Communications Security Establishment | Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

Choosing the best cyber security solution for your organization

Management

Canada

Foreword

This document is an UNCLASSIFIED publication that has been issued under the authority of the Head of the Canadian Centre for Cyber Security (Cyber Centre). For more information, email, or phone our Contact Centre:

Contact Centre
contact@cyber.gc.ca
(613) 949-7048 or 1-833-CYBER-88

This publication takes effect on October 03, 2022.

Revision history

Revision	Amendments	Date
1	First release.	October 03, 2022

ISBN 978-0-660-45677-5
CAT D97-4/10-023-2022F-PDF

Overview

As technology evolves and becomes more sophisticated, threat actors look for new ways to exploit individuals and organizations. Falling victim to a cyber attack can lead to devastating, and sometimes irreversible damage. Due to these evolving threats, organizations of all sizes face challenges in finding security solutions that fit their budget and are tailored to their cyber environments and business needs.

This document discusses the various options available to organizations of all sizes when looking to strengthen their cyber security posture. It will introduce the basic cyber security best practices that organizations can implement with existing resources, as well as outline those that can be implemented with the assistance of a managed security service provider (MSSP). MSSPs provide a variety of cyber security services including network security, endpoint protection and monitoring. In addition to information security services, MSSPs can also host, deploy, monitor, and manage their clients' security infrastructures.

The cyber security best practices and controls presented in this document are intended for organizations of any size. We present the five baseline security controls any organization can implement with existing resources that will enhance their cyber security posture. Several other security controls are identified, with varying levels of resources and technical knowledge required, to successfully implement in your organization. For those who lack in-house technical knowledge and have the resources, outsourcing some or all of your cyber security needs to a third party such as an MSSP can enhance your organization's resiliency and protection against cyber incidents.

For more information, phone, or email our Contact Centre:

Contact Centre

contact@cyber.gc.ca

(613) 949-7048 or 1-833-CYBER-88

Table of contents

1 Introduction 5
2 Determining your cyber security posture 6
2.1 Basic cyber security best practices 7
2.2 Advanced cyber security best practices 8
3 Outsourcing your cyber security 9
3.1 Internet Service Provider (ISP) 9
3.2 IT/Cyber security consultant 10
3.3 Cloud Service Provider (CSP) 10
3.4 Managed Security Service Provider (MSSP) 11
3.4.1 Differences between an MSSP and an MSP 12
3.4.2 Criteria to consider 13
3.4.3 Benefits and disadvantages of contracting an MSSP 14
3.5 Managed security service categories 15
3.5.1 Managed security service technologies 15
3.5.2 Data protection and security monitoring 15
3.5.3 Risk and vulnerability assessment and management 16
3.5.4 Compliance monitoring and management 16
4 Summary 17
5 Supporting content 18
5.1 List of abbreviations 18
5.2 Glossary 19
5.3 References 20

List of tables

Table 1: Risk Assessment Questions 6
Table 2: Differences Between an MSSP and an MSP 12
Table 3: List of Criteria to Evaluate MSSP 13

1 Introduction

With an evolving threat landscape and increased levels of cyber attacks, organizations of all sizes and business lines are facing increased and more complex threats. The damage caused by threat actors can be disastrous, costly, and sometimes irreversible. Every organization, irrespective of its size, is at risk of cyber security threats. Some common cyber attacks that organizations face include the following:

- **Phishing**: Threat actors attempt to solicit confidential information from an individual, group, or organization by mimicking or spoofing, a specific, usually well-known brand for financial gain. Phishers attempt to trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information, which they may then use to commit fraudulent acts.
- **Malware**: Malicious software designed to infiltrate or damage a computer system without the owner's consent. Common forms of malware include computer viruses, worms, trojans, spyware, and adware.
- **Insider threats**: An insider threat is anyone who has knowledge of or access to your organization's infrastructure and information and who uses, either knowingly or inadvertently, the infrastructure or information to cause harm.
- **Ransomware**: Malware that denies you access to your files until a sum of money is paid.
- **Credential stuffing:** A cyber attack where stolen account credentials are used to gain unauthorized access to user accounts through large-scale automated login requests directed against a web application.

Cyber criminals are targeting organization of all sizes; however, many small and medium organizations feel their data and assets are of little value or interest to cyber criminals. Cybercriminals target small to medium organizations because they:

- Lack adequate cyber security resources to protect their information which makes them easier to hack
- May not be backing up their data which makes them vulnerable to ransom threats
- Store valuable data, such as personal and financial information
- Serve as a gateway to larger organizations that procure services and supplies from these smaller organizations

The National Cyber Threat Assessment 2020 judges that cybercrime is the cyber threat most likely to affect Canadian organizations [1]. If you are targeted and your systems are breached, your organization may face some of the following consequences:

- Reputational damage
- Productivity loss
- Operational disruptions
- Intellectual property and data theft
- Recovery expenses
- Potential fines and legal fees

Following the guidance outlined in this publication will help you strengthen your organization's cyber security posture. We will introduce basic cyber security best practices that organizations can implement, starting with the most obtainable for smaller organizations to a full complement of cyber security controls and best practices for larger organizations. Regardless

of the size of your organization, this document will assist you in strengthening your cyber security posture and provide you with guidance on more comprehensive security services and technologies that can be procured from MSSPs. We will demonstrate how enlisting the assistance of an MSSP can enhance the cyber security posture of your organization, as well as your ability to detect, mitigate, and recover from a cyber incident.

2 Determining your cyber security posture

Implementing mitigation measures to enhance the security of your infrastructure, networks, systems, and data can seem daunting, especially if your organization lacks in-house expertise. Some organizations choose to outsource cyber security to third party service providers; however, it may not be an affordable option for all. The information presented in this section will assist you in assessing your organization's cyber security posture by addressing primary cyber security best practices.

The first step in understanding the cyber security requirements of your organization is to conduct a risk assessment, which will identify any known or potential vulnerabilities and security priorities within your infrastructure and data repositories, especially as it concerns your most sensitive information assets. The risk assessment will define what potential threats exist, what their sources might be, and what incidents could occur if these vulnerabilities are exploited. The assessment will also identify the impacts of various threats or incidents on your organization, as well as the relative likelihood of each possible scenario.

As a second step you should identify the cyber security requirements specific to your organization's functions, roles, and responsibilities. Understanding the value of your information assets is critical in this process. For example, your organization may store sensitive information about customers that requires additional protection. As a business owner you are legally responsible under the Personal Information Protection and Electronic Documents Act (PIPEDA) [2] or similar provincial legislations to protect your clients and customers personal information and report privacy and data breaches that pose a risk of harm to individuals to office of the Privacy Commissioner of Canada. Safeguarding your proprietary information from cyber incidents is also important to maintain your competitive edge and business continuity. Your organization is responsible for protecting the confidentiality, integrity, and availability of your data and assets.

Table 1 provides examples of preliminary questions organizations of all sizes should address when conducting a risk assessment.

Table 1: **Risk Assessment Questions**

Number	Risk Assessment Questions	Answers
1	Do you have a list of all assets (e.g. systems, devices) that are connected to your network?	
2	What are the different levels of protection that are needed for your assets?	
3	Who has access to those assets?	
4	Where are they stored?	
5	What security controls are currently in place to protect them?	
6	What are the likeliest incidents that will threaten those assets?	
7	Do you have an Incident Response Plan (IRP) in place (i.e. do you know who to call and what to do when an incident occurs - communications, security, legal, executive)?	

2.1 Basic cyber security best practices

Baseline security controls and good cyber hygiene practices can enhance your organization's resiliency and protection against cyber incidents. These controls are not a one-size-fits-all approach to cyber security. They are guiding principles that you can use to create your organization's own cyber security framework. These baseline security controls are meant to help small and medium sized organizations, namely organizations that have less than 500 employees, protect their assets and information and to improve their resiliency via cyber security investments. The baseline security controls were chosen based on our analysis of cyber threat activity trends and their impact on Internet-connected networks. Organizations that implement these recommendations will address many vulnerabilities and enhance their protection against cyber threats.

Organizations should determine what elements of their information systems and assets are within the scope they wish to consider for the baseline controls. Information systems and assets in this context refer to all computers, servers, network devices, mobile devices, information systems, applications, services, cloud applications, etc. that an organization uses to conduct its business. We strongly recommend that organizations consider all of their information systems and assets, (whether owned, contracted, or otherwise used) within the scope for the baseline controls.

You should scope and tailor these controls based on your organization's risk assessment, business needs, and requirements. While it is ideal for organizations to implement all of the baseline security controls, it may not always be possible. For organizations that are lacking in-house IT support or have limited resources, starting with the following five controls will strengthen your cyber security posture and help minimize the risk of cyber incidents:

1. **Implement strong user authentication:** Use authentication policies that balance security and usability. Ensure your devices authenticate users before they can gain access to your systems. Wherever possible, use two factor authentication (2FA) or multi-factor authentication (MFA).
2. **Patch operating systems and applications:** When software issues or vulnerabilities are identified, vendors release patches to fix bugs, address known vulnerabilities, and improve usability or performance. Where possible, enable automatic patches and updates for all software and hardware to prevent exposure to known vulnerabilities.
3. **Backup and encrypt data:** We recommend that organizations back up all essential business information and critical applications regularly to one or more external secure location, such as the cloud or an external hard drive. Data backups are a critical piece of the effort to ensure quick recovery not only from cyber security incidents such as ransomware or malware but also from natural disasters, equipment failures, or theft. Backups can be done online or offline and can also be done in three different iterations: full, differential, or incremental. Store back-ups in a secure, encrypted state to protect the confidentiality of your data. Back-ups should only be accessible to those responsible for the testing and/or use of restoration activities. Test your backups regularly to ensure you can restore your data.
4. **Train your employees:** Tailor your training programs to address your organization's cyber security protocols, policies, and procedures. Having an informed workforce can reduce the likelihood of cyber incidents.
5. **Develop an incident response plan:** If you have a plan, you can quickly respond to incidents, restore critical systems and data, and keep service interruptions and data loss to a minimum. Prior to implementing your plan, you need to know what assets, information and systems are of value to your organization. Analyze what type of incidents you might face and identify what would be an appropriate response. Consider who is qualified to be on the response team and how you will inform your organization of your plan and associated policies and procedures. For more

information on how to develop an incidents response plan you can refer to the publication *Developing your incident response plan* [3].

2.2 Advanced cyber security best practices

The security controls presented in this section build upon the five foundational controls mentioned in section 2.1. These controls require additional resources and may be suitable for an MSSP or other third-party cyber security services to manage for your organization.

1. **Enable security software:** Activate firewalls and install anti-virus, anti-malware and endpoint detection and response (EDR) software on your devices to thwart malicious attacks and protect against malware. Ensure you download this software from a reputable provider. Install Domain Name System (DNS) filtering on your mobile devices to block out malicious websites and filter harmful content.
2. **Secure websites:** Protect your website and the sensitive information it collects by encrypting sensitive data, updating your certificates when required, using strong passwords or passphrases on the backend of the site, and using HTTPS for your site. If you have outsourced your website, ensure the host has security measures in place that align with your internal security controls, policies, and procedures.
3. **Secure mobile devices:** Choose a device deployment model (e.g. bring-your-own device, corporately provisioned devices) that aligns with your organization's security posture and policies. Ensure your employees can only use applications approved by your organization and can only download applications from trusted sources.
4. **Access control and authorization:** Apply the principle of least privilege. Only provide employees with access to the functions and privileges necessary to complete their tasks to prevent unauthorized access and data breaches. Employees should only have access to the information that they need to do their jobs. Each user should have their own set of log-in credentials, and administrators should have separate administrative accounts with associated privileged access rights.
5. **Establish basic perimeter defences:** Defend your networks from cyber threats by implementing basic perimeter defences, such as using a firewall or virtual private network (VPN). A firewall can be used to defend against outside intrusions by monitoring incoming and outgoing traffic and filtering out malicious sources. A VPN can be used when employees are working remotely to secure the connection and protect sensitive information.
6. **Configure devices securely:** Ensure you review the default settings of your devices and make modifications as required. At a minimum, we recommend changing default passwords (especially administrative passwords), turning off location services, and disabling unnecessary features.
7. **Secure portable media:** Storing and transferring data using a portable media device, like a USB key, is convenient and cost-effective, but they can be prone to loss or theft. Your organization should use encrypted portable storage devices, maintain an inventory of all assets, and sanitize devices properly before reusing or disposing of them.

The last control is one your organization should understand and implement when outsourcing all or part of your cyber security.

8. **Secure cloud and outsourced services:** Ensure you research a service provider before entering into an agreement to procure their products or services. Your research should determine whether the service provider has the measures in place to meet your security requirements that will support your business needs. If working with a cloud service provider (CSP) it is important to understand their data management policies, including where their data centres are

located as there are differing international privacy laws and data protection requirements you may be unfamiliar with.

For more information on these security controls, please refer to the publication *Baseline Cyber Security Controls for Small and Medium Organizations* [4].

In addition to these baseline controls, organizations can also engage MSSPs to assist in providing in-depth advice and guidance, as well as concrete security measures your organization can implement to improve your cyber security posture. Section 3 provides clarity regarding the services provided by MSSPs and what your organization should consider prior to acquiring their services.

3 Outsourcing your cyber security

Selecting effective security and risk management solutions to protect your organization against attacks and safeguard your data is crucial to your cyber security posture. Some organizations choose to outsource a portion or all their cyber security requirements to a third party. This has become a common practice for organizations of all sizes.

There are many cyber security professional services available. All of them should have the ability to develop an effective cyber security plan that will benefit your organization. Implementing your plan will benefit your organization in many ways, including:

- Reducing the risk and potential impact of cyber attacks
- Protecting your systems, networks, and technologies from exploitation
- Preventing unwanted third parties from accessing sensitive information
- Protecting against disruption of services
- Maintaining productivity by reducing down-time from malware
- Enabling improved business continuity

3.1 Internet Service Provider (ISP)

The level of protection, along with the cost of implementing and maintaining cyber security controls, varies depending on the nature and requirements of your organization. While outsourcing services can be beneficial, the cost can be prohibitive to some organizations. If hiring a cyber security company like an MSSP is not a viable option for your organization, you should consult with your ISP to see if they offer cybersecurity services. For example, many ISPs provide anti-virus, anti-malware, and firewall software to customers as an add-on service for an additional fee in their plans.

The following list highlights some questions you should ask an ISP if you wish to procure add-on security services to your organization's network.

- Do you offer intrusion prevention systems?
- Can you detect cyber intrusions as they are formed and before they reach their targets?

- Do you offer malware detection?
- Can you detect and block IP address spoofing?
- Do you send your users notifications of any infections or intrusions (i.e. botnet)?

3.2 IT/Cyber security consultant

It can be challenging to understand exactly what your organization's cyber security needs are as well as identify the potential impacts to your organization if you were a victim of a cyber incident. An IT or cyber security consultant can help you identify which areas of security need to be addressed and how your implementation of security controls and action items should be prioritized.

An IT or cyber security consultant is often hired by a client to:

- Conduct a thorough risk assessment of their business
- Test their current security measures
- Assess software, computer systems, and networks for vulnerabilities
- Help design and implement a robust cyber defense model
- Provide recommendations and technical advice
- Design, build, and deploy cyber security solutions

Discussing your organization's cyber security posture and determining the actions needed to ensure your networks, systems, and data are secure will also help you decide if your organization needs MSSP services. Many MSSPs will also do a preliminary assessment of your cyber security posture to support you in choosing what type and level of service is best suited for your security needs.

3.3 Cloud Service Provider (CSP)

Many organizations are migrating their IT infrastructure, storage, applications, databases, and data to the cloud. This may be partly because they lack their own full-time IT resources, or because cloud computing can help reduce the cost of IT services and security. Cloud computing can also reduce the cost of in-house IT resources, hardware, servers, storage, and maintenance. Many organizations look to CSPs for assistance as they can offer on-demand and scalable computing environments and a richer set of capabilities.

While cloud services are convenient and cost-effective, they do not automatically ensure protections to your organization's assets in the cloud or managed by a CSP. When engaging with a CSP, you are giving up direct control over many aspects of security and privacy, and in doing so, granting a level of trust to the CSP. With cloud services, your organization is still accountable for protecting the confidentiality, integrity, and availability of IT services and information hosted by the CSP. To benefit from cloud computing, your organization should identify all business and security requirements and ensure that security risks are properly managed, cloud-specific security considerations are addressed, and security controls of cloud-based services are properly assessed before authorized for use.

In general, CSPs offer three different service models for clients to choose:

- **Infrastructure as a service (IaaS):** In an IaaS service model, the capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer can deploy and run arbitrary software, which may include operating systems and applications.

- **Platform as a service (PaaS):** In a PaaS service model, the capability provided to the consumer is to deploy onto the cloud infrastructure consumer created or acquired applications created using programming, libraries, services, and tools supported by the provider.
- **Software as a service (SaaS**): In a SaaS model, the service provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface such as a web browser (e.g. web-based email), or a program interface (e.g. local application).

To enable the adoption of cloud computing, the Government of Canada (GC) developed an integrated risk management approach to establish cloud-based services Which is outlined in the publication *Cloud Security Risk Management (ITSM.50.062*) [5]. This publication outlines the approach that can be applied to all cloud-based services independently of the cloud service and deployment models.

Note that there are differences between cloud services and managed services. The main difference revolves around who has control over the data and the processes. With managed services, the consumer (e.g. your organization) dictates the technology and operating procedures. However, with cloud services, the service provider dictates both the technology and the operational procedures available to the consumer (e.g. your organization).

3.4 Managed Security Service Provider (MSSP)

Cyber threat actors continue to improve their tactics and are sometimes able to bypass the most sophisticated security measures. Organizations are facing heightened and more complex risks to their environments and even with dedicated IT professionals on staff, they are becoming victims of cyber-attacks. Now, more than ever, organizations of all sizes are outsourcing a portion or all their cyber security to MSSPs.

An MSSP is a technology firm that provides cyber security services to companies and organizations. MSSPs can host security services, deploy cyber security software and hardware, and manage your security infrastructure in addition to providing information security (IS) services. They provide outsourced monitoring and management of security devices and systems, and in some cases can take mitigative action on your IT systems to help combat and prevent compromises.

There are many reasons why organizations choose to work with an MSSP. Some may lack the in-house resources or expertise for certain areas of security or they may need security monitoring and management outside of normal operating hours. Other organizations may want to hire an MSSP to conduct security audits or respond to and investigate incidents.

Other reasons for hiring an MSSP include the following:

- Scaling up security
- Layering on your in-house security to help fill some gaps
- Implementing/Integrating tailored third-party security solutions and technologies to your IT Infrastructure/architecture
- Increasing visibility of threats while expediting a security response

The services that an MSSP can provide include:

- Managing firewalls, intrusion detection systems (IDS), threat defense technologies and VPNs

- Managing Security Incident and Event Management (SIEM) tools
- Continuous device and system monitoring
- Managed Detection and response (MDR) Services including monitoring, detecting, alerting, and managing response to potential attacks on your system
- Overseeing patch management and upgrades of security equipment and software
- Performing security assessments and security audits
- Conducting vulnerability tests and threat scans to provide recommendations and advice on cyber security solutions
- Security Awareness Training
- Operationalizing threat intelligence

Note that there are differences between a managed service provider (MSP) and an MSSP. An MSP offers information technology (IT) administration, whereas the MSSP takes care of cyber security. There are, however, some MSPs that offer endpoint, network, and cloud security services. If you have a contract with an MSP, check to see which security services they offer. A more in-depth comparison is explained in the next section.

3.4.1 Differences between an MSSP and an MSP

An MSSP establishes one or more security operations centers (SOCs) which is responsible for monitoring and protecting the security of their customer's infrastructure (e.g., networks, applications, databases, servers). An MSP may have its own network operation center (NOC) to ensure that the customer's IT operations run smoothly. They handle all IT aspects of an organization on a subscription basis but may not provide security related monitoring as part of that service.

Table 2 highlights the main differences between an MSP and an MSSP.

Table 2: **Differences Between an MSSP and an MSP**

MSSP	MSP
Focus on IT security operations.	Focus on baseline IT operations such as Help desk, endpoint management, backup management, networks, and firewalls management.
Provides security monitoring and defense. Ensures that IT systems are always protected. Can include scanning and analysing of threats and Managed Detection and Response (MDR).	Monitors networks and IT infrastructure to ensure they are running smoothly.
Provides specialized security tool integration and support.	Manages, updates, and maintains network systems and provides IT solutions and support.
Provides security operations support including detection, alerting and possibly response.	Provides IT operation support and services, including help desk.
Provides incident management and ensures business continuity and disaster recovery.	Provides maintenance, bug fixes, and updates after a threat detection.

The focus of an MSP is IT administration, whereas an MSSP offers cyber security support. Choosing an MSSP is a complex decision for any organization and requires thorough research and analysis. The next section lists criteria to consider when engaging with an MSSP.

3.4.2 Criteria to consider

When making the decision to outsource certain security functions, you need to thoroughly understand the objectives that your organization wants to achieve. Your security goals need to be identified before any decisions are made. Not all MSSPs offer the same sets of services or capabilities, so you should choose a provider that can address your organization's security requirements.

When evaluating potential MSSPs, consider the criteria listed in Table 3. These will help you to choose a provider that has the right capabilities to keep your assets and data protected.

Table 3: **List of Criteria to Evaluate MSSP**

Number	Criteria
1	Does the MSSP provide well-established and trusted sets of security standards, processes, and procedures they apply and follow for their operations?
2	What services does the MSSP offer around management, monitoring, response, and reporting of security incidents to their customers. Do these integrate well with your organizations' operations?
3	Does the MSSP have an experienced cyber security team with recognized knowledge on cyber security skills and capabilities. Do they have accreditations or other certifications required for their staff?
4	Does the MSSP understand your organization's compliance and regulatory standards as they relate to cybersecurity requirements?
5	What technology and infrastructure is the MSSP using to support and deliver threat detection and response, enable change management on your systems, and provide alerts? Do these technologies/systems look to be a good fit to integrate with your operational systems? Is the service mostly cloud based? On premises with remote monitoring? A hybrid?
6	Does the MSSP adhere to an IT security risk management framework (e.g. ITSG-33 [6], NIST 800-53 [7], ISO27001 [8], COBIT, CIS Controls) for its own security planning?
7	Can the MSSP provide confirmation that they have customers from your industry? Can they provide references from customers working in your industry?
8	Does the MSSP have a baseline service level agreement (SLA) or a set of service level objectives (SLO) that defines their commitments to response times/time to resolution and other important metrics? Ask for an example SLA and review it to see if it responds to your requirements in terms of speed of detection, alerting, and resolution.
9	What mechanisms can they support for alerting? Do they support emailing alerts, and do they provide an administrative portal for reporting? Do they offer mobile alerting (short messaging service (SMS), applications or other messaging)?
10	Does the MSSP have an ability to integrate with any of your on-premises security tooling/software. Can the MSSP easily feed information back to an on-premise Security Information and Event Management (SIEM) device, or consume data based off of your organization's antivirus/endpoint logs?
11	How does the MSSP protect your systems/information from compromise – where do they store their logs? How do they protect that data at rest? In transit? How do their systems/employees connect to your networks/systems/data? How is this monitored/controlled/audited? Do you have access to any of the audit data? Can the MSSP respond to your data residency requirements (if any)?

Number	Criteria
12	How can the MSSP help with remediation in the case of a compromise? Ask questions around being able to perform forensic analysis and how it is supported on data/services they manage on your behalf. Do they offer mitigation support after an intrusion has occurred such as emergency incident response?
13	Can the MSSP produce a certificate of evaluation from a third party against security standards (e.g. SSAE SOCII/TYPE II, ISO 270001)?
14	Does the MSSP offer community shared threat intelligence to their costumers?
15	Is the client given access to the MSSP's systems and interfaces (dashboarding/APIs/accounts)?
16	Who are the MSSP's suppliers?
17	How much do the various services cost?

3.4.3 Benefits and disadvantages of contracting an MSSP

Some of the benefits of engaging with an MSSP include:

- Enhancing the skillset and coverage of your existing security team
- Reducing the costs of hiring in-house, skilled IT security specialists, updating technologies, and implementing malware detection equipment, and new programs
- Having access to skilled, certified security experts and their research and threat intelligence
- Having access to cutting-edge technology
- Mitigating threats and vulnerabilities by using highly efficient processes and workflow automation to significantly improve remediation time for security issues and
- Providing 24/7 SOCs to validate and send alerts on potential security threats

There are also some disadvantages to consider:

- When you choose to engage with an MSSP to protect your business data, you are putting your security in outsiders' hands while you ultimately own the risk.
- MSSPs are lucrative targets for cyber attacks as the impact of a breach of a service provider can result in the breach of personal information of many clients at once. It is important to understand how your networks and data, which are supported by the provider, are protected against a possible compromise of the service provider itself.
- Unlike an in-house IT team, an MSSP may not always be aware of the new services and changes that your organization implements.

Mitigating the risks associated with using contracted security services is a responsibility that your organization shares with the MSSP. However, your organization is legally responsible for protecting its data including personal information and must defend its network and information systems. If your organization decides to outsource its cyber security, you should have an open dialogue with the MSSP and understand the measures they take to secure their business and services. Ongoing communication with the MSSP is important to ensure that the security strategies are being reviewed and updated as required by your evolving business priorities and systems.

3.5 Managed security service categories

Whether your company is looking to outsource some or all of its cyber security services, consulting with a trusted MSSP can offer an unbiased perspective to help you align your organization's goals to the best security solutions possible.

Typical MSSPs offer on-site consultancy to assist their clients with the following:

- Assessing their risks
- Determining key business security requirements
- Developing security policies and processes
- Integrating security technology
- Providing on-site mitigation support after an intrusion has occurred such as emergency incident response and forensic analysis

3.5.1 Managed security service technologies

The most common MSSP IT services include deploying, managing, and configuring the following:

- Intrusion detection and prevention systems (IDPS)
- Endpoint detection and response (EDR)
- Web content and traffic filtering
- Security incident and event management (SIEM)
- Extended detection and response (XDR)
- Identity and access management (IAM)
- Privileged access management
- Vulnerability scanning and assessment
- Patch management
- Anti-virus, anti-spam, anti-malware
- Firewalls
- VPNs
- Data loss prevention (DLP)
- Threat intelligence
- Device and systems monitoring

3.5.2 Data protection and security monitoring

MSSPs offer services to protect data, ensure devices and systems are functioning as intended, and identify existing or imminent threats. These services include, but are not limited to the following:

- **Anti-malware**: Help identify and address malicious code within clients' systems, infrastructure, and applications.

- **Backups and disaster recovery**: Protect clients' data against the risk of loss due to security breaches and other disruptions. Help ensure that there is a copy of data to restore if systems are compromised.
- **Digital forensics**: Investigate security incidents to determine what went wrong and prevent them from recurring.
- **Application allow lists and DLP**: Distinguish known-safe resources from potentially malicious ones.
- **Email security**: Mitigate the risk of phishing and other types of email attacks.

MSSPs offer day-to-day monitoring and interpretation of important system events throughout the network including unauthorized behavior, malicious hacks, denial of service (DoS), anomalies, and trend analysis.

3.5.3 Risk and vulnerability assessment and management

An MSSP can help your organization identify, prioritize, and remediate known vulnerabilities, which cybercriminals can exploit to gain access to applications, systems, and data. Vulnerability management services range from providing vulnerability assessments of networks, systems, and applications to the client where the remediation actions are the client's responsibility, to a complete vulnerability management service where discovered vulnerabilities are also remediated through automated patching and system reconfiguration.

To find and respond to different risks, an MSSP provides these types of services:

- **Vulnerability scanning and patching**: Help identify known vulnerabilities within applications and address them.
- **Penetration testing:** Simulate attacks that cybercriminals might perform to evaluate how well a client's infrastructure can withstand them.
- **Security assessment and audits:** Identify misconfigurations that could lead to security vulnerabilities, as well as opportunities to make security policies even stronger.
- **Intrusion detection**: Monitor for and respond to intrusions and intrusion attempts.
- **Threat hunting**: Identify and eradicate threats proactively in your environment using computer forensics, cyber threat intelligence, and malware analysis.

Risk management offerings may include monitoring, maintaining the firewall's traffic routing rules, and generating regular traffic and management reports to the clients. Intrusion detection management, either at the network level or at the individual host level, involves providing intrusion alerts to a client, keeping up to date with new defenses against intrusion, and regularly reporting on intrusion attempts and activities. Content filtering services may be provided by email filtering and other data traffic filtering.

3.5.4 Compliance monitoring and management

If you are required to prove that your state of security is compliant with government and industry regulations, you may request that the MSSP assesses, tracks, and documents your organization's adherence to specific compliance mandates.

In addition, compliance monitoring could include monitoring event logs for change, sometimes referred to as change management. This service identifies changes to a system that violates a formal security policy. In short, it measures compliance to a technical risk model.

4 Summary

In this publication we offer organizations of all sizes cyber security solutions that can help enhance and strengthen their cyber security posture and improve their resiliency to cyber threats. We present the cyber security best practices and controls that should be implemented by all organizations, irrespective of their size. Organizations needs to determine if they have the resources and in-house technical knowledge to provide adequate protection against cyber threats or if they will need to outsource some or all of their cyber security needs to a third party such as an MSSP. The overall objective is to creates and maintains a strong cyber security posture by establishing a robust cyber security solution.

5 Supporting content

5.1 List of abbreviations

Term	Definition
CIS	Center for Internet Security
DLP	Data loss prevention
DNS	Domain name system
DoS	Denial of service
EDR	Endpoint detection and response
IAM	Identity and access management
IaaS	Infrastructure as a service
IDPS	Intrusion detection and prevention systems
IDS	Intrusion detection systems
IS	Information security
ISO	International Organization for Standardization
IRP	Incident response plan
ISP	Internet service provider
IT	Information technology
MDR	Managed detection and response
MSP	Managed service provider
MSSP	Managed security service provider
MFA	Multifactor authentication
NIST	National Institute of Standards and Technology (US)
NOC	Network operation center
PIPEDA	Personal Information Protection and Electronic Documents Act
PaaS	Platform as a service
SaaS	Software as a service
SIEM	Security incident and event management
SLA	Service level agreement
SLO	Service level objective
SOC	Security operations centers
2FA	Two factor authentication
VPN	Virtual private networks
XDR	Extended detection and response

5.2 Glossary

Term	Definition
Adware	An advertising supported software that displays unwanted advertisements to the user of a computer.
Availability	The ability for the right people to access the right information or systems when needed. Availability is applied to information assets, software, and hardware (infrastructure and its components). Implied in its definition is that availability includes the protection of assets from unauthorized access and compromise.
Baseline security controls	The minimum mandatory protective mechanisms outlined by Treasury Board of Canada Secretariat (TBS) policy instruments to be used in interdepartmental IT security functions and information systems.
Botnet	Several Internet-connected devices infected by malware that allow malicious actors to control them.
Confidentiality	The ability to protect sensitive information from being accessed by unauthorized people.
Cybercrime	Crime that uses computers and/or computer networks.
Data breach	A cyber security incident wherein someone takes sensitive information without the authorization of the owner.
Encryption	Converting information from one form to another to hide its content and prevent unauthorized access.
Firewall	A security barrier placed between two networks that controls the amount and kinds of traffic that may pass between the two.
Injury	The damage that businesses suffer from the compromise of information systems and IT assets.
Integrity	The ability to protect information from being modified or deleted unintentionally or when it's not supposed to be. Integrity helps determine that information is what it claims to be. Integrity also applies to business processes, software application logic, hardware, and personnel.
Intellectual property	Legal rights that result from intellectual activity in the industrial, scientific, literary, and artistic fields. Examples of types of intellectual property include an author's copyright, trademark, and patents.
Least privilege	The principle of giving an individual only the set of privileges that are essential to performing authorized tasks. This principle limits the damage that can result from the accidental, incorrect, or unauthorized use of an information system.
Patching	The application of updates to computer software or firmware.
Personal information	Information that is about an identifiable individual and recorded in any form, as defined in section 3 of the Privacy Act.
Privacy Breach	A privacy breach is an incident involving the unauthorized collection, use or disclosure of personal information. Such activity is "unauthorized" if it occurs in contravention of the Privacy Act. A breach may be the result of inadvertent errors or of malicious actions by employees, agents, contractors, third parties, partners in information-sharing agreements, or intruders.

Term	Definition
Ransomware	A type of malware that denies a user's access to a system or data until a sum of money is paid.
Risk Assessment	A risk assessment is the process of identifying, analyzing and prioritizing risk to the organization's operation. It helps determine what cyber security controls are required for the organization's level of risk.
Role-based access control	Access control based on user roles (i.e. a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals.
Security control	A management, operational, or technical high-level security requirement needed for an information system to protect the confidentiality, integrity, and availability of its IT assets. Security controls can be applied by using a variety of security solutions that can include security products, security policies, security practices, and security procedures.
Sensitive information	Information that requires protection against unauthorized disclosure.
Threat	Any potential event or act (deliberate or accidental) or natural hazard that could compromise IT assets and information.
Trojan	A malicious program that is disguised as or embedded within legitimate software.
Virus	A computer program that can spread by making copies of itself. Computer viruses spread from one computer to another, usually without the knowledge of the user. Viruses can have harmful effects, ranging from displaying irritating messages to stealing data or giving other users control over the infected computer.
Virtual private network	A private communication network usually used within a company, or by several different companies or organizations to communicate over a wider network. VPN communications are typically encrypted or encoded to protect the traffic from other users on the public network carrying the VPN.
Vulnerability	A flaw or weakness in the design or implementation of an information system or its environment that could be exploited by a threat actor to adversely affect an organization's assets or operations.
Spyware	An unwanted software that infiltrates a computing device, stealing internet usage data and sensitive information.

5.3 References

Number	Reference
1	Canadian Centre for Cyber Security. *National Cyber threat assessment 2020.* November 16 2020.
2	Office of the Privacy Commissioner of Canada. *The Personal Information Protection and Electronic Documents Act*. February 2021.
3	Canadian Centre for Cyber Security. *ITSAP.40.003 Developing Your Incident Response Plan*. February 2022.
4	Canadian Centre for Cyber Security. *Baseline Cyber Security Controls for Small and Medium Organizations*. February 2020.

Number	Reference
5	Canadian Centre for Cyber Security. *ITSM.50.062 Cloud Security Risk Management*. March 2019.
6	Canadian Centre for Cyber Security. *ITSG-33 IT Security Risk Management: A Lifecycle Approach*. December 2014.
7	National Institute of Standards and Technology. *NIST Risk Management Framework*. December 2020
8	International Organization for Standardization. *ISO 27001: Information Security Management*. 2018.