not reading or opening suspicious email attachments could have prevented this situation. Responsibility does not only fall to the individual, but to those charged with ensuring that adequate email protection systems are in place, enforced, and regularly updated.
- **Security Action #3 Reduce Risks from Partners and Third-Party Providers:** Company B should have considered that the attack surface to an organization enterprise network is dramatically increased with third party providers and partners having access to sensitive data and network processes. In this situation, risk assessments for both companies could have identified this dependency and associated risk to connected networks, and procedures, policies, and technologies could have been put in place to mitigate the risk.
- **Security Action # 3: Reduce Risks from Partners and Third-Party Providers:** Both companies could have drafted a formal agreement governing such areas as data ownership, confidentiality, intellectual property, network usage, and non-disclosure before allowing company A to have access to company B's network.
- **Security Action #5 Provide Training, Raise Awareness and Conduct Exercises:** Employees should be educated in good internet and email hygiene, and made aware of the potential dangers an organization

could face if compromised via these channels. Formal training for all employees in security awareness should be mandatory and enforced regularly through bulletins, newsletters, emails, and corporate social media channels.

- **Security Action # 6 Identify Critical Assets and Protect Them:** The critical asset in this case was the propriety information stored on Company B's systems. Had this information been properly identified and segmented and/or protected, it is possible that the intruder may not have been able to access the data. Each organization must determine what is mission critical and take the measures required to protect those assets from compromise.



ANNEX B

Security Action Checklist

Resilience to Insider Risk

8 Recommended Security Actions

Establish a Culture of Security

- ☐ Establish senior management engagement and accountability
- ☐ Identify a senior official responsible for managing insider risks
- ☐ Build a whole-of-organization commitment to security and emphasize leadership at all levels

Develop Clear Security Policies and Procedures

- ☐ Define clear expectations and outcomes
- ☐ Identify risk levels of positions in the organization
- ☐ Align employee access with position risk levels

Reduce Risks from Partners and Third Party Providers

- ☐ Understand key assets and systems
- ☐ Know your partners
- ☐ Know your risks

Implement a Personnel Screening Life-Cycle

- ☐ Conduct pre-employment screening
- ☐ Implement ongoing employee security screening
- ☐ Incorporate departure and internal movement procedures
- ☐ Establish transparent security policies

Provide Training, Raise Awareness and Conduct Exercises

- ☐ Provide regular training to decrease the risk of unintended security infractions
- ☐ Raise awareness of potential warning signs
- ☐ Foster a culture of vigilance and empower employees

Identify Critical Assets and Protect Them

- ☐ Identify and rank key assets and systems
- ☐ Secure key assets and systems
- ☐ Leverage signage and visible deterrents to access
- ☐ Apply the principle of least privilege
- ☐ Separate duties

Monitor, Respond to and Mitigate Unusual Behaviour

- ☐ Track remote access and monitor device endpoints
- ☐ Establish effective incident reporting, tracking, and response measures
- ☐ Raise Awareness of best practices regarding the use of social networking sites

Protect Your Data

- ☐ Establish and test business continuity plans and procedures
- ☐ Implement procedures to limit information exit points

Public Safety Canada | Sécurité publique Canada

Canada

Security Action #1:
Establish a Culture of Security

- ✓ Identify an organizational champion for managing insider risks with full accountability;
- ✓ Identify a senior executive accountable for the development of a company-wide security policy and program;
- ✓ Develop a governance structure, including an insider risk working group, to develop, deliver and manage an insider risk program;
- ✓ Establish an organizational "pledge" to recognize the importance of security in delivering a profitable and sustainable business;
- ✓ Design comprehensive physical and cyber network security policies and procedures encompassing all departments; and,
- ✓ Promote a culture of security at all levels by linking employee and management performance to security metrics.

Security Action #2:
Develop Clear Security Policies and Procedures

- ✓ Clearly define, post, and educate employees in corporate security policies;
- ✓ Conduct employee screening based on position requirements; and
- ✓ Assign appropriate risk levels of employees commensurate with the criticality and importance of the information, systems, and area that they access.

Security Action #3:
Reduce Risks from Partners and Third-Party Providers

- ✓ Conduct an organization-wide risk assessment identifying all key assets and critical systems; Identify all security concerns related to third-party access to its networks, data and systems;
- ✓ Independently verify the security posture of third party service providers, including background checks of employees with access to an organization's critical facilities or networks;
- ✓ Ensure comprehensive third-party security agreements, with assurance language included in the agreements, to reduce supply chain risk; and
- ✓ Build long-term trusted relationships with key service providers.

Security Action #4:
Implement a Personnel Screening Life-Cycle

- ✓ Conduct thorough pre-employment and continuous screening of all personnel using all resources available, including social media;
- ✓ Update security access and clearances for employees based on the roles and responsibilities of their position;
- ✓ Amend access privileges for employees that have moved to new positions within the organization; and
- ✓ Promote a transparent security program to all employees to manage physical and network security expectations.

Security Action #5:
Provide Training, Raise Awareness and Conduct Exercises

- ✓ Develop a security training program for all employees;
- ✓ Raise awareness of indicators of potential security concerns;
- ✓ Provide access to employee assistance programs to help prevent employees from becoming at risk of compromise;
- ✓ Develop and promote a culture of security vigilance by encouraging employees to say something if they see something;
- ✓ Conduct periodic exercises to test the security posture within an organization.

Security Action #6:
Identify Critical Assets and Protect Them

- ✓ Conduct an organization-wide assessment to identify and rank critical assets and systems and security measures to protect them;
- ✓ Monitor system usage by authorized and unauthorized users as well as physical premises access;
- ✓ Outline how/what data is being sent to 3rd parties and the sensitivity of the data, as protect data appropriately;
- ✓ Consider the principle of least privilege and separation of duties for critical systems and data; and
- ✓ Leverage visible deterrents to decrease the likelihood of unintended access to facilities, networks and systems.

Security Action #7:
Monitor, Respond to and Mitigate Unusual Behaviour

- ✓ Establish a means of monitoring physical and network access from all endpoints and remote devices;
- ✓ Develop a culture that enhances employee awareness of security and reporting suspicious activity or abnormal behaviour;
- ✓ Raise awareness of the potential risks associated with social media sites;
- ✓ Limit remote access to non-critical assets and systems where possible;
- ✓ Establish protocols to report, track and respond to unusual incidents; and
- ✓ Consider engaging the security and intelligence community, including the RCMP or CSIS.

Security Action #8:
Protect Your Data

- ✓ Backup and protect all organizational data and essential systems on a regular basis;
- ✓ Develop policies for downloading large amounts of data or sensitive files;
- ✓ Consolidate access points to the internet;
- ✓ Implement segregated systems to prevent data loss; and
- ✓ Limit or restrict portable storage devices.

Annex C: Bibliography

Bowen, P., Hash, J., & Wilson, M. (2006). Information Security: A Guide for Managers. Gaithersburg: National Institute of Standards and Technology.

Caralli, R., Allen, J. H., White, D. W., Young, L. R., Mehravari, N., & Curtis, P. D. (2016). CERT Resilience Management Model, Version 1.2. Pittsburgh: Carnegie Mellon University.

CERT Inside Threat Center. (2016, December). Common Sense Guide to Mitigating Insider Threats. (5th Ed.). Pittsburgh, PA, USA. Retrieved from https://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_484758.pdf

Government of Canada. (2009). National Action Plan for Critical Infrastructure. Ottawa: Her Majesty in Right of Canada.

Joint Task Force Transformation Initiative. (2013). Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53 (Revision 4). Gaithersburg, MD, USA: National Institute of Standards and Technology.

Nieles, M., Dempsey, K., & Yan Pillitteri, V. (2017). An Introduction to Information Security. Gaithersburg: National Instute of Standards and Technology.

Wilson, M., & Hash, J. (2003). Building an Information Technology Security Awareness and Training Program. Gaithersberg: National Institute of Standards and Technology.