OCI
Where Next Happens

Ontario

ONTARIO CENTRE OF INNOVATION DIGITALIZATION COMPETENCE CENTRE

Cybersecurity Workbook

Workbook prepared by WHITE TUQUE

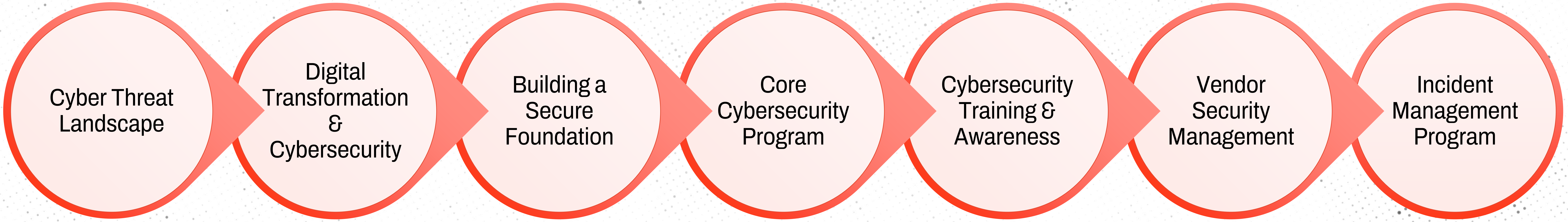
Table of Contents

Introduction

For small and medium enterprises, the need to safeguard sensitive data, protect against cyber threats, and ensure operational continuity is paramount. This workbook is your introductory guide to understanding, implementing, and strengthening your organization's cybersecurity defenses.

Workbook Overview

This resource will walk you through the essential principles, best practices, and strategies to safeguard your digital assets:



Cyber Threat Landscape

- The Data Behind Cyber Incidents
- Current Threat Landscape & Evolving Threats

Digital Transformation & Cybersecurity

- Significance of Cybersecurity in Digital Transformation
- How can businesses prioritize cybersecurity?

Building a Secure Foundation

- Cybersecurity Governance
- Data Classification and Handling
- Understanding Standards and Certifications

Core Cybersecurity Program

- Where do my security controls stand?
- Common Cybersecurity Controls
- Focused Cybersecurity Areas

Cybersecurity Training & Awareness

- Overview of organization change management
- Employee Training Programs
- Promoting Security Awareness

Vendor Security Management

- Assess Vendor Security Practices
- How to Evaluate Vendors
- Identifying Green Flags and Red Flags

Incident Management Program

- Preparing the Organization for an Incident
- Incident Response Plan & Reporting
- Building an Effective Improvement Process

Supporting Materials

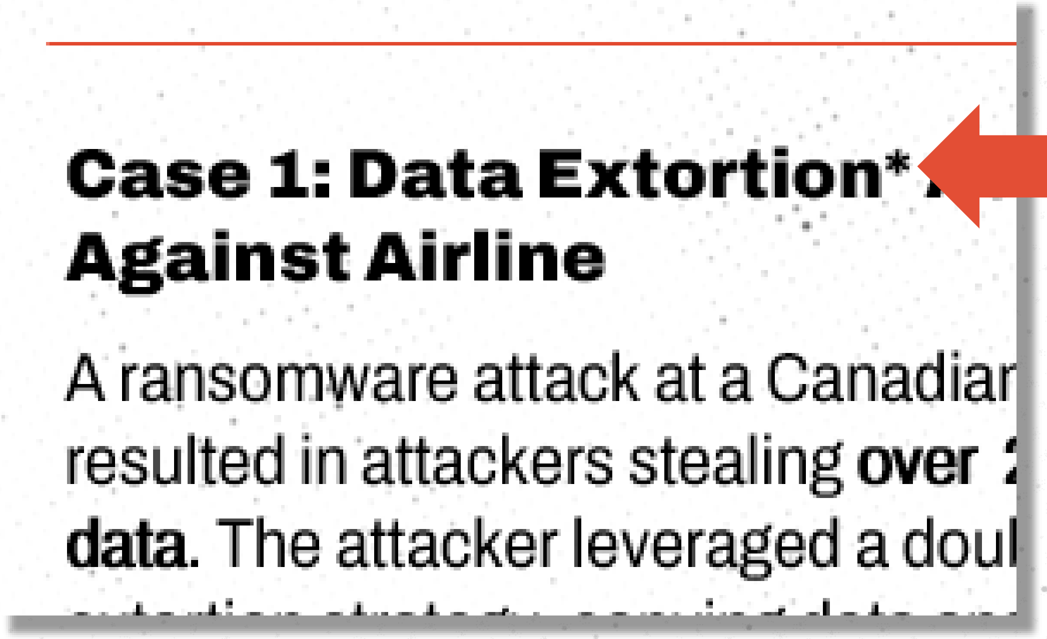
Supplemental Materials

In addition to this workbook, there is a supplemental package with questionnaires, templates, and guides. You'll find the "gold seal" throughout the workbook to indicate where there is supplemental material available for you to use.

- Risk Register Template
- Cyber Security Framework
- Self-Assessment Checklist
- Vendor Questionnaire Template
- IR Plan Template
- IR Contact Sheet
- Lessons Learned Template

Glossary

We know that cybersecurity uses a lot of jargon; we've provided some helpful definitions in the glossary, and highlighted these terms with an asterisk (*):



Case 1: Data Extortion* Against Airline

A ransomware attack at a Canadiar resulted in attackers stealing **over 2** **data**. The attacker leveraged a doul

Note the * after Data Extortion shown in this example. Clicking on the term "Data Extortion" will take you to a definition in the glossary.

Cyber Threat Landscape

Small and medium enterprises face many of the same threats as large enterprises, it’s just not as well publicized. Before going further into how to protect your business, we’re providing a view into the threats you’re facing today, even if you don’t know it.

The Data Behind Cyber Incidents

Fraud and scams are almost certainly the most common form of cybercrime that Canadian organizations will experience over the next two years as threat actors* attempt to steal personal, financial, and corporate information via the Internet.

Most Targeted Industries in Canada

Services	20%
Manufacturing	16%
Public Sector	10%
Construction	8%
Information &Technology	8%
Health care	8%
Retail	8%
Finance	6%
Energy and Utilities	6%
Transportation	4%

Recent surveys and analysis of Canadian small and medium enterprises provide a unique insight into why cybersecurity is critical:

61% of all cyberattacks are aimed at small businesses

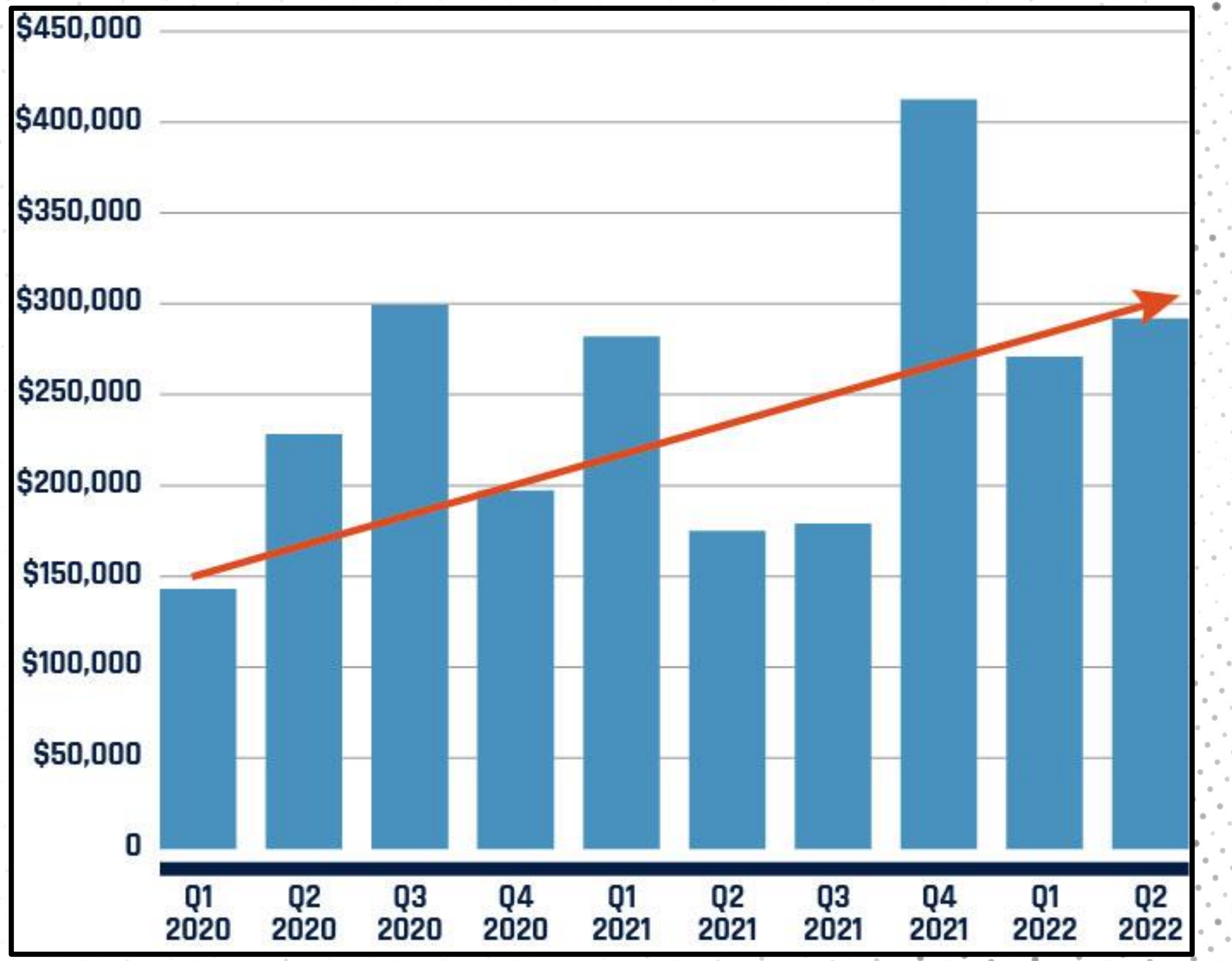
57% of owners said they had no form of cybersecurity training

only 51% said their firm uses two-factor or multifactor authentication to protect logins

95% of cybersecurity incidents at small and medium businesses cost between $826 and $653,587

34% of businesses that were hit with malware could not get back to their data for a week or more

Average Ransomware* Payments Since 2020



According to the Canadian Anti-Fraud Centre, there have been over 150,000 reports of fraud in Canada with over $600 million stolen since January 2021.

The Data Behind Cyber Incidents

Case 1: Data Extortion* Attack Against Airline

A ransomware attack at a Canadian airline resulted in attackers stealing **over 210GB of data**. The attacker leveraged a double extortion strategy, copying data and threatening to sell or give it away as well as encrypting as many servers as it could. This airline faced financial losses due to loss of data, operations and reputation damage.

What data does your company hold that would be damaging if stolen?

What actions would you take if someone threatened to expose your sensitive information?

Case 2: Microsoft's Data Breach*

Microsoft has recently been a victim of a large data breach which led to potential theft of nearly **30 million customer accounts, including emails, and passwords.** The group specializing in distributed denial-of-service (DDoS)* attacks, can lead to service disruptions and outages. With millions of customers leveraging Microsoft account services across Canada, it led to users being not able to access their accounts and disruptions across organizations.

Was your business impacted by this event?

How much does your business rely on external technology services for core functionality like email and communications?

Do you have a plan for how you would operate in the event of a major disruption?

Case 3: Retailer's Cyber Attack

A ransomware attack compromised the data of current and former employees at a major Canadian retail chain. Customers were unable to make purchases as the retailer had to halt website and application operations due to the attack. Website services were not available for nearly two weeks after the incident and stores were forced to work cash only purchases. The retailer **lost $50M in that year, in large part due to this cyberattack**.

How would your company be impacted if all IT systems for order processing were offline for two weeks?

What if it impacted inventory management or other critical business operations?

Current Threat Landscape & Evolving Threats

Types of cyber threats experienced by Canadian businesses in the past year:

Ransomware

Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files until a ransom is paid.

Social Engineering Attacks

Social engineering is the tactic of manipulating, influencing, or deceiving a victim in order to gain control over a computer system, or to steal personal or financial data.

Phishing

Phishing is the practice of tricking Internet users (using deceptive email messages or websites) into revealing personal or confidential information which can then be used illicitly.

Password Attacks

A password attack is an unauthorized attempt to gain access to computer system, network or account by trying various passwords through brute force through often automated methods.

State-sponsored threat actors

State sponsored attacks are a form of cyber warfare in which a government or state sponsors or carries out cyber attacks against other governments, businesses, organizations, or individuals.

Supply chain attacks

Supply chain attack refers to when someone targets your outside provider or partner that has access to your data and systems to infiltrate your digital infrastructure.

Key Takeaways: Cyber Threat Landscape

Over 35% of the cyber attacks were targeted towards the Manufacturing and Services sectors

Small and medium enterprises continue to lose significantly due to lack of cyber security capabilities

Case studies illustrate how attacks across industries within Canada are paralyzing businesses, stopping operations and causing millions in losses

Personal data continues to be the most prominent asset cyber attackers are going after

Attacks are increasingly targeting vulnerable areas such as emerging technologies and supply chains

Risk Register Template

Digital Transformation & Cybersecurity

Digital transformation is a major strategy for small and medium enterprises, and while it can be a major boost to business it also has potential risks.
This section discusses how security is part of digital transformation, both as a consideration for your transformed services, and as a service to be transformed.

Significance of Cybersecurity in Digital Transformation

When we look at cybersecurity the objectives of Digital Transformation, there are many ways that cybersecurity goals can be aligned to support and enhance the digital transformation journey. (Page 1 of 2)

Cybersecurity Goal		Digital Transformation Goal
Protection and Privacy	Cybersecurity is critical in ensuring that the customer feels that their data is secure and private throughout the digital journey.	**Improved Customer Experience**
Business Continuity	Effective cybersecurity measures help maintain efficiency by protecting digital assets from cyberattacks and ensuring that services remain available in the face of disruptions.	**Higher Process Efficiency**
Scaling and Flexibility	Cybersecurity designed to scale with digital transformation initiatives be flexible enough to adapt to evolving technology and threat landscapes.	**Increased Agility**
Risk Management	Digital transformation brings new risks, and cybersecurity is integral to identifying, assessing, and mitigating these risks. It allows organizations to make informed decisions about technology adoption.	**Business Process Improvement**

... continues on next page

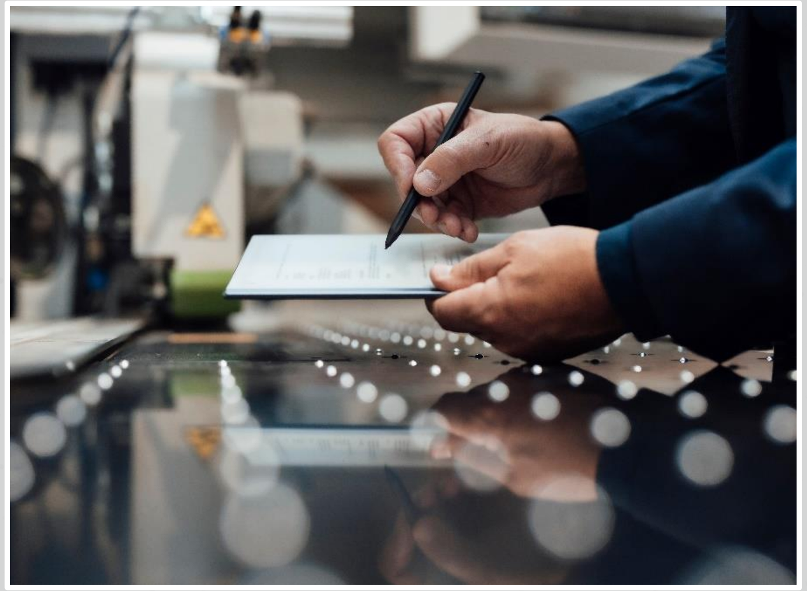
Significance of Cybersecurity in Digital Transformation

When we look at cybersecurity the objectives of Digital Transformation, there are many ways that cybersecurity goals can be aligned to support and enhance the digital transformation journey. (Page 2 of 2)

Cybersecurity Goal			Digital Transformation Goal
Return on Investment	Investing in cybersecurity is an investment in protecting digital assets. A strong cybersecurity posture can ultimately lead to savings by preventing costly incidents.	→	**Cost Management**
Security by Design	Implementing a "security by design" approach in digital transformation initiatives ensures that security is an integral part of the development process, and a way to differentiate you from your competition.	→	**Gain a Competitive Advantage**
Training and Awareness	Security training ensures employees are prepared to deal with any social engineering or phishing attempts. This allows employees to improve their overall performance in delivering their duties.	→	**Improve Employee Performance**
Regulatory Compliance	Industries have specific regulations and compliance requirements related to data protection and cybersecurity. Ensuring compliance is a fundamental aspect of digital transformation initiatives.	→	**Governance & Compliance**

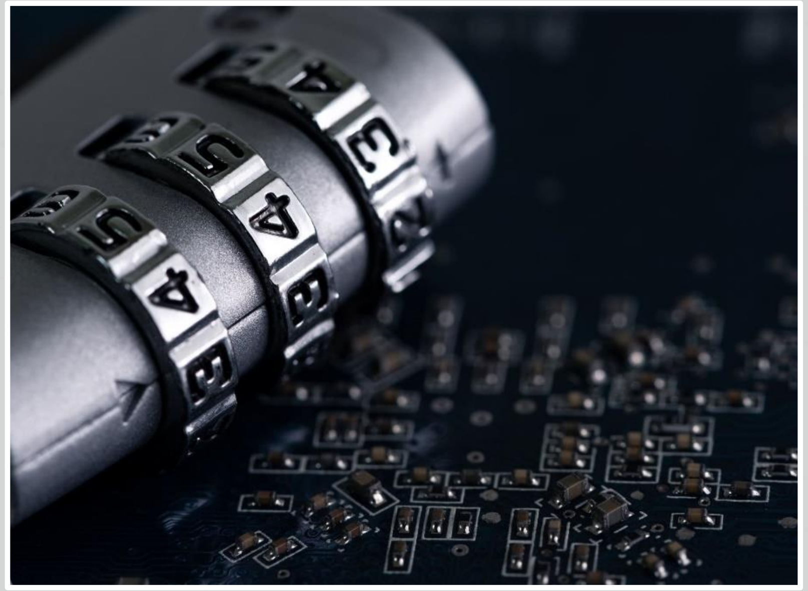
Prioritizing Your Cybersecurity Work

Prioritizing cybersecurity is an ongoing process. To get started, small and medium enterprises should allocate resources, including time and budget, to building a strong security posture starting with these five areas. While these five provide the most immediate reduction of risk for your organization, we'll go into more detail on these and additional controls that will round out your program in the coming sections.



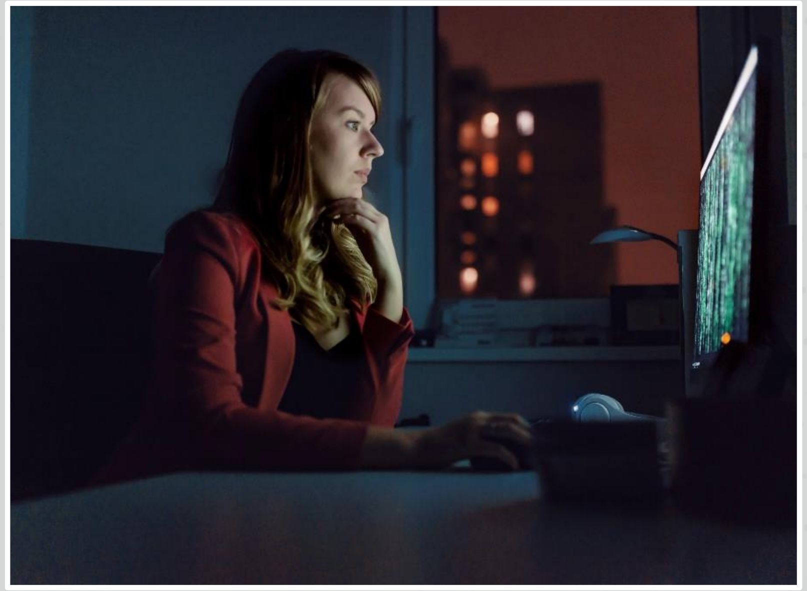
Cybersecurity Policy and Planning

Invest in Security Awareness and Training



Optimize Device-Level Security

Control Access to Systems and Networks



Incident Readiness & Cyber Insurance

Additionally, staying informed about emerging threats and adapting security measures accordingly is crucial to protecting your business against evolving risks. More on that in the section on building an Incident Management Program.

Key Takeaways: Digital Transformation & Cybersecurity

Cybersecurity and digital transformation are interlinked and can be used to drive each other forward.

Cybersecurity supports an organization’s digital transformation goals, such as customer experience, process efficiency, increased compliance, cost management and competitive advantage.

There are five key areas that small and medium enterprises can undertake as a priority in building and enhancing their cybersecurity posture.

Building a Secure Foundation

Building a strong cybersecurity foundation within a small or medium enterprise is essential for creating a structured approach to managing security risks. This section provides insights on how to build a security by design mindset.

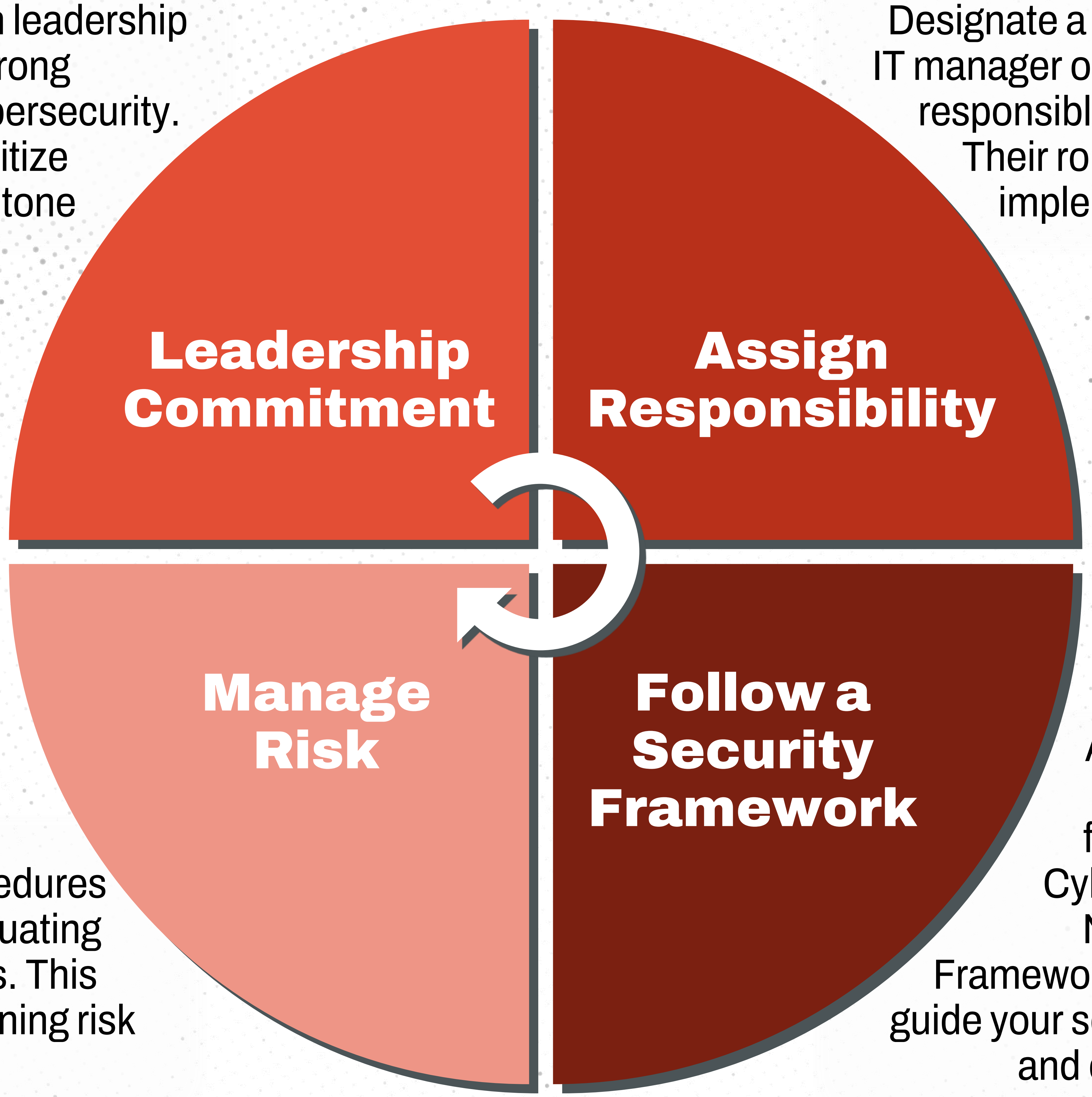
Cybersecurity Governance

Developing a security-first mindset in a small or medium enterprise is crucial for protecting sensitive data and mitigating cybersecurity risks.

By implementing these steps, small and medium enterprises can build a strong cybersecurity governance structure.

This organized approach provides the framework for addressing security issues in a systematic and effective manner.

Risk Register Template



Leadership Commitment

Start at the top with leadership demonstrating a strong commitment to cybersecurity. When leaders prioritize security, it sets the tone for the entire organization.

Assign Responsibility

Designate a senior executive or IT manager or another individual responsible for cybersecurity. Their role is to oversee and implement cybersecurity measures.

Manage Risk

Implement risk management procedures for identifying, evaluating and mitigating risks. This should include defining risk thresholds.

Follow a Security Framework

Adopt a recognized cybersecurity framework, such as Cybersecure Canada, NIST Cybersecurity Framework or ISO 27001, to guide your security governance and compliance efforts.

Understanding Standards and Certifications

Organizations should align to a cybersecurity standard to ensure comprehensive and consistent security measures. There are several, each with its own focus and strengths. Here are some of the most used cybersecurity standards and certifications with their key differences.

CAN/CIOSC 104

- **Focus:** Cybersecurity for Canadian SMEs, sometimes referred to as Cybersecure Canada
- **Purpose:** For small and medium organizations seeking to start their security program.
- **Key Features:** Invest in security strategically to maximize the benefit at lower cost.
- **When to Undertake:** Canadian SMEs looking to build their first cybersecurity program.
- **More Information:** https://dgc-cgn.org/standards/find-a-standard/standards-in-cybersecurity/cybersecurity-smes/

NIST Cybersecurity Framework

- **Focus:** Cybersecurity risk management.
- **Purpose:** Help organizations manage and reduce cybersecurity risk.
- **Key Features:** Intuitive breakdown of controls in 5 categories: Identify, Protect, Detect, Respond, and Recover.
- **When to Undertake:** Especially applicable for companies with US clients, and for mature organizations expanding their cybersecurity capabilities.
- **More Information:** https://www.nist.gov/cyberframework

ISO 27001

- **Focus:** Information Security Management System (ISMS).
- **Purpose:** Establish and maintain an ISMS that helps organizations manage and protect their information assets.
- **Key Features:** Risk assessment, controls, and continuous improvement.
- **When to Undertake:** Internationally recognized and broadly applicability across industries.
- **More Information:** https://www.iso.org/standard/ 27001

SOC 2 / SSAE 18

- **Focus:** Service organization controls (SOC).
- **Purpose:** Provides assurance to customers regarding trust services criteria, including security.
- **Key Features:** The report provides a description of the controls that protect the organization and the auditor's statement whether those descriptions are accurate.
- **When to Undertake:** Businesses who host a system and need to validate their security controls to customers.
- **More Information:** https://en.wikipedia.org/wiki/System_and_Organization_Controls

To Certify or Not To Certify?

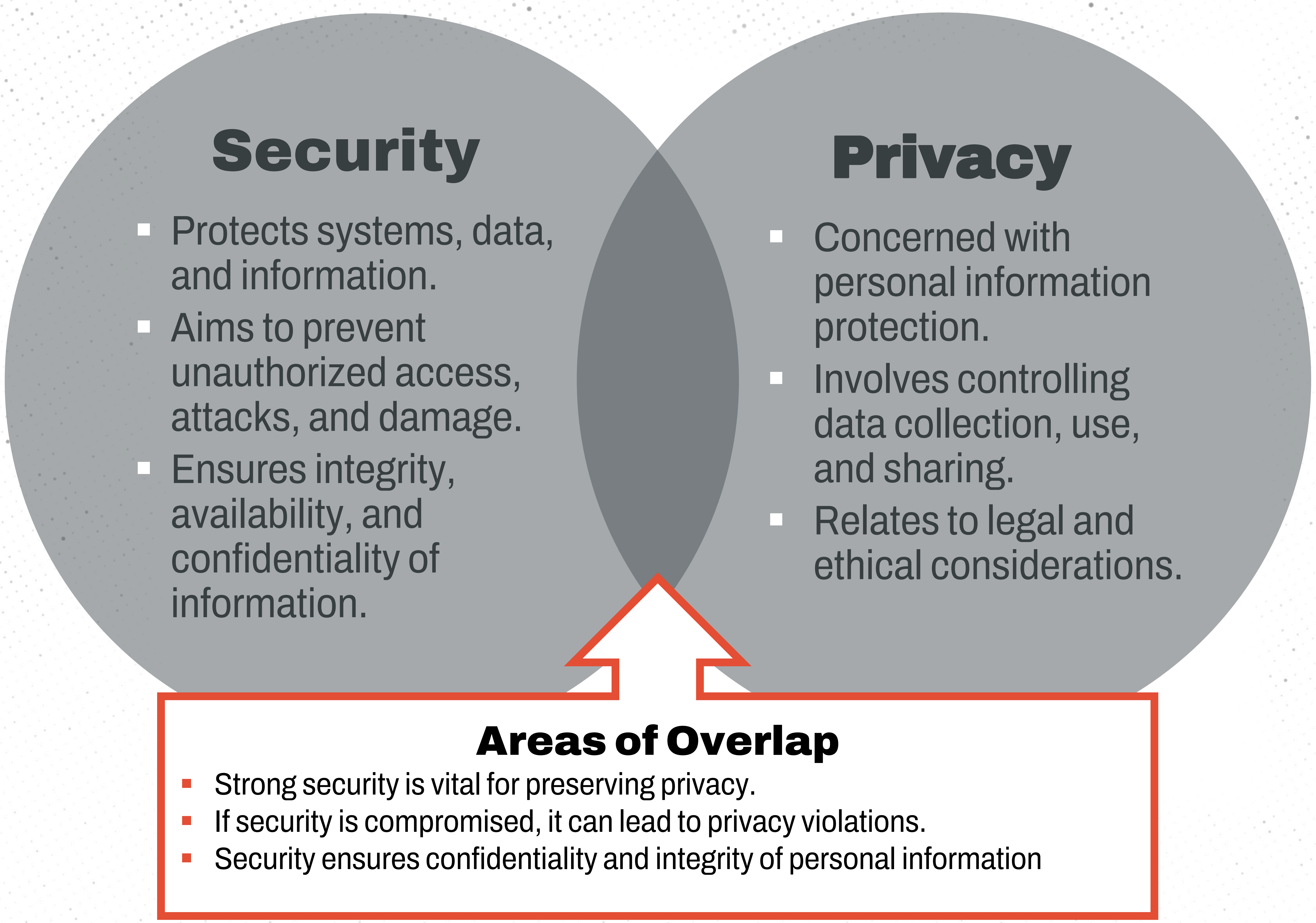
It mainly comes down to your customers – if they are looking for assurance that you have a strong program and / or your product is secure, audited certifications will save you a lot of hassle. They are an investment, so make sure to talk to an expert to understand the cost / benefit.

Security & Privacy – Similar but not the same

Security and Privacy are often talked about together, but they are distinct practices with sometimes conflicting goals.

Take, for example, a company that monitors employee behaviour for malicious activities – if you don't provide appropriate notification, it can be a breach of privacy.

Similarly, many privacy breaches occur that are not failures of cybersecurity – for example, a clinician accidentally sends a file with patient information to the wrong person.



Security

- Protects systems, data, and information.
- Aims to prevent unauthorized access, attacks, and damage.
- Ensures integrity, availability, and confidentiality of information.

Privacy

- Concerned with personal information protection.
- Involves controlling data collection, use, and sharing.
- Relates to legal and ethical considerations.

Areas of Overlap

- Strong security is vital for preserving privacy.
- If security is compromised, it can lead to privacy violations.
- Security ensures confidentiality and integrity of personal information

Learn More About Privacy Laws

Personal Information Protection and Electronic Documents Act (PIPEDA)

The Canadian standard that covers many kinds of personal information, including health information

- https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

Health Insurance Portability and Accountability Act (HIPAA)

The US standard for handling Protected Health Information (PHI):

- https://www.hhs.gov/hipaa/index.html

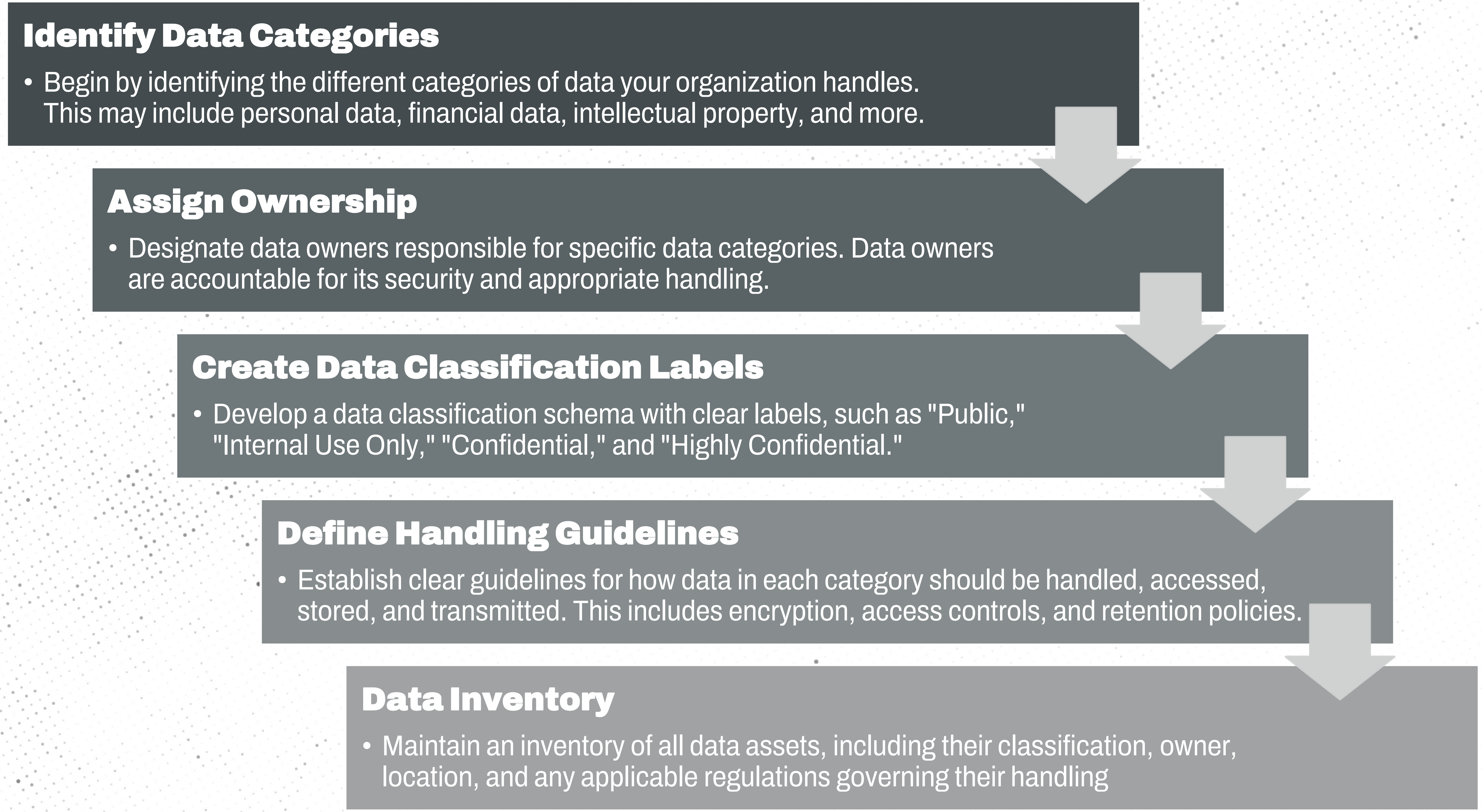
General Data Protection Regulation (GDPR)

From the EU, one of the strictest privacy regulations in the world

- https://gdpr-info.eu/

Data Classification & Handling

Implementing effective data classification and handling practices is crucial for protecting sensitive information, maintaining customer trust, and ensuring regulatory compliance for SMEs. It also helps in preventing data breaches and security incidents. There are solutions available in many of the common file-storage platforms to make this easier than ever before.



Identify Data Categories

- Begin by identifying the different categories of data your organization handles. This may include personal data, financial data, intellectual property, and more.

Assign Ownership

- Designate data owners responsible for specific data categories. Data owners are accountable for its security and appropriate handling.

Create Data Classification Labels

- Develop a data classification schema with clear labels, such as "Public," "Internal Use Only," "Confidential," and "Highly Confidential."

Define Handling Guidelines

- Establish clear guidelines for how data in each category should be handled, accessed, stored, and transmitted. This includes encryption, access controls, and retention policies.

Data Inventory

- Maintain an inventory of all data assets, including their classification, owner, location, and any applicable regulations governing their handling

Protecting Your Data

1. Data stored in shared drives, files and folders should be encrypted*
2. Store physical documents in a locked cabinet and secure the keys
3. Ensure all data is deleted or destroyed before discarding storage devices (USB, hard drive, etc.)

Key Takeaways: Building a Secure Foundation

Risk Register Template

4 key areas that can help businesses shape their cyber security governance – leadership commitment, assign responsibility, follow a security framework and manage risk

There are various security standards that are used to cyber maturity level and the ability to protect data. Organizations can choose to undertake one or more of these certifications and standards based on the industry they align to and the regulations they must abide by.

Security and privacy have some overlapping objectives, but they are distinct practices with different goals.

Data classification & handling requires businesses to map all the data flowing through organization and establish parameters to secure the data

Encrypting the data on devices and locking the cabinets for physical files are examples of ways to secure data

Core Cybersecurity Program

A core cybersecurity program is crucial for organizations to protect their sensitive data and mitigates cyber threats. Taking stock of your controls will give you a much better understanding of where you are taking risks that can impact your business.

Establishing Common Cyber Controls

Cyber Security Framework

Baseline cyber controls* that organizations should build into their infrastructure, to ensure strong protection against threats. It also signifies the presence of a mature cyber posture with this organization. We've selected some major ones common across all frameworks to highlight here, with a full suite of the CAN/CIOSC 104:2021 controls available in the supplementary materials.

Incident Response Plan

What is it? The incident response plan establishes a process of identifying, managing, and resolving security incidents in an organization.

Why? It helps reduce the impact of a cyber incident and ensures business continuity.

Example components:

- Incident response plan document
- Security incident reports
- Post-incident reviews
- Cyber insurance

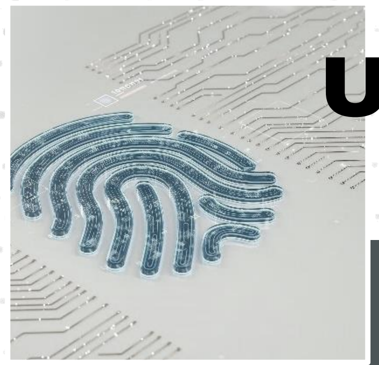
Patch Management

What is it? Patch Management is the process of planning, testing, and deploying software updates or "patches" to fix vulnerabilities*, bugs, and security issues in operating systems, applications, and software.

Why? It helps protect against cyber threats, as many attacks exploit known vulnerabilities that patches can address.

Example components:

- Installing security updates for your operating system (i.e. software releases for Windows and Mac).
- Updating web browsers, like Google Chrome, Mozilla Firefox, or Microsoft Edge.



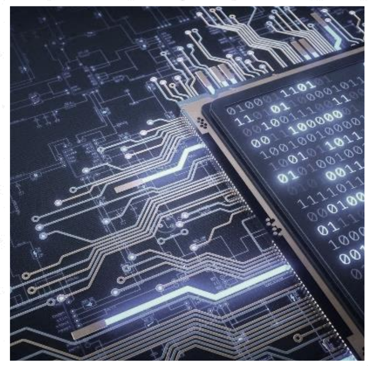
User Authentication & Access Control

What is it? Access management is the process of controlling and managing user access to an organization's systems, data, and resources.

Why? Access management enhances system security, preserves privacy and helps in preventing insider threats.

Example components:

- User authentication (e.g., username and password)
- Role-based access control (RBAC)
- Multi-factor authentication (MFA)



Endpoint Protection

What is it? Endpoint* protection refers to securing individual devices, such as computers and smartphones.

Why? Endpoint protection protects against threats such as malware and secures sensitive data.

Example components:

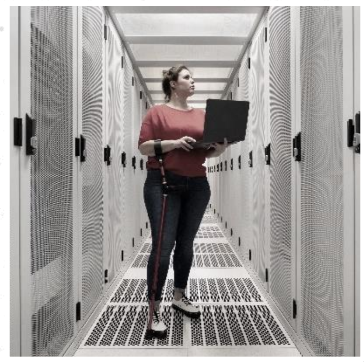
- Antivirus software
- Endpoint detection and response (EDR) solutions
- Mobile device management (MDM)

... continues on next page

Establishing Common Cyber Controls

Cyber Security Framework

Baseline cyber controls* (continued from previous page).



Backup and Encryption of Data

Backup: what is it? Backup involves making copies of data to safeguard against data loss due to various factors.

Why? Backup protects against data loss from hardware failures, accidents, and cyber threats.

Example components:

- On-prem, hybrid or cloud-based copies of your data.

Encryption: what is it? Encryption* is the process of converting data into a scrambled format so it can only be read by someone with the decoding key.

Why? Encryption secures data during storage and transmission, enhancing data confidentiality.

Example components:

- Employing tools like BitLocker (for Windows) or FileVault (for Mac) to encrypt storage drives.

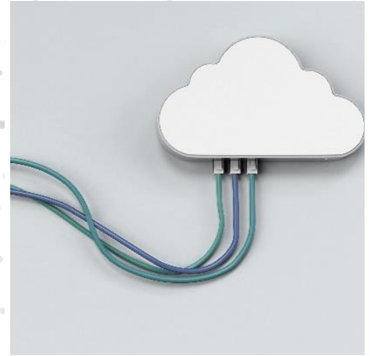
Network Security

What is it? Network security involves layering your external and internal communication channels with safeguards to protect against threats.

Why? Ensures that sensitive information remains secure during transmission, preventing unauthorized access. Ensures the information's authenticity.

Example components:

- Encryption* for transmitting emails and messages
- Virtual private networks (VPNs)
- SSL certificates for websites (HTTPS)



Cloud Security

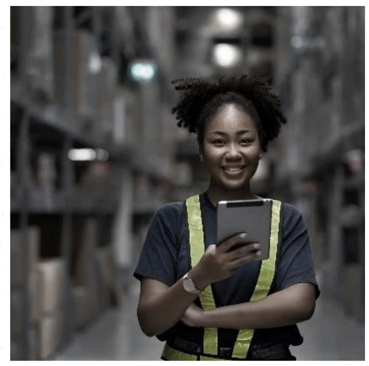
What is it? Cloud Security refers to the measures and practices designed to protect data, applications, and resources in cloud computing environments from threats and vulnerabilities*.

Why? Safeguards sensitive data from unauthorized access and data breaches in cloud environments.

Example components:

- Implementing strong access controls
- Encrypting data at rest and in transit
- Using cloud service provider security tools and services.

Go deeper: See the Cloud Security reference in the appendix.



Outsourced IT Services

What is it? Vendor security management involves assessing and ensuring the security of third-party vendors and service providers.

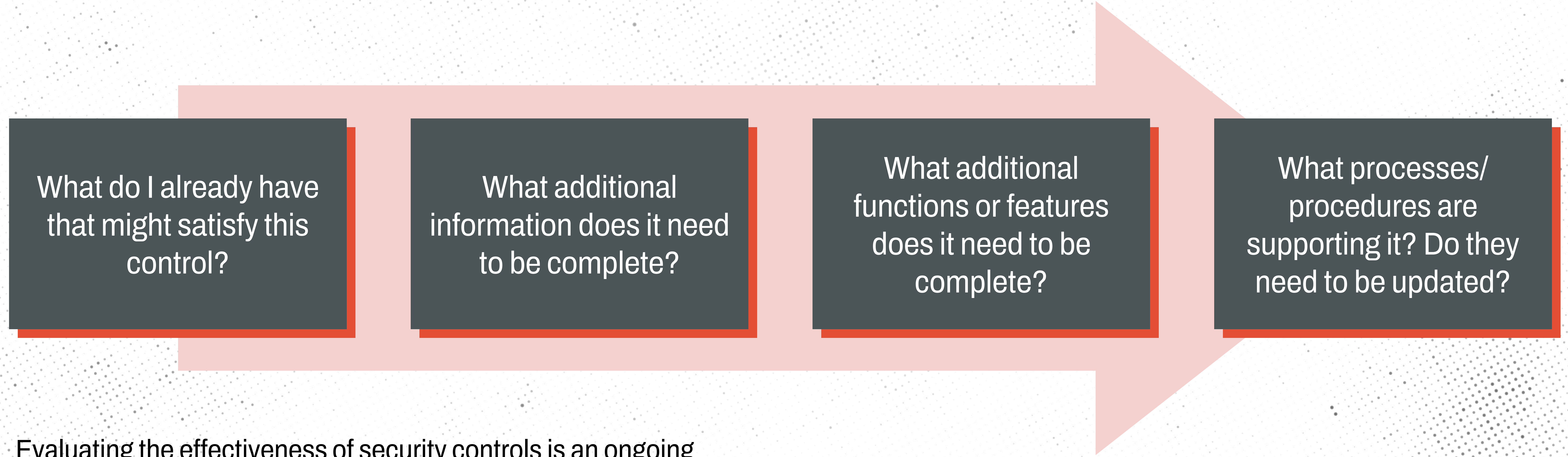
Why? Reduces the risk of data breaches and cyber incidents caused by vendor vulnerabilities. Further, safeguards sensitive data shared with vendors.

Example components:

- Vendor risk assessments
- Due diligence on vendor security practices
- Setting service level agreements (SLAs)

Where do my security controls stand?

For any organization to understand how to improve its security posture, it is critical that they first evaluate their controls by answering the following questions:



What do I already have that might satisfy this control?

What additional information does it need to be complete?

What additional functions or features does it need to be complete?

What processes/ procedures are supporting it? Do they need to be updated?

Evaluating the effectiveness of security controls is an ongoing process, and part of a security program's continuous improvement efforts.

Regular reviews and adjustments are essential to ensure that controls remain effective in an ever-evolving threat landscape.

Self-Assessment Checklist

Key Takeaways: Core Cybersecurity Program

Common controls found in security frameworks are: Incident Response Plan, Patch Management, User Authentication & Access Control, Endpoint Protection, Backup and Encryption of Data, Network Security, Cloud Security and Outsourced IT Services.

Each control family provides a different aspect of security coverage, so that together they create layers of security to protect your data and systems.

It is important that organizations pause and question themselves on where their security controls stand and how they can improve them.

Cyber Security Framework

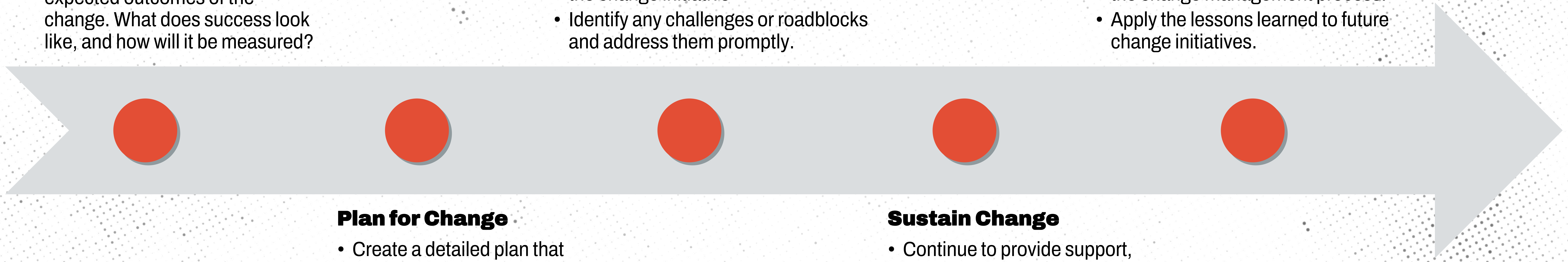
Self-Assessment Checklist

Cybersecurity Training & Awareness

Cybersecurity training focuses on educating employees and stakeholders about various aspects of cybersecurity, including best practices, security policies, and the identification of potential threats.

Overview of Organization Change Management

Organizational change management is a structured approach to transitioning an organization and its people through significant changes. Here's a 5-step process for effective change management:



Prepare for Change

- Identify the reasons and objectives behind the change. What problems or opportunities are driving this change?
- Clearly define the goals and expected outcomes of the change. What does success look like, and how will it be measured?

Plan for Change

- Create a detailed plan that outlines the strategies, activities, and timelines for implementing the change.
- Determine who will be impacted by the change and how
- Develop strategies for mitigating risks

Implement Change

- Put the change management plan into action. This includes communicating the change and providing training
- Continuously monitor the progress of the change initiative
- Identify any challenges or roadblocks and address them promptly.

Sustain Change

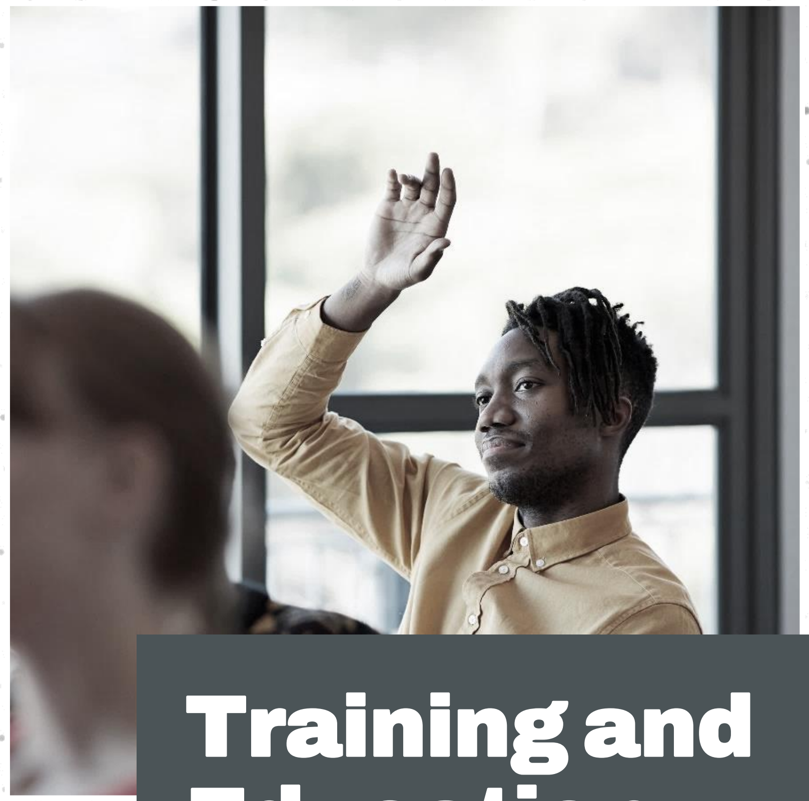
- Continue to provide support, training, and resources
- Gather feedback from employees to assess the impact of the change.

Evaluate and Learn

- Evaluate the outcomes of the change against the defined objectives.
- Identify and document what worked well and what could be improved in the change management process.
- Apply the lessons learned to future change initiatives.

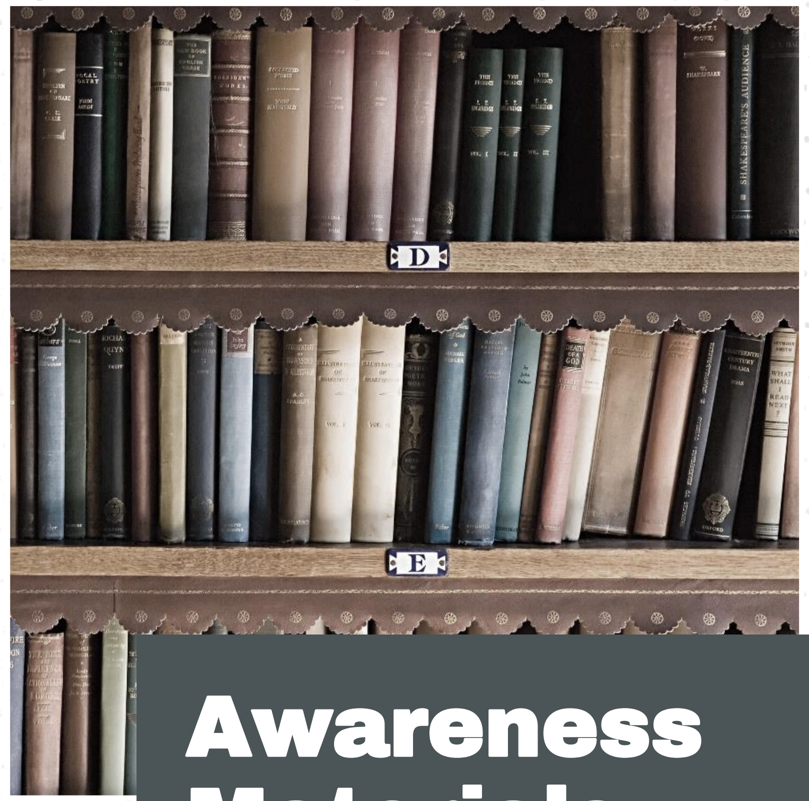
Promoting Security Awareness

The goal is a Cultural Shift: cybersecurity awareness is not a one-time event but an ongoing process that leads to a cultural shift within the organization, where security is a shared responsibility.



Training and Education

- Customize training to address specific roles and responsibilities within the organization

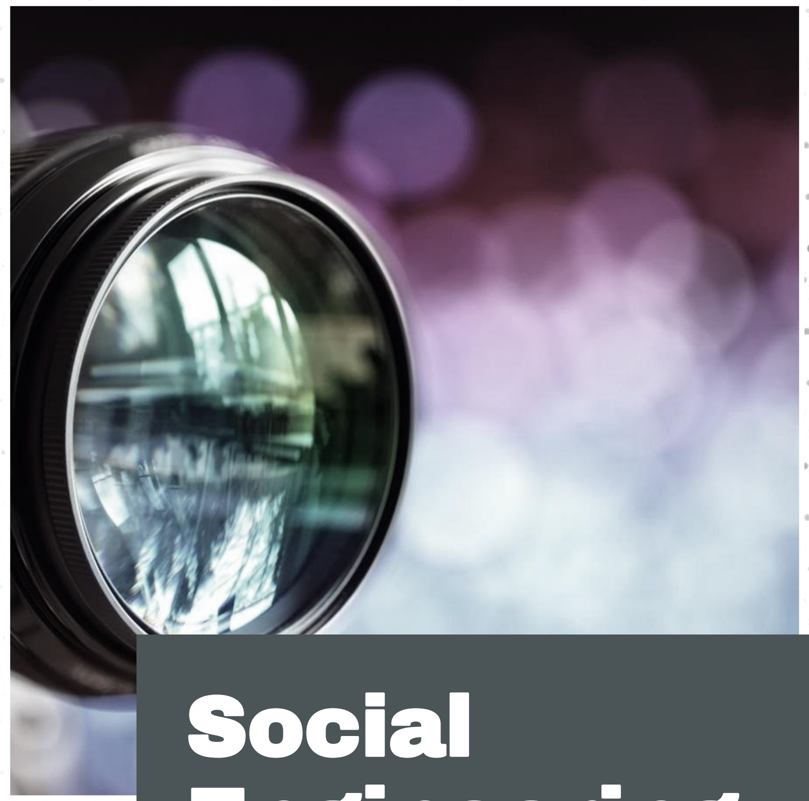


Awareness Materials

- Create and distribute awareness materials, including posters, infographics, and guides, that highlight key security practices and threats.

Security Champions

- Appoint security champions or advocates within the organization who can help disseminate information and encourage best practices.



Social Engineering Awareness

- Educate employees about social engineering tactics, such as pretexting, baiting, and tailgating, and how to spot and respond to them.

Employee Training Programs

Employee cyber security training programs can be customized to meet the organization’s industry and their needs. The frequency can be established by the organization, at least on an annual basis, but even better is to break it into chunks delivered throughout the year. Security is an ongoing process of education!

Topics to be covered:

- Recognizing phishing emails and social engineering attempts.
- Creating strong passwords and using multi-factor authentication.
- Secure web browsing and email practices.
- Safe use of company devices and networks.
- Understanding the organization's security policies and procedures.
- Incident reporting and response.
- Compliance with data protection and privacy regulations.

Full Online courses

Training can be delivered through many modes and it should be selected to suit the organization's specific needs.

In-person workshops

E-learning modules

Hybrid In-person + Online

Key Takeaways: Cybersecurity Training & Awareness

As organizations adopt new technologies, cybersecurity training and awareness programs become essential to educate employees and stakeholders about potential risks and best practices.

Follow an organization change management process to introduce new security controls and establish a security culture.

Raise awareness about the risks of cyber attacks, how they are leveraged and how they can harm the organization and its data.

Train employees in cybersecurity best practices. Teach them to recognize phishing emails, practice good password management, and understand the importance of security hygiene.

Encourage employees to report any suspicious activity or security incidents promptly.

Vendor Security Management

Vendor security management, often referred to as third-party security management, is the practice of assessing and ensuring the security of third-party vendors, suppliers, and service providers with whom an organization interacts.

Assess Vendor Security Practices

Small and medium enterprise owners should ask their IT service providers or vendors a range of questions to ensure they are receiving the best services and support for their specific needs. Here are some basic questions to consider, and you decide what the right answer is that will meet your needs.

Service Offerings

- Do you provide both on-site and remote support?
- Do you offer service level agreements (SLAs), and what do they include?

Response Times

- What are your response and resolution times for different types of IT issues?
- How do you handle after-hours and emergency support?

Security and Compliance

- How do you ensure the security of our data and systems?
- How do you ensure you comply to the regulations specific to our industry?

Backup and Disaster Recovery

- What are your backup and disaster recovery plans to ensure my systems are not affected?
- Can you help us develop a disaster recovery plan in case of data loss or system failures?

Scalability

- How easily can we upgrade or downgrade services if necessary?

Support and Communication

- How do we contact you for support, and what are your support hours?
- Do you provide ongoing communication and status updates on our IT systems?

Monitoring and Maintenance

- How do you monitor our systems for potential issues or vulnerabilities?
- What proactive maintenance do you perform to prevent IT problems?

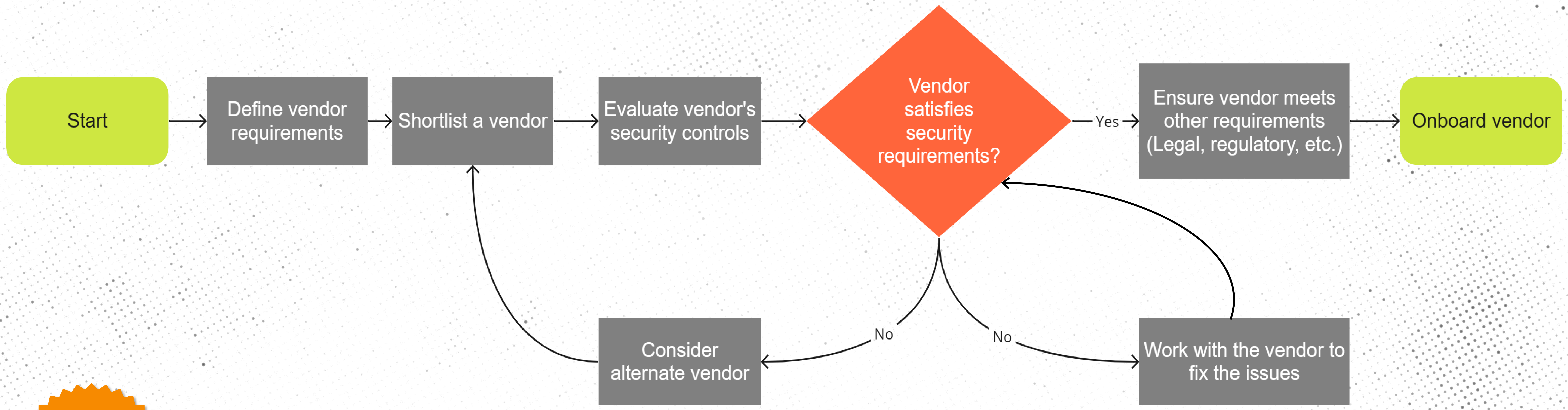
Data Privacy and Ownership

- Who owns the data stored and managed on your systems?
- What steps do you take to protect our data privacy?

Asking these questions can help small business owners make informed decisions when selecting an IT service provider or vendor and ensure that the chosen provider aligns with their business goals and IT requirements.

How to Evaluate Vendors

Evaluating an IT vendor is a crucial process to ensure that you select a reliable and trustworthy partner to meet your organization's technology needs. Here are the steps to follow when evaluating an IT vendor:



Start
Define vendor requirements
Shortlist a vendor
Evaluate vendor's security controls
Vendor satisfies security requirements?
Yes
Ensure vendor meets other requirements (Legal, regulatory, etc.)
Onboard vendor
No
Consider alternate vendor
No
Work with the vendor to fix the issues

Vendor Questionnaire Template

Green Flags for Positive Points and Red Flags to Avoid

Green Flags

Transparent Security Practices

- Vendors that openly share their security practices, policies, and certifications, demonstrating a commitment to transparency

Strong Compliance

- Compliance with relevant security standards and regulations, such as ISO 27001, GDPR, or industry-specific requirements

Data Protection Measures

- Demonstrated commitment to data protection, encryption, and secure storage practices for sensitive information

Redundancy and Disaster Recovery

- Strong redundancy, backup, and disaster recovery capabilities, minimizing the risk of operational disruptions

Cybersecurity Certifications

- Certifications or credentials for cybersecurity staff, indicating a skilled and knowledgeable security team

Red Flags

Lack of security policies

- Polices are poorly documented, rarely updated or missing altogether

Sensitive data breach in the past

- Vendor has experienced having data such as personal information, credit card numbers, health information, or intellectual property in the past

No Incident Response Plan

- Vendor without a well-defined incident response plan may not be prepared to handle security breaches effectively.

Inadequate Employee Training

- Vendors that don't prioritize security awareness training for their employees may pose a greater insider threat risk or;

Unclear Ability to Exit

- The absence of a clear exit strategy for you to recover your data and have their copy destroyed upon contract termination can lead to data exposure or loss

What should I do if there's a red flag?

Red flags are just information that help you make better decisions. An important part of risk management is deciding if the opportunity is worth pursuing if the risk can't be lowered.

Talk about it with your team to be clear on what you stand to gain by moving forward, then compare that against the potential impacts of taking that risk so you can make the decision that fits your business goals..

Not sure what the impacts might be? Talk to a security expert who can explain and give you context.

Key Takeaways: Vendor Security Management

Establish vendor security management to mitigate risks associated with these external entities to safeguard your organization's data, systems, and operations.

For small organizations without a specific IT security team, it’s important to question the vendors on their ability to support your services and secure your infrastructure & data.

Conduct due diligence on prospective vendors by identifying potential security risks and vulnerabilities.

For higher-risk vendors, scrutinize their security practices, policies, and incident response capabilities before entering into any contracts or agreements.

Vendor Questionnaire Template

Incident Management Program

An incident management program plays a critical role in an organization's ability to effectively respond to and mitigate the impact of security incidents and disruptions.

Preparing the Organization for an Incident

Preparing for a cyber incident is essential for organizations of all sizes to minimize the impact of a potential breach or security event. Here are four key ways organizations can prepare themselves:

Develop an Incident Response Plan (IR Plan)

- Create a comprehensive incident response plan that outlines the steps to take in the event of a cyber incident.
- Define roles and responsibilities for incident response team members.
- Include communication protocols, escalation procedures, and contact information for internal and external stakeholders.
- The IRP should cover various types of incidents, including data breaches, malware infections, and denial-of-service attacks.

Implement Security Controls and Monitoring

- Deploy security controls and monitoring solutions to detect and prevent cyber threats.
- Utilize intrusion detection systems (IDS), intrusion prevention systems (IPS), anti-malware software, and firewalls to safeguard the network.
- Implement continuous monitoring to detect suspicious activities and anomalies.
- Utilize security information and event management (SIEM) tools to centralize and analyze security event data.

Regular Training and Drills

- Ensure that employees, including the incident response team, receive cybersecurity training and awareness programs.
- Conduct tabletop exercises and simulated incident response drills to test the effectiveness of the IRP.
- Use these exercises to identify gaps, refine procedures, and familiarize team members with their roles.

Post-Incident Review and Improvement

- After an incident, conduct a thorough post-incident review to assess the effectiveness of the response and identify areas for improvement.
- Use the lessons learned to update and enhance the incident response plan and security controls.
- Share insights and best practices with the incident response team and relevant stakeholders.

Components of Your Incident Response Plan

Incident response plans are dynamic documents that require regular testing, review, and updates to remain effective. It should adapt to evolving threats and technology changes, ensuring that the organization can respond effectively to a wide range of security incidents.

Incident Response Team

Establish a well-defined incident response team (IRT) with assigned roles and responsibilities. Include key personnel from IT, security, legal, compliance, and communication teams.

Detection and Analysis

Define procedures for detecting security incidents, whether through automated security tools, monitoring, or reports from end-users. Describe how to collect and preserve evidence related to the incident for further analysis

Containment Strategies

Develop strategies for containing the incident to prevent further damage or unauthorized access. This might involve isolating affected systems, closing vulnerabilities, or restricting network access.

Data Recovery and Restoration

Describe how to restore affected systems, data, and services to normal operations. Ensure that backups are verified and can be safely restored.

Stakeholder Communication

Specify how to communicate with internal and external stakeholders, including employees, customers, partners, regulatory bodies

Incident Reporting

Document the incident response process and outcomes in a post-incident report. Include details about the incident, actions taken, impact, and lessons learned.

IR Plan Template

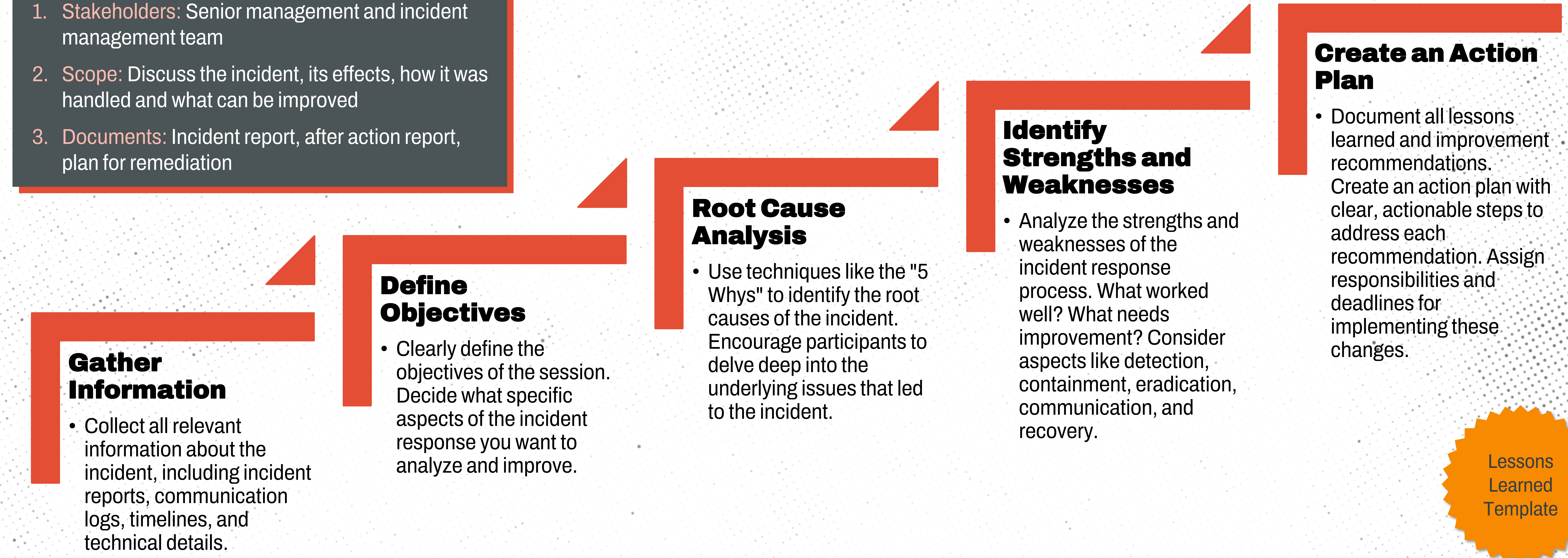
IR Contact Sheet

Building an Effective Improvement Process

Lessons learned and improvement sessions are not just about addressing immediate issues but about building a culture of continuous improvement in incident management. Each session should contribute to enhancing an organization's cybersecurity maturity and response capabilities.

Keys to Success

1. Stakeholders: Senior management and incident management team
2. Scope: Discuss the incident, its effects, how it was handled and what can be improved
3. Documents: Incident report, after action report, plan for remediation



Gather Information

- Collect all relevant information about the incident, including incident reports, communication logs, timelines, and technical details.

Define Objectives

- Clearly define the objectives of the session. Decide what specific aspects of the incident response you want to analyze and improve.

Root Cause Analysis

- Use techniques like the "5 Whys" to identify the root causes of the incident. Encourage participants to delve deep into the underlying issues that led to the incident.

Identify Strengths and Weaknesses

- Analyze the strengths and weaknesses of the incident response process. What worked well? What needs improvement? Consider aspects like detection, containment, eradication, communication, and recovery.

Create an Action Plan

- Document all lessons learned and improvement recommendations. Create an action plan with clear, actionable steps to address each recommendation. Assign responsibilities and deadlines for implementing these changes.

Lessons Learned Template

Discovering Threats: Cyber Threat Intelligence

Now that you know that you need to be aware of when incidents are occurring, here are some practical first steps to start monitoring for threats.

Monitor for Compromised Accounts

Scan for Vulnerabilities

Advanced: Subscribe to threat intelligence monitoring

Knowing when account credentials have been leaked gives you time to change them before a hacker can get in.

For example, registering your domain with www.haveibeenpwned.com to receive alerts, using identity protection services

A lot of threat intelligence is about knowing what vulnerabilities the attackers are exploiting so you can fix those weaknesses.

Scanning for vulnerabilities and applying fixes proactively can stop many of the most common technical attacks.

If your organization has very sensitive information or provides critical infrastructure services, it might be worthwhile subscribing to threat intelligence monitoring services that will proactively gather, analyze and report relevant intelligence to you.

Key Takeaways: Incident Management Program

Ensure that your incident response plan aligns includes procedures for reporting incidents to legal and regulatory authorities and affected individuals (when necessary).

Implement monitoring systems and an incident response plan to detect and respond to unauthorized access attempts and breaches.

Analyze historical security incidents and events to determine if the control has successfully prevented or mitigated potential threats.

After each exercise and major incident, conduct a post-incident review to analyze the response, identify lessons learned, and make necessary adjustments to improve future incident responses.

Discuss how the organization will incorporate insights from incident reports into future incident response improvements. Ensure that incident reports are shared with relevant teams and leadership for review and decision-making.

IR Plan Template

IR Contact Sheet

Lessons Learned Template

Workbook Summary & Next Steps

You've now been introduced to the essence of a cybersecurity program suitable for small and medium enterprises. Here are three key takeaways as you start your cybersecurity journey:

Don't wait to get started

Decide who in your organization will lead security and start building a security culture

Address the areas of highest risk first

Anywhere you have data and systems exposed to the internet, including laptops/desktops and their users, ensure they defended against common threats

Hope for the best but prepare for the worst

Have a plan to follow in the event of an incident, because it's not a matter of if but when an attack will be successful

Next Steps

1. Check out the appendix for additional insights and best practices on the focused areas of Internet of Things (IoT), Cloud Security and Threat Intelligence.
2. Leverage the supplementary package, which contains various security templates and questionnaires, to kick start your cybersecurity program and manage cyber risks in a systematic manner.
3. Run into challenges? You're not alone! Connect with a cybersecurity expert who can help you overcome issues and take your program to the next level.

Appendix

- Securing Your Internet of Things (IoT) Environment
- Securing Your Cloud Environment
- Leveraging Cyber Threat Intelligence
- Glossary
- About White Tuque

Securing Your Internet of Things (IoT) Environment

IoT (Internet of Things*) devices have become increasingly prevalent across industries, however they pose unique security challenges due to their diversity and the potential for widespread consequences if compromised.

Security Challenges

Device Overload

The sheer number of IoT devices makes it difficult to manage and secure all of them effectively.

Resource Constraints

Many IoT devices have limited processing power, memory, and storage, making it challenging to implement robust security measures.

Standardization

The absence of standardized security protocols and practices across IoT devices and platforms can lead to vulnerabilities.

Data Privacy

IoT devices often collect and transmit sensitive data, raising concerns about privacy and data protection.

Firmware Updates

Ensuring that IoT devices receive timely security updates and patches can be challenging, especially for devices in remote locations.

Interoperability*

Integrating IoT devices from different manufacturers can be complex, leading to security gaps.

Securing Your Internet of Things (IoT) Environment

IoT (Internet of Things) Security Best Practices

1. Device Authentication and Authorization

- Implement strong device authentication methods, such as unique identifiers.
- Use role-based access control to limit device access to necessary resources.

2. Vulnerability Management

- Regularly scan and assess IoT devices for vulnerabilities.
- Implement a process for promptly applying security patches and updates.

3. Data Minimization and Privacy

- Only collect and retain data necessary for the device's function.
- Follow data privacy regulations, such as GDPR or CCPA, when handling user data.

4. Encryption

- Encrypt data both in transit and at rest using robust encryption algorithms.

5. Physical Security

- Physically secure IoT devices with locks, tamper-evident seals, and surveillance cameras where appropriate.

Note: Best practices are a starting point and are do not cover all security controls needed to ensure a secure environment.

Securing Your Cloud Environment

Cloud computing offers significant benefits for small and medium-sized enterprises, such as cost savings and scalability. However, it also presents unique security challenges.

Security Challenges

Data Breaches

The risk of unauthorized access to sensitive data stored in the cloud is a significant concern.

Data Loss

Data stored in the cloud may be subject to loss due to accidental deletion, service provider errors, or cyberattacks.

Compliance

Meeting regulatory requirements and ensuring data privacy (e.g., PIPEDA, GDPR, HIPAA) can be challenging in a cloud environment.

Identity and Access Management

Managing user identities and permissions across multiple cloud services can become complex.

Shared Responsibility

Understanding the shared responsibility model between the cloud provider and org. to secure data and applications.

Shadow IT

Employees may use unsanctioned cloud services without IT approval, which can create security blind spots.

Securing Your Cloud Environment

Cloud Security Best Practices

1. Choose Reputable Cloud Service Providers (CSPs)
   - Select CSPs with a strong track record of security and compliance.
   - Review their security certifications and standards.
2. Data Encryption
   - Encrypt data both at rest and in transit using encryption protocols and keys. Utilize encryption services provided by the CSP.
3. Access Control
   - Implement strong authentication methods, such as multi-factor authentication (MFA), for access to cloud services.
   - Enforce the principle of least privilege for user access.
4. Compliance and Legal Considerations
   - Understand the legal and regulatory requirements applicable to your industry and region.
   - Ensure your cloud setup aligns with these requirements
5. Regular Security Assessments
   - Conduct periodic security assessments, including vulnerability scanning and penetration testing, to identify and remediate vulnerabilities.

Note: Best practices are a starting point and are do not cover all security controls needed to ensure a secure environment.

Leveraging Cyber Threat Intelligence

What Are Threat Intelligence Feeds?

Threat intelligence feeds are live data streams that give your IT and security team information about possible online dangers. These updates typically include simple signs or clues, and each update usually concentrates on one specific area. For instance, an update might share information about:

- Websites that seem suspicious
- Lists of hashes (like a fingerprint) for known harmful software
- Internet addresses linked to malicious activity

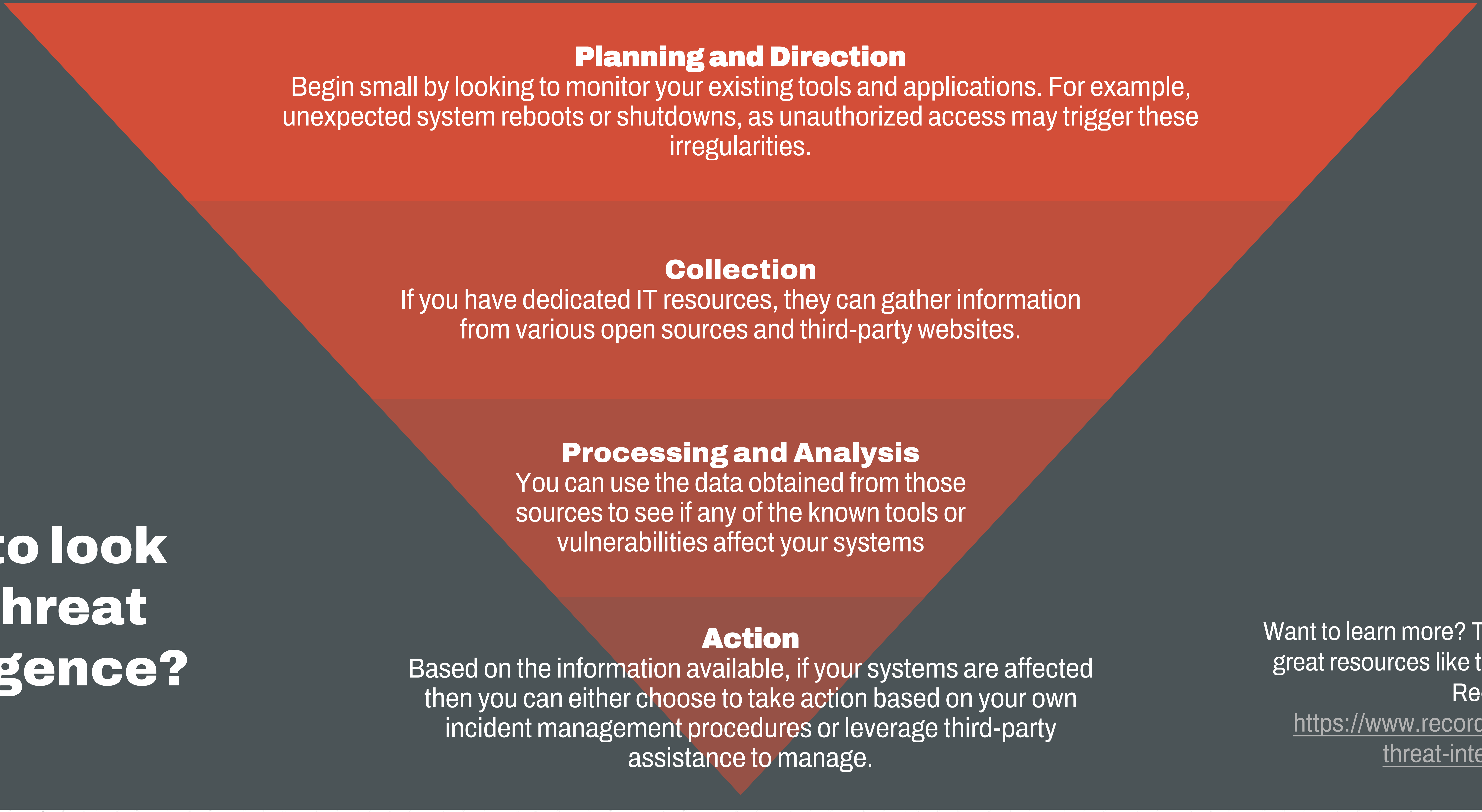
It's important for organizations to gather threat intelligence from a combination of these sources and use it to inform security policies, risk assessments, and the configuration of security tools. Additionally, threat intelligence should be shared and analyzed to enhance collective cybersecurity efforts.

Common Sources of Threat Intelligence

- Government and Law Enforcement Agencies
- Cybersecurity Blogs and Forums
- Social Media and Dark Web Monitoring
- Cybersecurity Threat Feeds from Security Vendors

Leveraging Cyber Threat Intelligence

What to look for in threat intelligence?



Planning and Direction
Begin small by looking to monitor your existing tools and applications. For example, unexpected system reboots or shutdowns, as unauthorized access may trigger these irregularities.

Collection
If you have dedicated IT resources, they can gather information from various open sources and third-party websites.

Processing and Analysis
You can use the data obtained from those sources to see if any of the known tools or vulnerabilities affect your systems

Action
Based on the information available, if your systems are affected then you can either choose to take action based on your own incident management procedures or leverage third-party assistance to manage.

Want to learn more? There are many great resources like this article from Recorded Future: https://www.recordedfuture.com/threat-intelligence-feeds

Glossary

- Cybersecurity Controls: mechanisms used to prevent, detect and mitigate cyber threats and attacks. Mechanisms range from physical controls, such as security guards and surveillance cameras, to technical controls, including firewalls and multifactor authentication.
- Data Breach: any security incident in which unauthorized parties gain access to sensitive data or confidential information
- Data Extortion: act of coercing an individual or company to pay in exchange for gaining back access to stolen cyber assets
- Distributed Denial of Service (DDoS): is usually performed by bombarding the targeted computer or resource with unnecessary requests to overload systems and prevent some or all legitimate requests from being completed
- Encryption: process of encoding data or information in such a way that only the parties who have the key to unscramble it can access the data.
- Endpoint: endpoints are physical devices that connect to and exchange information with a computer network. Some examples of endpoints are mobile devices, desktop computers, virtual machines, embedded devices, and servers.
- Internet of Things (IoT): collective network of connected devices that facilitates communication between devices and the cloud, as well as between the devices themselves.
- Interoperability: the real-time data exchange between different systems that speak directly to one another in the same language.
- Ransomware: a type of malicious software designed to block access to a computer system until a sum of money is paid
- Threat Actor: any person or organization that intentionally causes harm in the digital sphere. They exploit weaknesses in computers, networks and systems to carry out disruptive attacks.
- Vulnerability: weakness in an IT system that can be exploited by an attacker to deliver a successful attack

Couldn't find a term that you're looking for? Check out https://niccs.cisa.gov/cybersecurity-career-resources/vocabulary

Our Mission

White Tuque is your trusted partner in best practices for cyber defense with expertise in cyber risk, vulnerabilities, protection, and intelligence.

We're focused on providing solutions that protect your assets and are practical for your business. We work with organizations of all sizes because we believe cybersecurity is important for everyone.

Our team of experts helps clients identify risk and quantify potential impacts, develop security policies, and construct security controls that identify, prevent, and recover from incidents.

Our Approach

We study your people, processes, and technology to understand how to best defend your organization. The solutions are built, tailored, and customized to your organization's specific needs.

This approach ensures your investment leads to meaningful and measurable reduction of risks, and better defense against future threats.

DCC Cybersecurity Workbook
prepared by

WHITE TUQUE

We Understand the Risk.
We Know the Threat.
We can help.

www.WhiteTuque.com
1-844-WT-TUQUE
https://www.linkedin.com/company/whitetuque/