ROAD INFRASTRUCTURE OPERATIONAL TECHNOLOGY CYBER SECURITY PRIMER

December 2022

Transport Canada Transports Canada

Canada

Cette publication est aussi disponible en français sous le titre Technologie opérationnelle d’infrastructure routières guide d’introduction sur la cybersécurité.

TP 15529E

Cat. T89-14/2022E-PDF

ISBN 978-0-660-42293-0

Prepared by Transport Canada.

CONTENTS

1. Executive summary

This primer was created to share guidance and best practices with Canadian infrastructure owners and operators (IOO) so they can develop and/or continue to refine their cyber security programs for intelligent transport systems and traffic management systems (TMS).

Intelligent transport systems (ITS) integrate different information and communications technologies into road transportation infrastructure and vehicles to help make the transportation system safer and more efficient. TMS are types of operational technology (OT) that help control and produce products and services like traffic light systems and active road management systems.

Both ITS and TMS systems are being combined with information technology (IT) systems to optimize and improve the efficiency and safety of Canadian roads.

However, most legacy ITS equipment wasn't designed to be combined and connected with other systems and networks, and often were not developed with emerging cyber security risks in mind. As these systems are combined, IOOs should consider new threats and apply appropriate security controls.

This primer gives an overview of the current ITS landscape, existing and emerging cyber threats and vulnerabilities that should be considered, and the potential impacts of cyber-attacks. The primer also identifies tools, resources and frameworks that can be used to assess and improve your organization's cyber security posture (the strength of your organization's cyber security and ability to resist and respond to cyber threats).

The recommendations section introduces 6 actions that IOOs should consider putting in place:

1. **Understand the environment.** Understanding the environment, including the sensitivity and exposure of data moving through the network, is essential to planning and implementing new technologies while also managing risk.
2. **Understand the current cyber security posture**. Improving systems and protecting against vulnerabilities that are known. This starts with assessing the current state of your organization's cyber security posture, identifying areas for improvement, and prioritizing work.
3. **Make sure the organizational structure and planning processes support OT cyber security**. Make sure the organizational structure and planning processes will help to understand OT cyber security risks and assign enough resources to address them.
4. **Use cyber security policies and best practices**. Use industry standards and compliance frameworks to make sure cyber security controls and considerations are applied to IT and OT assets.
5. **Develop and test incident response plans and processes**. Develop formal incident response plans that are understood by key stakeholders, tested, and updated regularly.
6. **Continue assessing cyber risk.** Cyber risks are always changing. The rapid use of new technologies and information and operational technologies merging means you need to be aware of zero-day vulnerabilities (vulnerabilities that vendors don't know about) and emerging risks.

By using these best practices and other cyber hygiene activities, IOOs can limit cyber risk today and into the future.

2. How to use this guide

Road transportation technologies are changing quickly. These changes can improve road safety, introduce new forms of mobility, and create economic opportunities. While these technologies bring many benefits, they also introduce new cyber security vulnerabilities.

Integrating these technologies into your organization's environment, along with constantly evolving cyber security threats, has introduced new risks to Canada's road transportation system.

Road transportation is a shared responsibility between federal, provincial/territorial, and municipal governments. Transport Canada established vehicle safety standards and regulations, and Canada's provinces, territories, and municipalities (collectively known as "road authorities") are responsible for planning, designing, building, operating, and maintaining most of Canada's road network.

This primer will help IOOs better understand the unique cyber security considerations of Traffic Management Systems (TMS) and Intelligent Transportation Systems (ITS). While most organizations already have well-established Information Technology (IT) cyber security practices in place, securing the Operational Technology (OT) used in TMS and ITS requires an approach that is based on Industrial Control System (ICS) cyber security practices. It also includes real-world examples that highlight the need to be proactive.

Since cyber security is always evolving, the aim of this primer is to help organizations understand this complex task and includes practical steps and best practices to improve cyber security posture. While some of the technical standards in this guide will eventually become out-of-date, the best practices and need to stay both vigilant and current will endure.

The recommendations in this primer offer strategic cyber security guidance. They are not technical standard or exhaustive solutions for TMS and ITS cyber security.

This primer should be used alongside best practices, guidance and standards developed by:

- Public Safety Canada
- the Communications Security Establishment
- other federal departments with cyber expertise
- trusted international regulators
- industry associations
- relevant cyber security resources for other sectors, and
- standard setting bodies

3. The current state of intelligent transport and traffic management systems

Today's TMS are made up of heavily interconnected systems that use technology to improve the flow of traffic and safety. A by-product of connecting these technologies is an increasingly connected environment that exposes vulnerabilities to more threats.

As shown in Figure 1, there are 3 key factors that must be considered when integrating a traditionally segregated OT environment with an IT environment:

- **convergence**: Uniting IT and OT infrastructures blurs the divide between the physical and cyber worlds, which could make it hard for an organization to understand and protect the whole environment
- **interoperability**: Combining old and new systems and platforms can be complicated and hard to manage and protect
- **integration and connectivity:** Blending services across domains through the "internet of things" (IoT - the network of everyday devices that can connect and share information with each other) and digital technologies can be complicated and hard to manage and protect

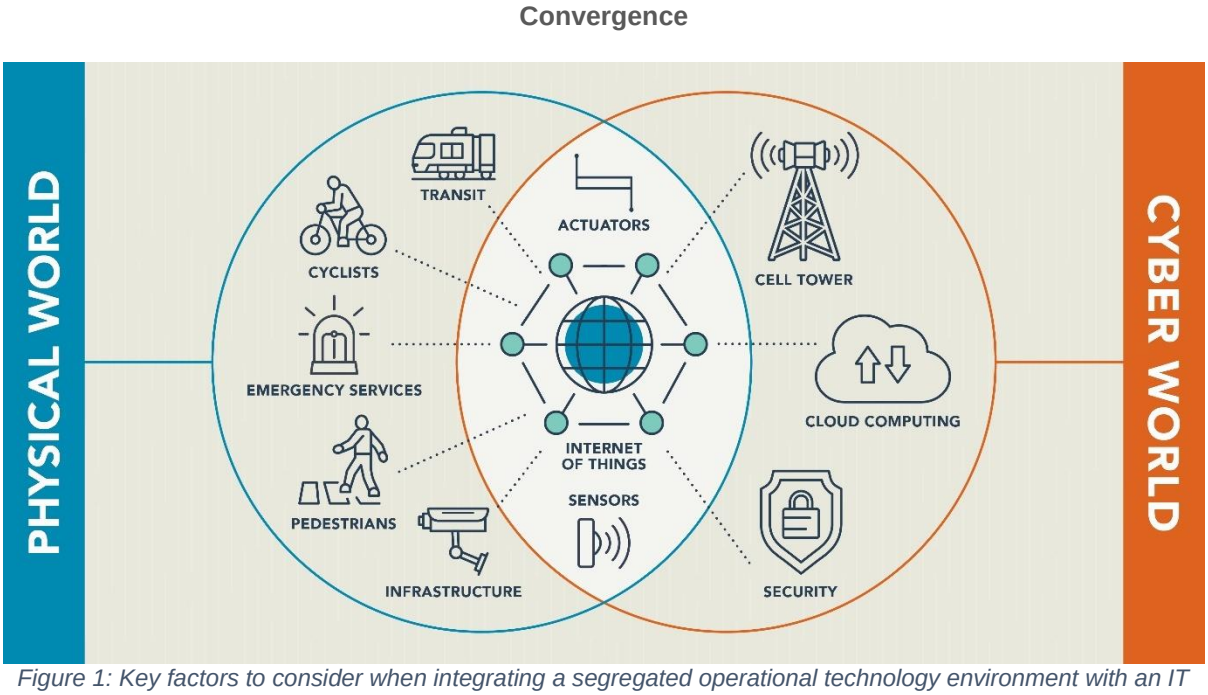

Figure 1: Key factors to consider when integrating a segregated operational technology environment with an IT environment

Interoperability

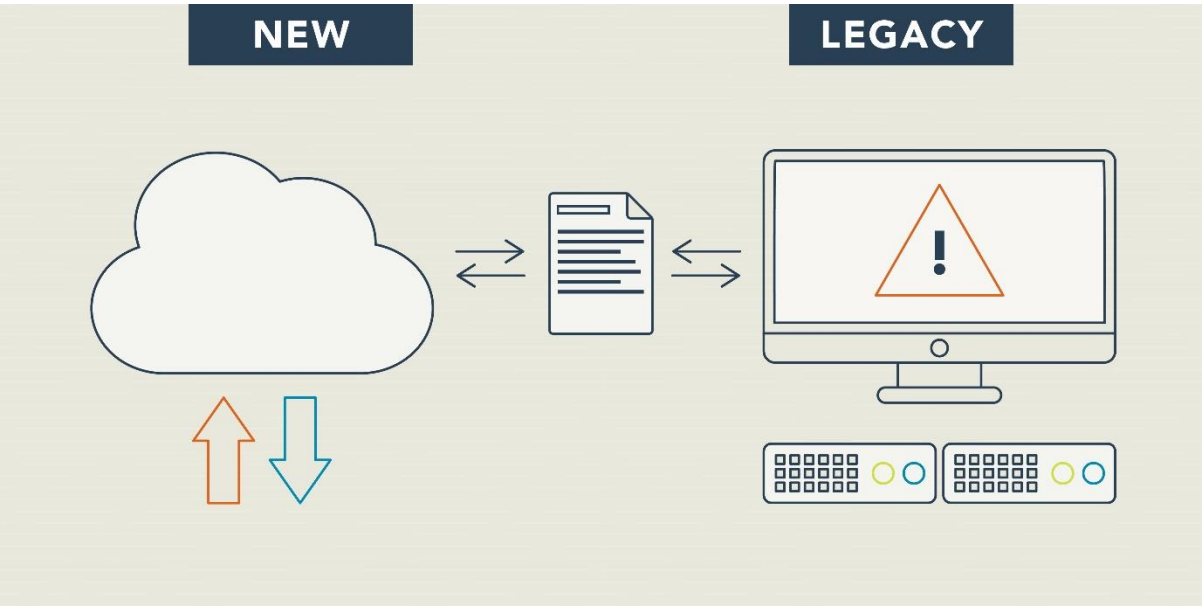

Figure 2: Interoperability between new modern systems and legacy systems

Integration

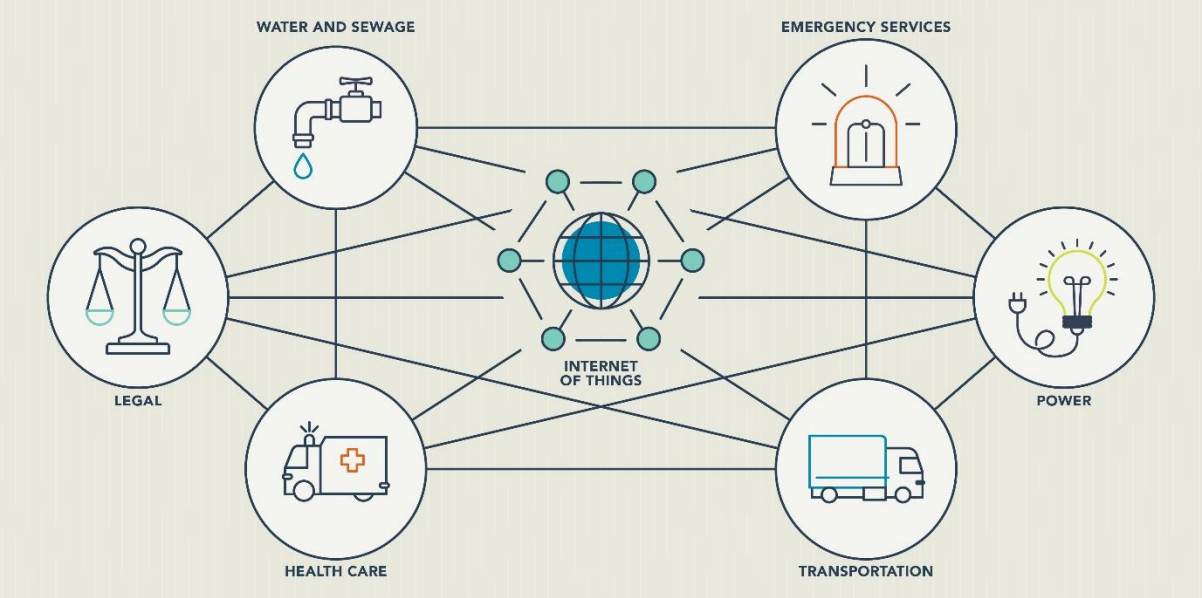

Figure 3: Integration and connectivity of different critical infrastructure

Traditional TMS have many parts like signal controllers (software that controls traffic signals), traffic sensors, closed circuit tv (CCTV), and variable message signs. The parts in many existing TMS systems weren't designed to connect to external networks.

As a result, standard security controls that are common to IT systems, like mandatory authentication and authorization, may not have been implemented or prioritized when the systems were developed. The lack of basic security controls poses a serious risk when adding them to such advanced systems.

TMS gather and send large amounts of data to various endpoints and through connected devices. This data keeps the system operating correctly, efficiently, and safely. Endpoint devices that send and receive data within a TMS are connected Internet of Things (IoT) devices with built-in access to the Internet.

In many cases, these IoT devices aren't protected enough before they're deployed, and data may be unencrypted. If someone gained access to the network with these IoT devices, they could steal or change the data, or add harmful data.

If a TMS is hacked, the system could be manipulated, traffic patterns disrupted, or safety could be compromised. Since the data within the TMS directly affects user's experiences and safety, securing these systems is critical.

Finally, it's important to understand that the lifecycle of new digital ITS equipment may be shorter than previous generations of electro-mechanical systems. It may also require more frequent software-based maintenance (like firmware updates), similar to newer IT systems and equipment.

3.1. Emerging threats

2020 saw a spike of cyber threats against OT systems and OT asset owners around the world. Recognizing the vulnerabilities introduced by combining information and operational technology, cybercriminals have been increasingly targeting critical OT infrastructure around the world. These groups range in sophistication (severity of attacks) and vary in their motives.[1]

> "Canadian organizations of all sizes, like small- and medium-sized enterprises, municipalities, universities, and critical infrastructure (processes, systems, facilities, technologies, networks, assets, and services that keep government running and Canadians healthy, safe and secure) providers, face a growing number of cyber threats.
>
> These organizations control a range of assets that are of interest to cyber threat actors, including intellectual property, financial information and payment systems, data about customers, partners and suppliers, and industrial plants and machinery. Generally, the more Internet-connected assets an organization has, the greater the cyber threat it faces."
>
> - Canadian Centre for Cyber Security – 2020 National Cyber Threat Assessment

The most common motive for cyber criminals is financial gain. A common method is using a ransomware attack to block access to a critical system or application and demanding a ransom before

[1] Canada. Communications Security Establishment. *An Introduction to the Cyber Threat Environment*. https://cyber.gc.ca/sites/default/files/publications/Intro-to-cyber-threat-environment-e.pdf. Accessed 22 April 2022.

restoring access. User privacy can be compromised during a ransomware attack if data is stolen, leaked, or sold.

Outside of hacking variable message signs in the Deutsche Bahn - WannaCry example, there haven't been any major publicly reported cyber-attacks against TMS as of early 2022. However, many other critical infrastructure systems (like power generators, oil and gas, chemicals) have and continue to be the target of cyber-attacks. Find other examples of attacks in Section 4.2.

Critical infrastructure may also be the target of a politically motivated attack, due to the critical importance to the nation and its citizens.

Other than political or financial gain, attacks may be motivated by curiosity or vandalism. These types of attacks are less likely due to the skills and knowledge required for a successful attack. Appendix A has a detailed description of potential threat actors and their typical motivations.

As more connected infrastructure is put in place, IOOs need to use secure design principles to limit the attack surface of TMS. Not only will it be important to design systems securely, IOOs will need to design their infrastructure and OT environment to protect and handle large volumes of data. This data will need to be protected both at rest and in transit, using encryption technologies and best practices for the industry.

Implementing these encryption technologies at-scale isn't easy and may result in performance issues. A thorough understanding of the environment, including the sensitivity and exposure of data traversing the network, is essential to properly plan and implement encryption technology.

It's also important to make sure of the following:

- properly manage configurations
- monitor for malicious behaviour and
- apply security patches, where possible

Threat actors will often take the path-of-least-resistance. Through diligent vulnerability management and mitigation of known vulnerabilities, IOOs can reduce the likelihood of being targeted by a malicious threat actor.

It's crucial that critical infrastructure systems (like power generators, oil and gas plants, chemical plants) stay isolated from and not directly connected to the Internet as this would be a significant and easily used vulnerability. Generally, various IT networks exist in front of critical infrastructure systems. Through applying the requisite security controls to these IT networks, organizations can begin to harden their OT systems from the risks posed by external threats. General cyber security best practices, like following the principal of least privilege, help to protect computers and servers used by organizations. Refer to the recommendations section for more best practices.

Identifying and assessing potential risks and determining your organization's risk tolerance is key. This will help to make risk-based decisions when determining the appropriate security controls to put in place. Whenever possible, organizations should replace unsupported systems and hardware. Organizations can still use unsupported devices in a secure manner, by performing appropriate cyber security risk management assessments, implementing the appropriate security controls through architecture design techniques (like segmenting networks), and by implementing other measures for defence in depth.

4. Potential impact of cyber attacks

4.1. Potential impacts of intelligent transportation systems

As stated previously, there are various groups who may target critical infrastructure systems with specific goals in mind. Depending on the nature of the attack, their goals, and the organization targeted, the impact may vary.

Stolen data, disrupted networks, malware, and other cyberattacks can have significant consequences for the victim organization or individuals. The likelihood and impact of these threats will continue to increase. It's important to understand the potential impacts that may result from a cyber attack, as they can inform the decisions around security controls.

Safety

The infrastructure involved in traffic and transportation is developed with safety measures to protect riders, commuters, and workers. If safety systems and their fail-safes are compromised, riders, commuters, and operators could be seriously injured. Safety systems are likely targets since they can be a powerful tool for extorting an organization.

Operations

A well-executed attack may result in disrupting the underlying transportation infrastructure. From the perspective of critical infrastructure systems, a widely distributed attack could have a ripple effect, impacting other public sectors significantly. These impacts could have negative economic effects like supply chain disruptions. For example, a targeted attack could result in the loss of function in a lane control system which will lead to increased congestion, the potential for traffic accidents, and disruptions to major transport routes.

Reputation

A significant breach or disruption could damage public perception of ITS and the organizations involved (IOOs, technology suppliers etc.). In situations where there's a personal data breach (like names, addresses or plate number data) there are privacy implications for the public that could impact an organization's reputation.

Finances

Organizations that have experienced a major cyber-attack are likely to suffer financial consequences. This may come in many forms, whether it's choosing to pay a ransom (ransomware), legal costs, decreased public perception impacting revenue, and operational and capital costs to mitigate the attack and repair/replace damaged equipment. As an example, an attacker could target a vulnerable system, encrypting a high-value asset like a traffic control system. Attackers would request a ransom to be paid before releasing the system for use.

4.2. Examples of attacks

With all the new technology being added to transportation systems, there are new dimensions to the cyber risks associated with these systems. The transportation sector has become exploitable by malicious cyber-attacks or susceptible to accidental compromise.

The likelihood of new or more significant events is increasing along with the cost of cyber incidents and cyber-crime. By analysing previous breaches, road authorities can prepare for a cyber event. Below are some high-level examples of cyber-attacks on similar industries or systems.

Toronto Transit Commission – Ransomware (2021)

The Toronto Transit Commission disclosed that it was the target of a ransomware attack that affected vital communication systems. Systems used to communicate with vehicle operators, platform screens, external applications, email systems, and many other elements were encrypted and rendered unusable. The attack was discovered and initially had a small impact, but the following day the attackers broadened their attack and infected multiple systems and network services.[2]

Israel Water Treatment Plant – Advanced persistent threat (2020)

An advanced persistent threat is sophisticated, highly skilled and well-funded. They are usually a nation state or state-sponsored group, which accesses a computer network and stays undetected for a long time.

Israel revealed that its water infrastructure had been targeted to increase the chemical levels in drinking water and sabotage agricultural pumping stations. Had the attacks been successful, chemicals would have made the water poisonous, possibly triggering fail-safes to shut-down the water pumps leaving thousands without water.[3]

Deutsche Bahn - WannaCry (2017)

Deutsche Bahn announced the organization had been targeted with the “WannaCry” ransomware. While train service wasn’t disrupted, electronic boards at stations across the country displayed notices from the attacker demanding payment from Deutsche Bahn. German officials assured the public that the attack didn’t affect government computer systems.[4]

San Francisco Municipal Transport Agency - HDDCryptor malware (2016)

The San Francisco Municipal Transport Agency was the target of a large-scale ransomware attack using a version of the HDDCryptor malware. Officials from the agency stated the attack had infected 2,112 computers, encrypting them for a ransom of 100 bitcoin ($73,086 USD at the time). The attack froze the agencies point-of-sale terminals and fare-gates so they couldn’t function. To reduce the customer impact on the train system, the agency was forced to allow customers to ride for free.[5]

[2] https://www.thestar.com/news/gta/2021/10/29/ransomware-attack-on-ttc-shuts-down-vital-communication-systems.html
[3] https://www.timesofisrael.com/cyber-attacks-again-hit-israels-water-system-shutting-agricultural-pumps/
[4] https://www.reuters.com/article/us-cyber-attack-germany-rail-idUSKBN1890DM
[5] https://www.theguardian.com/technology/2016/nov/28/passengers-free-ride-san-francisco-muni-ransomeware

These examples prove that threat actors can use many different kinds of attacks to exploit vulnerabilities in OT. These attacks can vary in complexity, but a general theme is that these attacks use multiple entry points, techniques, and attack vectors.

We recommend IOOs further analyse case studies to identify positive practices and potential opportunities for improvement to minimize the impact of a potential cyber event.

5. Recommendations

As previously noted, the introduction of IT into traditionally physical OT systems and TMS improves core functionality and makes these systems “smart”. In these scenarios the software and hardware of these OT/ICS/TMS remain the same but have introduced an element of digitalization through connected software and networks. This may encompass connected and automated vehicle (CAV) communications devices, centralized traffic monitoring and management, connected infrastructure, AI supported traffic management, amongst numerous other use cases such as signal prioritization for buses. While TMS capabilities have improved with increased IT/OT convergence, so has the exposure to multiple threats coming from local and distant sources. IOOs need to improve their cyber security posture to avoid being vulnerable to attacks. Disruptions to the function of the underlying OT software may have significant consequences, such as disrupting supply chains, having negative socioeconomic impacts, and even more importantly, jeopardizing public safety and national security. IOOs can limit the impact of a cyber-attack by using best practices to improve their organization’s resilience. Here are examples of some best practices and next steps that your organization could take to manage cyber risk.

ⓘ These recommendations are not exhaustive. They have been included to give IOOs some ideas on next steps to improve your organization’s resilience.

Understand the environment

A good understanding of the operating environment, including the sensitivity and exposure of data traversing the network, is essential to properly plan and implement new technologies, while managing risk.

This understanding will help to identify vulnerabilities and risks that may arise as you begin to integrate new technology. To accomplish this, an organization should stay informed on the latest standards, frameworks, and guidance available. Appendix C includes reference materials that can help an organization stay current with cyber security tools and best practices.

Understand your cyber security posture

To reach a target cyber security posture, organizations must meaningfully protect against cyber threats and address weaknesses within the system. Organizations can only prepare and protect for vulnerabilities that are known. To do this, organizations will need to:

- assess the current cyber security posture
- identify areas for improvement, and

- prioritize cyber security work, as needed

Appendix B includes details on different types of attacks.

Transport Canada's Road Infrastructure Cyber Security Maturity Assessment Tool, which can be found on the Road Transportation Cyber Security web page, will help IOOs assess their current cyber security posture. In addition, the tool will allow IOOs to establish a target state and will provide recommendations to achieve it.

The target profile is customizable, so IOOs can implement security controls that reflect their unique risk assessment. The tool will be based on the NIST Cyber Security Framework and customized for TMS and ITS.

Support operational technology cyber security

It's critical for organizations to have a comprehensive cyber security program that considers potential threats and vulnerabilities across the organization, including both information and operational technology. IOOs should review their current cyber security organizational structure to make sure the planning processes support OT cyber security.

Senior leaders should emphasize the need to enforce cyber security controls and best practices across the organization and share security objectives and priorities via top-down direction. Strategic plans – financial, operational, human resources - should reflect the ongoing nature of OT cyber resilience.

An organization's ability to meet target cyber security posture depends on planning and dedicating funds for OT equipment, and for buying, training, and retaining staff.

Use policies and best practices

Organizations should develop an integrated approach and appropriate policies to manage cyber security across information and operational technology assets. Use industry standards and compliance frameworks to assess and model the organization's risk management policy as it relates to TMS assets, IT assets, processes, procedures, and vendors.

Whether organizations manage IT or TMS, the frameworks in Appendix C can be used by IOOs as a baseline for implementing the right people, process, technology, and governance practices to manage cyber risk.

These voluntary frameworks will help you create, maintain, and improve cyber security maturity and general preparedness. These frameworks will help IOOs divide these domains into manageable categories helping them meet their cyber security maturity and preparedness goals.

Practice

Even the most mature organizations may experience a cyber breach at some point. The way an organization can identify, assess, respond, and recover from the cyber event can dictate the impact to their organization.

IOOs should develop formal incident response plans that are communicated to key stakeholders, tested to ensure efficacy, and updated on an ongoing basis. A joint information and operational technology cyber incident response plan can help make sure that an organization can respond to cyber threats. Find more information in Appendix C.

Continue to assess cyber risks

Managing cyber risks is an ongoing process that needs to be embedded into an organization's risk management function. With the rapid use of emerging technologies and the combination of IT and OT, cyber risks are always changing. As such, IOOs must stay attuned to zero-day vulnerabilities and emerging risks, so they can react accordingly.

By understanding the evolving threat landscape and pro-actively implementing the cyber security best practices noted above, IOOs can reduce their cyber risk, while also improving their resilience.

Appendix A: Threats and motivations

An overview of potential threat actors and their motivations.[6]

Nation-state or state sponsored

State sponsored threats are generally considered the most sophisticated. These groups are funded and trained by adversarial nations states, which increases their abilities and resources substantially. An important distinction in this category of threat actors is they aren't usually financially motivated. Instead, attacks are done to advance geo-political interests.

Cybercriminals

Cybercriminals generally have moderately sophisticated attacks. They lack the resources that state-sponsored groups usually have but can still pose a major threat. Their motive is usually financial, and they often use ransomware to extort money from their victims. Some of the more advanced cybercriminal groups are related to organized crime.

Hacktivists, terrorist groups, and thrill seekers

These groups are generally less sophisticated than the previously mentioned groups. They rely on readily available tools for attacks and generally lack the technical skills of professional hackers. They are often motivated by a desire to disrupt and be a nuisance within OT systems.

Internal threats

Internal stakeholders may intentionally or unintentionally target OT and IT assets. A disgruntled employee may intentionally target a system, or a new employee may accidentally damage or infect one.

[6] Canada. Communications Security Establishment. *An Introduction to the Cyber Threat Environment*. https://cyber.gc.ca/sites/default/files/publications/Intro-to-cyber-threat-environment-e.pdf. Accessed 22 April 2022.

Appendix B: Types of attacks

Network intrusion

Malicious actors are always looking for vulnerabilities that they can use to gain access to networks and systems. In some cases, attackers will use these vulnerabilities to get remote access to modify a system.

When identified, these vulnerabilities can be dealt with by using patches from their vendors.

These vulnerabilities are important to ITS and OT networks. These systems, often consisting of legacy hardware, are out-of-support and un-patched. These legacy systems can often have significant real-world risk.

Zero-day vulnerabilities

Unfortunately, equipment vendors don't know about every vulnerability, so these systems can still be targeted by attackers. These are known as "zero-day vulnerabilities". Zero-day vulnerabilities are particularly difficult to detect if exploited, since the issue is unknown unless disclosed or discovered by someone other than an attacker.

Malware

Malicious software, known as "malware", is often used to attack internal systems. There are many types of malware, some custom developed by attackers, others purchased to be used by attackers, including:

- **remote access trojans** insert a "backdoor" into a network that allows an attacker to gain access. This access could then be used to steal data, damage systems, or manipulate controls
- **ransomware** encrypts infected systems, blocking access to files until a ransom is paid. This can render systems useless, which may not be fixed once a ransom is paid
- **point of sale malware** infects payment systems and is used to harvest the payment details of customers which are then sold through online marketplaces
- **keyloggers** are used to record a user's keystrokes. Attackers can use this to steal credentials which they can then use to gain access to systems
- **spyware** is used to secretly watch a computer user. It can be used to gain access to confidential information or steal credentials
- **rootkit** is a hard to detect type of malware which is designed to hide malicious activity on a computer. Rootkits can allow a remote attacker to gain control of a system

Denial of service (DDoS)

Denial of service attacks involve attackers coordinating multiple resources, often bots, to direct traffic towards systems to overwhelm and crash them. This is known as a distributed denial of service attack, which grew more common in the latter half of the 2010s.

Distributed denial of service attacks are known for their simplicity. Tools have been created and distributed across the internet so inexperienced users can launch coordinated attacks against different targets. Distributed denial of service tools significantly decreases the technical barrier of attacking and can significantly disrupt systems.

Social engineering and phishing

Social engineering is a broad term used to describe exploiting human interactions. Attackers may pose as someone they are not (an employee, an ISP, etc.,) and appear unassuming to the targets. First, these attackers will collect as much information as possible from someone. This could include addresses, gaining access to restricted areas, or even passwords.

Phishing is a form of social engineering. Phishing attacks are very common, and the attacks can range from basic to very advanced, some even targeting C-Suite executives with very specific information and specially crafted messages. Phishing attacks use emails to manipulate users into clicking malicious links or sharing sensitive data. Phishing is commonly used to install malware.

Other forms of phishing are “vishing” (phishing over a voice connection) and “smishing” (phishing over text/SMS). These types of attacks are less common, and aggressive, but still pose a risk of data leaks and malicious intrusion.

Side-channel attacks

A side-channel attack targets the indirect responses from hardware like electrical emissions or other physical effects to understand and then extract secrets. A common target of side-channel attacks are cryptographic systems (systems that protects information and communications by using encryption algorithms).

Side-channel attacks are possible because cryptosystems produce physical effects when they operate (like the sound an operation emits or the power it consumes), which can provide clues about the system. Leaks of this information may not seem valuable, but sophisticated attackers can use this information to guess the algorithmic keys used to encrypt data.

Once they have this information, attackers can decrypt sensitive data and compromise the system. These attacks are very hard to perform, but a skilled and committed hacker may coordinate with others on this type of attack.

In the OT space, side-channel attacks can be used to guess the link between control signals and their effect on the system, which is extremely valuable information for an attacker.

Appendix C: Standards and other resources

Cyber security is always evolving. Understanding the latest risks, trends, types of attacks and how to reduce the impact of attacks is one of the most important actions any organization can take.

Standards and frameworks

The Center for Internet Security's Critical Security Controls

A standard developed by the Center for Internet Security that focuses on prioritized safeguards to reduce cyber security risks using governance and technical controls.

National Institute of Standards and Technology's Cyber Security Framework

This framework can help an organization create or improve a cyber security program. It uses best practices to help organizations improve their cybersecurity posture. The framework is organized by 5 key functions: identify, protect, detect, respond, and recover. (English only)

National Institute of Standards and Technology's Guide to Industrial Control Systems (ICS) Security

Includes guidance on how to secure industrial control systems, while addressing their unique performance, reliability, and safety requirements. The document provides an overview of industrial control systems and typical system topologies (a network's structure that includes how the different parts are connected), identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to reduce risks.

National Institute of Standards and Technology's Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems

This publication covers how to develop more defensible and survivable systems. It includes the mechanical, physical, and human parts that make-up systems and the abilities and services that these systems deliver.

ISO/IEC/IEEE 15288 - Systems and software engineering - System life cycle processes

A standard that helps organizations manage the processes involved with developing solutions and maintaining systems.

Resources from the Government of Canada

The Canadian Centre for Cyber Security

The **Canadian Centre for Cyber Security (CCCS)** is Canada's authority on cyber security. They have brought together cyber security expertise from Public Safety Canada, Shared Services Canada, and the Communications Security Establishment in to one organization.

Cyber alerts

The **centre issues alerts and advisories** on potential, imminent or actual cyber threats, vulnerabilities or incidents affecting Canada's critical infrastructure systems.

Guidance documents

The centre's cyber security experts work with industry partners and departments and agencies to develop **guidance on cyber security topics**. These guidance documents include recommendations and actions that organization's can implement to protect their networks, systems, and information.

Transportation sector cyber call

To join the centre's Transportation Sector Partnerships Team distribution list, please email: **transport-par@cyber.gc.ca.**

Developing your incident response plan (ITSAP.40.003)

Your incident response plan must include the processes, procedures, and documents related to how your organization detects, responds to, and recovers from incidents.

Developing your IT recovery plan (ITSAP.40.004)

To make sure an organization can continue to work with limited down time and have an IT recovery plan as part of the business continuity approach. In this plan, an organization should identify critical data, applications, and processes and define how it will recover IT services that support business operations, products, and services.

Public Safety Canada

Industrial Control System (ICS) Community

Public Safety Canada hosts events to improve the resilience of industrial control systems.

Creating a Cyber Incident Response Plan

Being able respond to cyber threats in a coordinated and effective way is essential. A joint IT/OT Cyber Incident Response Plan can make sure that your organization has the skills you will need to respond to cyber threats. This document outlines a general approach, with specific factors to consider based on your organization's size, function, location, and sector-specific considerations.

Transport Canada

Transport Canada Vehicle Cyber Security Guidance

These guidelines set technology-neutral guiding principles to strengthen cyber security throughout a vehicle's lifecycle. The principles within the guidance will encourage organizations to:

- identify how they will manage cyber security risks
- protect the vehicle systems with appropriate safeguards
- detect, monitor, and respond to cyber security events, and

- recover from cyber security events safely and quickly

Resources from the U.S. Government

United States Department of Transportation - Intelligent Transportation Systems Joint Program Office (ITS JPO) – ITS Cyber Security Research Program

This program was developed to respond to the urgent need to protect ITS from cyberattacks. The program's goal is to share resources, information, and tools with stakeholders to support secure and cyber-resilient ITS.

United States Department of Transportation - Cybersecurity and Intelligent Transportation Systems: Best Practice Guide (FHWA-JPO-19-763)

This report presents the best practices in ITS cyber security, particularly in planning and penetration testing. The report details how to scope a test, including the goals, requirements, success criteria, test type, management, and test readiness. The report includes a test plan template to help local and state transportation department run their own cyber security plan and penetration tests.