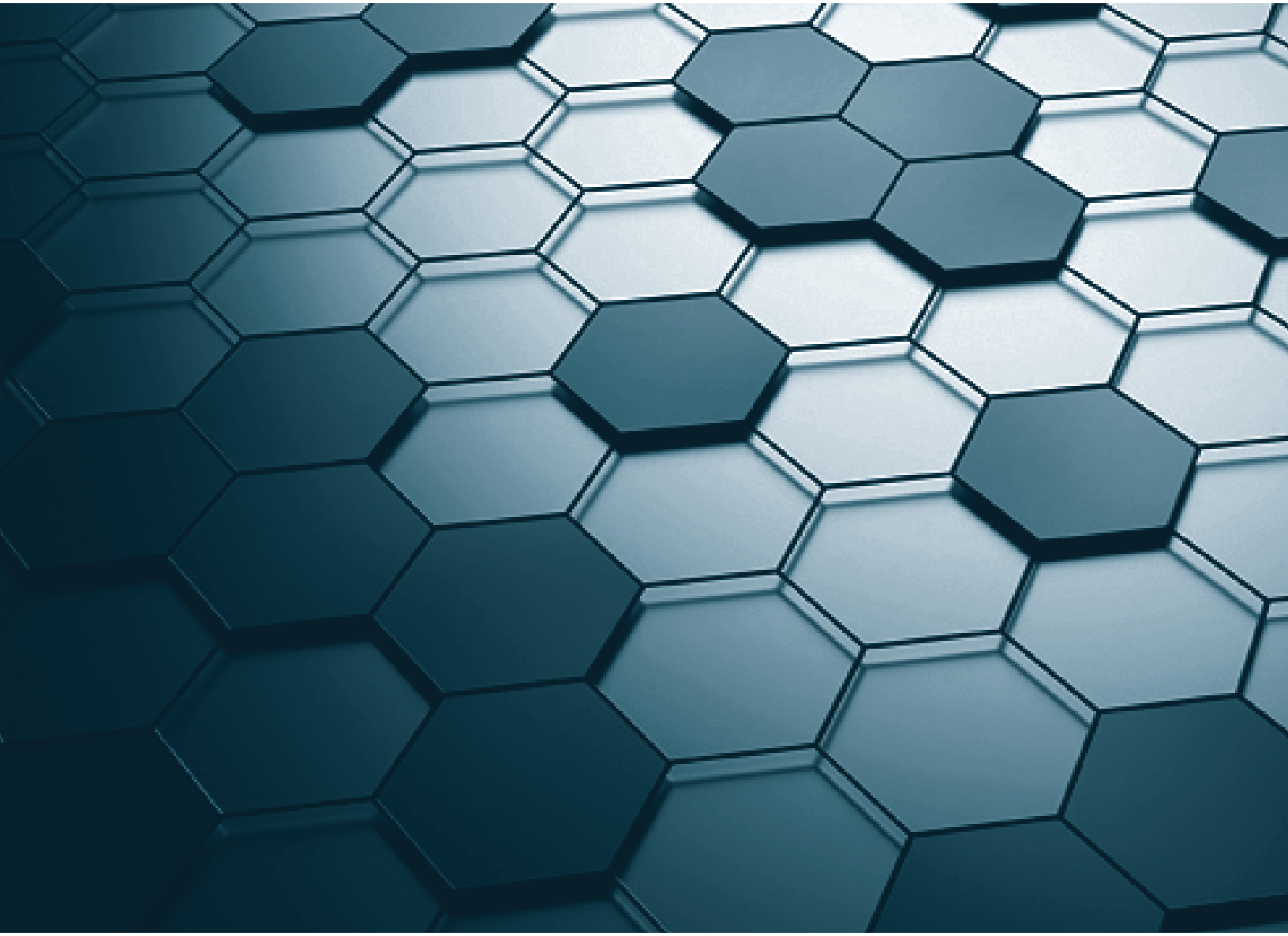
Developing an **Operational Technology and Information Technology Incident Response Plan**



Public Safety Canada
Sécurité publique Canada

Canada

Cat. No.: PS4-267/2020E-PDF
ISBN: 978-0-660-35443-9

Contents

Preamble

The convergence of Information Technology (IT) and Operational Technology (OT) environments is an increasing trend in today's cyber security landscape, and the development of this guidance is intended to inform organizations in how best to respond to this emerging trend. The information contained within this document is intended to be evergreen and will be reviewed and updated as required to meet the evolving needs of critical infrastructure owners and operators in Canada.

This document was a collaborative effort between Public Safety Canada, the Communications Security Establishment and members of the IT/OT working group, which includes members of the following organizations: Agnico Eagle Mines Ltd., Bruce Power, Cameco Corporation, Canadian Nuclear Laboratories, ENMAX Power Corporation, Hydro Ottawa, Independent Electricity System Operator (IESO), Newfoundland Labrador Hydro, Pembina Pipeline Corporation, SANS Institute, SaskEnergy, and SaskPower. This document is also endorsed by Natural Resources Canada (NRCan) as the Energy and Utilities sector lead for the Government of Canada. The advice and guidance in this document however is applicable to any organization that faces the convergence of IT and OT environments.

Executive Summary

While many organizations are equipped with tools and resources that are capable of resolving common IT cyber incidents, there is a growing need to address and mitigate the risks associated with cyber incidents that impact the OT environments of organizations.

As technology becomes more integrated and sophisticated, having the capability to provide a coordinated and effective response to cyber threats across an entire business becomes increasingly essential. A joint IT/OT Cyber Incident Response Plan (CIRP) can ensure that an organization is equipped with the necessary skills and preparedness to respond to cyber threats that arise throughout all technological environments that the organization possesses and utilizes.

“A joint IT/OT Cyber Incident Response Plan (CIRP) can ensure that an organization is equipped with the necessary skills and preparedness to respond to cyber threats that arise throughout all technological environments that the organization possesses and utilizes.”

The information provided in this guideline document is intended to provide organizations who are operating a component of OT in their environment with a framework that can be referenced, applied and leveraged during the development of a joint IT/OT CIRP appropriate to specific business needs. The document provides a general approach, with specific factors to consider based on an organization’s size, function, location and sector-specific considerations.

This guideline offers summary recommendations when creating a CIRP that can be catered to the specific needs of an organization, factors to consider when creating a corresponding Cyber Security Incident Response Team (CSIRT), guidance on how to maintain the CIRP over time, as well as advise on how to think about common OT cyber related threats.

Document Objective

To provide guidelines for establishing a joint Information Technology/ Operational Technology Cyber Incident Response Plan within an organization.

Assumptions

This document makes some assumptions about the state of your organization that need to be taken into consideration:

- A CIRP for IT assets already exists, but is not scoped to include OT/ Industrial Control System (ICS) response protocols; and
- An Organizational Emergency/Crisis Management Plan already exists

Understanding an OT Environment

In establishing a CIRP that covers both IT and OT based assets, it is important to understand what OT assets you may have within your organization. This often means first defining what OT means for your organization. For example whether it includes industrial process control, cameras, computer-based technology infrastructure, non-connected OT devices and/or simply anything that is outside the scope of IT.

Identifying OT Assets

An OT asset can usually be defined as any physical device or software that is used for controlling, monitoring, configuring, collecting information from, or supporting industrial control (or other related) systems. Across industrial-centric organizations, there are both commonalities and distinct differences in each of the systems that need to be considered in order to understand the organizational assets covered by a joint CIRP.

Commissioning a system that includes industrial control components requires Engineering, Electrical, and Maintenance specializations, in addition to the computer-based components that can be potentially disrupted and/or manipulated in a cyber incident. It is important to consider that the same specialists used during commissioning may also be required if the industrial control process is compromised or impacted by a cyber incident.

Organizations utilizing Operational Technology can be large or small in their compositions. Asset inventories and organization risk assessments are keys tools in expanding awareness of the systems that fall under the jurisdiction of a CIRP.

A typical ICS may be comprised of the following technologies:

Protection Systems	Generator Protection Transformer Protection Power Distribution Protection

Supporting Computer-based Technology Infrastructure	Associated Networking Equipment (switches, routers, firewalls) Authentication and remote access systems Log, monitoring and system management servers

Control Systems	Distributed Control Systems (DCS) and components Programmable Logic Controllers (PLC) Systems Turbine Control Systems (TCS) and components Safety Instrumented Systems (SIS)

SCADA, HMI, Data Aggregation, and Engineering Systems	Control Room Systems Human Machine Interface (HMI) Systems and components SCADA Systems and components Engineering Workstations and laptops

Environmental Systems	Continuous Emissions Monitoring Systems

> "...OT systems are not typically designed with cyber security as a priority."

It is important to remember that many of the ICS components listed above may lack basic protection mechanisms, such as strong authentication, authorization, auditing, and input validation, as OT systems are not typically designed with cyber security as a priority. Instead, industrial protocols and systems are often developed for trusted or isolated networks. This puts reliability and availability as the main priorities, without regard for where digital network instructions originate from and without the ability to handle malformed input data. For this reason, it is quite possible for an unsophisticated cyber attack on an ICS system to do a lot of physical damage.

> "What will be the resulting impact to my organization, should this service or system no longer be readily available?"

Cyber Incidents

In order to understand how an organization can better protect and serve its systems, it is important to determine the impacts that cyber based incidents or events could have on these systems prior to an incident occurring. The fundamental question that should be asked in order to effectively address these incidents ahead of time is "What will be the resulting impact to my organization, should this service or system no longer be readily available?"

The following are a few example scenarios that illustrate how dependencies between IT and OT systems can be exploited by cyber incidents, thus resulting in potential negative impacts on industrial organizations. Consider these scenarios when answering the above question:

- Ransomware affects a Windows-based machine, impacting operations at a shipping port. Port technicians are unable to monitor and control critical equipment for port operations, so operations are suspended until the machine can be restored.
- An attacker exploits a company's remote access tools, such as the virtual private network (VPN), and gains unauthorized access to a critical system. The attacker is able to abuse motor controls as a result, and destroys food processing equipment, resulting in a loss of inventory and machinery.
- A disgruntled employee working in a power generation plant abuses the change management system to covertly alter interlock logic settings between programmable logic controllers (PLCs), causing significant damage to equipment and disrupting the plant's operations.

All of the above scenarios have the potential to draw both IT and OT teams into an incident response scenario that would require both groups and systems to organize and work together. These scenarios could have significantly negative impacts on any of the businesses listed above. In situations and events such as these, it is important for organizations to understand the potential ramifications of cyber based disruptions within their area of responsibility, and be able to organize across technology disciplines (IT and OT) effectively in order to provide necessary responses.

Risk Assessments

A Risk Assessment is a valuable tool in developing a more comprehensive understanding of the IT and OT assets that make up an organization. Various assessment options are available, ranging from freely-available open source products such as the Cyber Security Evaluation Tool (CSET)

issued by the US Department of Homeland Security, all the way through to paid services of professional organizations.

Once a comprehensive risk assessment is conducted, it is then important to consider how vulnerabilities may be leveraged or exploited in ways that could cause harm to your organization. In doing so, it is important to consider:

- How will the following be impacted as a result of organizational risks?
  - Equipment
  - Controlled processes
  - Business processes
  - Customers.
- What are the potential attack paths into and across the network?
- What are the organization's network configurations, and how might they be bypassed?
- Are there proper security practices in place, and are they being properly enforced?

Additional considerations:

- Review other examples of real-world OT cyber incidents and the impact they have on businesses (cost, reputation, downtime, etc.);
- Consult relevant security reports from other vendors, industries, and trusted partners; and
- Compare their lessons learned with your own systems to develop more effective solutions.

Understanding the Organizational Structure

Once the role of the OT team is established and the potential cyber impacts to the organization's ICS systems is properly understood, you must then gain a better understanding of the organizational structure, and how a combined IT/OT CSIRT can best function within it.

It should be noted that there is not a one-size-fits-all model that can sufficiently address the unique complexities and considerations of any given organization, and that any approach to the establishment of a dedicated or integrated CSIRT must be reflective of the organization's particular needs and structure.

Organizational Structure

A typical CSIRT consists of two major kinds of resources: (1) Resources that are completely *dedicated* to responding to events; and, (2) Resources with other primary functions that are *later augmented* to respond to incidents as needed (depending on the nature and scope of the event). Organizations should also have roles defined and assigned before an incident occurs, so as to avoid having to develop response procedures whilst dealing with a crisis.

When evaluating the organizational structure, determine all other services and areas that could be associated with or affected by a cyber event or incident in order to better understand all response efforts that may be needed.

Identify any unique characteristics of the systems being served by the CSIRT, such as the team's composition, the physical and geographical

> “Having an understanding of the IT and OT skills currently available within the organization will assist in understanding the assets that need to be organized, which will help in establishing an effective CSIRT.”

location/distribution, and the sector in which the organization operates. The Response Plan structure to be selected will also depend on factors such as:

- Size of the organization;
- Number of geographical locations;
- The systems and platforms that support the organization;
- Incident Response Team (IRT) services that are to be offered; and
- Technical expertise of the existing staff members.

Having an understanding of the IT and OT skills currently available within the organization will assist in understanding the assets that need to be organized, which will help in establishing an effective CSIRT.

CSIRT Members

After developing a clear understanding of the systems that exist within an organization, you should then identify who the CSIRT team members of your organization will be. Consideration must be given to the technical expertise required to perform the specific duties associated with various incident response activities. Choose CSIRT members based on their capabilities, skills and expertise within the organization. Other relevant team members may include representatives from Legal Counsel, Human Resources, Public Relations, Risk Management, Vendors, Law Enforcement and Criminal Investigation groups.

It is also viable to consider outsourcing arrangements, such as managed service providers, maintenance, security operations centres and incident response companies. As technology increasingly relies on multiple disciplines, it is therefore important to ensure ahead of time that their related functions and capabilities are properly integrated into the response plan. Finally, an element or structure for management must be in place to guide the team during instances of crisis. These elements are further explained below.

The CSIRT Manager: The CSIRT manager will be the first person to respond to incidents, and will maintain an ongoing reporting relationship with senior management representatives. This may require reporting to the Chief Information Officer (CIO), Chief Security Officer (CSO), Chief Risk Officer (CRO) or any other equivalent manager. The IRT manager is key in ensuring that all incidents are met with responsibility and accountability, in order to directly manage incidents. While the CSIRT manager is particularly

essential during an incident, they should ensure there is ongoing training, program development and overall general awareness throughout the organization with regards to cyber security and incident response when incidents are not taking place.

IRT Responders: CSIRT Responders may include individuals hired specifically to fill the role of a dedicated IRT member, and will share roles across the organization, outside resources, or a combination thereof. They may also have various skillsets designed to meet the needs of the organization, and should be assigned to roles based on the severity of the event, should they occur. It is important to note that not all CSIRT members are needed for every incident, and the same person might fill multiple roles within the CSIRT, based on the specific considerations of the organization and/or the magnitude of the incident.

Taking a Centralized or Decentralized Approach

The decision to take a centralized or decentralized approach to incident response will depend largely on the structure of the organization in question. Both models are discussed below.

Centralized Approach

A centralized model involves having a close proximity to the constituency, either physically or geographically. In a centralized model, resources are normally located in the same building or complex as the IT/OT assets, and are responsible for all incident-handling activities across the organization. With this model, there is a fully-staffed, dedicated CSIRT that handles all incidents within an organization. This would mean that team members would spend 100% of their time working for the CSIRT. Choosing whether to employ a centralized model would therefore depend on the size and complexity of the organization, and whether the organization is in constant need of dedicated incident responders or not. A larger organization will benefit from a centralized approach, given the general assumption that a larger size will often result in an increased exposure to risk.

Decentralized Approach

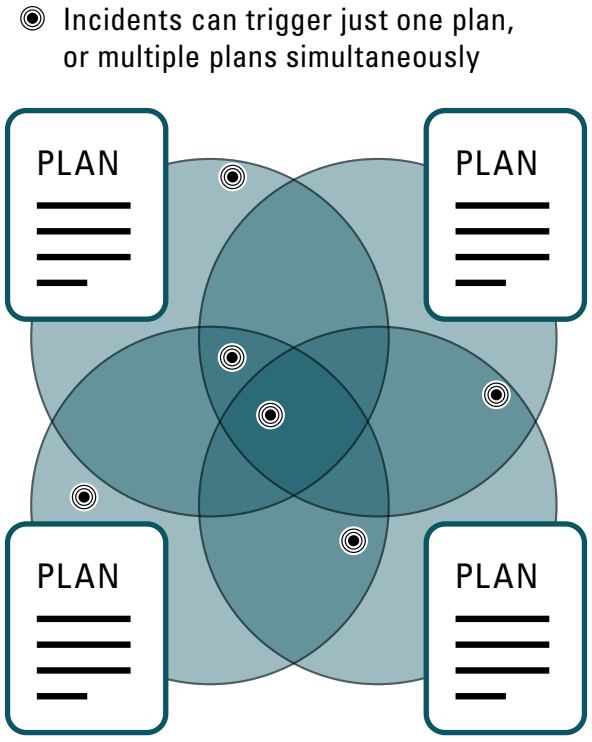
A decentralized model exists when the constituency is located across different buildings, cities, countries, geographic regions or time zones. It requires a different approach than what is required under the centralized model, in that the decentralized model is more flexible and adoptive. An organization utilizing a decentralized model utilizes existing staff members to provide a "virtually distributed CSIRT". Team members often consist of people with primary job roles outside of incident response, with their roles being attributed to a particular skillset, level of expertise, or geographical location. They are called upon to provide support to the IRT when and if an incident occurs.

Organizational Structure Options for CIRP Design

It is possible to structure a joint IT/OT CIRP plan in different ways. Plans can all be connected and can support each other depending on how a technology incident comes into the business. In addition, joint IT/OT plans can be aligned in such a way that they mutually support each other.

As mentioned previously, a CIRP complements and works with other organizational wide response plans such as Crisis or Emergency Plans. In a decentralized organization, it is possible for cyber incidents to vary in their impacts; affecting small areas of a single site to affecting the entire organization from one incident. It is also possible that a technology incident could lead to a company-wide crisis or emergency, or that a crisis or emergency could require a cyber incident response. All of these scenarios require multiple response plans that may reference each other.

An event can affect both the IT and OT spaces. Plans have to work in isolation, but also together when required.



Discovery Through Exercise

An exercise (functional or table-top) may be an effective way to determine the approach that will be needed to properly manage an incident in your organization. This can also help in better understanding how your organization is actually structured, as well as know what capabilities are available to you when responding to an incident. Through exercises, it is possible to determine both the strengths and weaknesses of your organization. Through later analysis, a structure that best fits the particular needs of your organization can then be determined.

> "All organizations are different, and the approach will depend on the specific needs of your business."

When considering whether a decentralized or centralized approach will work better for your organization, keep the following considerations in mind:

- All organizations are different, and the approach will depend on the specific needs of your business;
- Highly distributed organizations may want to consider having individual plans tailored to each business unit that all point to a master company-wide plan;
- More integrated organizations may want to consider having a dedicated IRT, with a centrally-coordinated plan; and
- Table-top exercises are an excellent way to test your plans.

Taking an OT Viewpoint

Differences Between IT and OT Network Systems

While IT and OT have many overlapping and complementary technologies, taking the time to discuss some of the key differences between both systems before implementing a unified CSIRT is recommended.

IT and OT networks differ in infrastructure, technology, vendors, protocols and physical environment, and thus require different types of skill-sets, training and safety requirements. An IT approach to an OT incident might not necessarily be the best solution, if the technology is fundamentally different for each system.

The physical environments of the IT and OT networks are also different. An IT network is often accessed from an office, whereas an OT network tends to be inside an industrial environment. This means that OT networks are typically decentralized and can be located in very remote areas, often times co-located next to the equipment that the network and related devices are controlling.

Information Technology	VS.	Operational Technology
Priority is confidentiality		Priority is availability and integrity
Not time critical		Real time
Latest technology / Frequent upgrades		Proven technology / Infrequently updated
Consumer products		Specialized small market
Patch now		Patch later maybe
Modifications freely permitted – test in field		Modification difficult – prove non-interference, re-qualify, test online
Restart anytime		Restarts planned and coordinated
Online system monitoring and diagnostics		Limited system monitoring and diagnostics
Physical access anytime		Limited access – maybe only during outages
Weak asset tracking and change control processes		Strict regulatory requirements and rigorous change controls
Typically requires access to internet for licensing and updates		Increasing access to internet permitted
Allows remote maintenance and support		Increasing levels of remote access
Impact of failure is person hours		Impact of failure is safety and production
Strong security culture		Strong safety culture

Safety Training

Depending on the environment and the specific requirements of your organization, a CSIRT may be required to certify employees in additional safety training that addresses the specific risks associated with working in an OT-centric environment. Safety training should be maintained wherever possible to assist in reducing the response times of the incident responders who are required to work in OT-based environments.

Ideally, the first time an incident responder is required to wear a hard hat when entering a facility should **not** be when responding to an actual incident. These types of requirements, in this case the need for personal protective equipment, should be considered in the initial development of the team, and taught simultaneously with the training in necessary technical capabilities.

Impact on Resilience

The C-I-A Triad (Confidentiality – Integrity – Availability) of Information Security is often used as a gauge to assess the security of an IT environment. However, in OT environments, there is less of a focus on "confidentiality" as there is a need for lower latency and 100% uptime (i.e., "availability"). The C-I-A Triad also differs for OT environments in that there is *interdependence* amongst organizations, which could have a cascading effect on other systems, stakeholders and even nations. For example, consider the North American power grid, and how it is integrated and connected across different states, provinces and countries. Given this type of interdependence, one incident could have cascading affects across many others.

Due to these key differences, IRTs within an OT network must take into consideration several different geographical, technical, and at times political factors that are unique to an OT environment. Due to this requirement, and especially when dealing with critical infrastructure where often the safety and well-being of citizens is at stake, the following differences related to OT environments should be sufficiently considered:

- **Proprietary nature of technology:** OT hardware/software is often proprietary in nature, requiring incident responders to be familiar with and have experience working in different types of operating environments. Many hardware products are "hardened" or otherwise adapted for different environments or operating conditions, and traditional methods of gathering incident response data may have to be adapted as a result. Consider the fact that the toolkits used for incident response within an IT environment

> “Know your environment, and build your response kits accordingly.”

might not necessarily work for an OT environment for the same reason. Know your environment, and build your response kits accordingly.

- **Product lifecycle:** In contrast to traditional IT-based systems, OT computer-based equipment typically has longer lifecycles, lasting approximately 10-15 years. Therefore, incident response techniques across IT-based systems that are normally more catered to modern operating systems will have to be adjusted when being applied to an OT-based environment. For example, incident responders will need to be equipped with data investigation skills that range from Windows XP to Windows 10, and everything in-between (or earlier!).
- **Incident Response tools and techniques:** Regardless of the environment (IT or OT), any tools and/or processes used for Incident Response must be tested and validated for use within the designated network. OT environments are often very sensitive, and incapable of sustained scanning activity, where the simple execution of a Network Mapper (NMAP) can have dire consequences. Log collection, storage and retrieval is also different across an OT and IT environment. Since this is a primary source when determining the root cause during an investigation, it is important for responders to be familiar with and efficient in the related collection and investigation techniques.

The intent of highlighting the key differences between IT and OT Systems is not to create a division between the two groups, but instead to foster a sense of understanding between the two areas when developing a joint IT/OT IRT. Fostering a culture of understanding and collaboration between the IT and OT groups can be re-enforced through events such as cross-cultural workshops and/or lunches, where each group can present and share information about their reality and gain an appreciation and understanding of the job functions of one another.

Developing the Joint IT/OT CIRP

Once a better understanding of an organization's structure, needs and circumstances is achieved and a decision has been made to move forward with the establishment of a joint IT/OT IRT, the following steps are recommended to stand-up an operational capability:

Step 1: Assemble a Cross-Functional Team

Developing a successful joint IT/OT CIRP requires the participation of key stakeholders working in both IT *and* OT environments in an organization. At this initial planning stage, it is crucial to properly identity and establish the roles of who will currently have or will be given the decision-making authority and capability when responding to a cyber incident. Recommended considerations may include:

- **Reviewing** the organization's crisis and emergency response plans. If they do exist, roles and responsibilities may already be defined, thus negating the need to build from the ground up. If not, further clarification on roles and responsibilities will be required (see step 2 below for more information).
- **Conducting** interviews or workshops with business owners in Engineering, Operations, Senior Leadership, etc., utilizing different containment scenarios to test response effectiveness. Focusing the interviews/workshops on evaluating the impacts to safety and operations may offer further assistance in instances when a clear understanding of cyber security issues is lacking in the context of the organization's OT. Emphasizing the different skill-sets and expertise within each area of the organization can help in bringing different perspectives and contributions to the table. This may help in supporting the incident response, and help to facilitate necessary dialogue that could ultimately assist in the decision-making process.

- **Reviewing** lessons learned from past cyber incidents that occurred within the organization, and leveraging the information gained through past experiences. This can provide valuable context and background on how previous incidents were handled, which can assist in identifying the different roles/teams that are necessary to respond to an OT incident in the future.

Step 2: Review Any Existing Incident Response Plans (IRPs) Within the Team

The primary purpose of this step is to leverage any IRPs that may already exist within the organization, which can often serve as a starting point for the development of a joint IT and OT IRP. It is important to acknowledge that no IRP exists in a vacuum, and that a truly coordinated approach to risk is only achieved through unifying the different capabilities and teams within all levels of an organization. The following steps should be considered when conducting a review of existing IRPs within an organization:

> "...a truly coordinated approach to risk is only achieved through unifying the different capabilities and teams within all levels of an organization."

1. Identify any pre-existing IRPs (physical and/or cyber). These may include response plans related to:
   - IT
   - OT
   - Physical security
   - Emergency or crisis response (health & safety, environment, etc.)
   - Business continuity
2. Host an open discussion, or conduct a table-top exercise that includes relevant security personnel, such as:
   - Chief Information Security Officers
   - Automation Programmers and Process Engineers
   - Information/IT Security
   - Physical security
   - Legal counsel
   - Corporate Communications
   - Other relevant entities, as required
3. Review any existing plans in the context of an IT and OT joint response plan, keeping the following in mind:
   - The organizational definition of an "incident" must be widely understood, while recognizing that something that constitutes an

incident within one domain may not be applicable to an incident that takes place in another;

- It is possible for technology incidents to differ in their level of impact, as they can range from affecting a small area within a single site to affecting an entire organization;
- Incidents can be both physical and cyber, each having the ability to have consequential impacts on one another;
- If a platform or process currently exists to actively and historically track incidents, cross reference it for commonalities;
- Identify if there are any areas where it makes sense to keep IT and OT plans separate from one another, and alternatively, where it makes sense to combine them;
- If the IT and OT response teams are separate, identify if there are any areas where either team can aid the other when responding to an incident; and
- Identify if there are any tools, systems or terms that are used by both IT and OT teams, and determine when and how those shared resources can be utilized to identify any areas of improvement.

4. If no existing IRPs or resources exist within an organization, consider the following options as possible sources of reference:
    - Internet-based IRPs
    - Vendor-provided solutions
    - Templates provided by cyber insurance underwriters.

It is also important to note that some organizations may have "home-grown" or "grassroots" approaches to addressing incident responses. These processes may not necessarily be considered as official organizational policy, but they could reflect what methods and procedures work well for the organization. Should such policies, standard operating procedures (SOPs) or agreements exist, it is essential to review them, so that they can be considered throughout the development of a joint IT/OT IRP.

Step 3: Defining an Incident

It will be important to understand and define what an incident that can kick-off the IRP may look like inside your organization. For example, a small incident that affects a single system will certainly be something to investigate, though it may not necessitate invoking the entire IRP.

In addition, your organization may find it necessary to define the difference between an event and an incident to help in knowing when to invoke the IRP:

- **Cyber event**: Any observable action, behaviour or interaction within a systems environment (ex: Network traffic, system process, or application behaviour)
- **Cyber incident**: Any intentional or unintentional cyber security event that compromises, or attempts to compromise the confidentiality, integrity or accessibility of a system, network, or digital information

Note: Your regulatory framework may have more exact definitions that pertain to your particular environment, and users of this guide are encouraged to consult such material.

The following examples illustrate the difference between events and incidents:

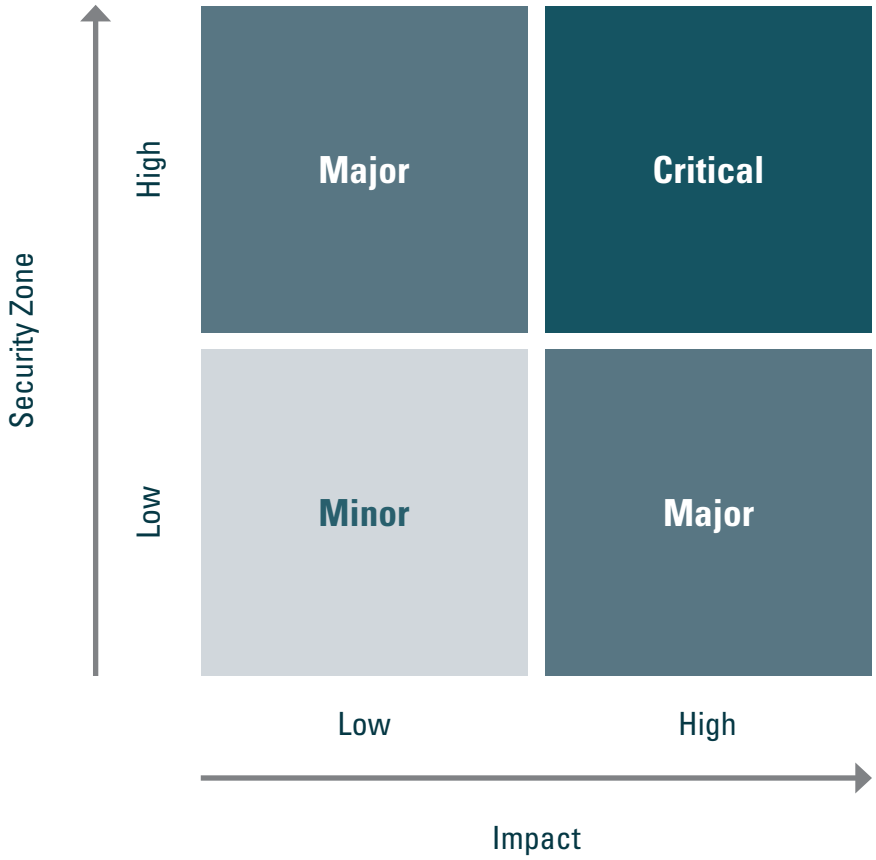
- Examples of cyber **events**:
  - User connected to a file share;
  - User logs into a system;
  - User failed login because of a bad password; and
  - HTTP request.
- Examples of cyber **incidents**:
  - Unusual behavior from a privileged account;
  - Phishing email attempts;
  - Unauthorized network traffic observed by external host; and
  - Violations of change management process.

Classifying Incident Severity

Classifying an incident will help determine whether it is necessary to invoke the IRP. In order to classify an incident's level of severity, the CSIRT should consider the security zone that the incident takes place in, and the impact or potential impact to the organization and/or the surrounding area where the incident is occurring.

The classification matrix shown below demonstrates one way to use the relationship between security zones and impact to determine an incident's level of severity. An organization's IRP should include different methods for responding to different incidents, based on their level of severity, as is illustrated in the following diagram:

IT/OT Incident Severity Classification Matrix



- **Security Zone:** The physical and logical grouping of one or more cyber IT/OT assets having the same (or similar) requirements for cyber security in an organization
- **Impact:** An estimate of the potential or realized losses associated with an identified incident for an organization or for public safety

Step 4: Determine How Teams Will Assemble

This step helps to outline the different teams that should be engaged within a joint IT/OT CSIRT. At a minimum, two major team roles should be chosen to manage an organization's cyber security incidents:

1. The Cyber Security Incident Response Team (CSIRT)
2. The Senior Leadership/Crisis Management Team (SLT/CMT)

The Cyber Security Incident Response Team

The CSIRT should be made up of IT and OT team members with subject matter expertise who can investigate incidents, as well as identify and implement the appropriate containment and remediation actions to resolve them. This team may include (as appropriate) members from:

- Various IT disciplines, including:
  - The IT cyber security team
  - Enterprise architecture
  - IT systems infrastructure (network, server and desktop support)
  - IT Service desk (or Helpdesk)
  - Affected system owners
- OT systems teams, including:
  - The OT cyber security team
  - OT systems infrastructure (network, server)
  - Industrial programmers and OT system specialists (as required)
  - Engineering partners (internal and/or 3rd party)
- Managed Service Providers (as appropriate):
  - Third-party Security Operations Centre (SOC) analysts
  - Cloud service providers (as appropriate)
  - Incident Response partners (ex: forensics specialists)

The CSIRT should have a designated lead (or Incident Commander) who will be responsible for important decision-making and remediating items such as:

- Developing and maintaining cyber security incident response processes, outlining the incident response process, how and when to engage internal and external stakeholders, and when to engage the Senior Leadership/Crisis Management Team (SLT/CMT);
- Defining and assigning roles and responsibilities to CSIRT team members;
- Declaring when an incident has occurred, and invoking the cyber Incident Response process (when required);
- Maintaining the tools required to convene the CSIRT (when required);
- Maintaining the contact information of all members, as well as the SLT/CMT and other external parties (when required);
- Convening the CSIRT, investigating incidents and liaising with relevant stakeholders (when required); and
- Escalating and liaising with the SLT/CMT (when appropriate).

The Senior Leadership/Crisis Management Team

The SLT/CMT serves as the primary liaison needed in the instance of an IT/OT incident. The SLT/CMT works to coordinate communications with external parties, Law Enforcement, other IRTs, senior leadership, Human Resources, the Board of Directors, Legal Counsel, compliance, etc. This team should include (when appropriate) members from:

- Senior IT & OT leadership
- Legal Counsel
    - Provide legal support as required or requested by the CSIRT;
    - Provide guidance to the team with respect to laws and regulations governing the team's operations, and the legal ramifications of particular incidents;
    - Assist in ensuring that evidence collection that pertains to policy violations is properly collected, and a chain of custody is maintained;
    - Provide guidance on data breaches that may have legislative or regulatory compliance reporting mandates; and
    - Ensure that requirements pertaining to cyber insurance are met (if the organization has taken out a cyber insurance policy).

- Finance Department
  - Work with any cyber insurance providers to ensure that cyber insurance coverage services are being utilized, and the claims process is being followed.
- Corporate Communications
  - Provide communications support as requested by the CSIRT (and as approved by the SLT/CMT).
- Human Resources
  - Provide guidance on incidents pertaining to inappropriate use, insider threat, etc. from a human resources perspective.

Step 5: Determine How Teams Will Communicate

Effective communication among all key stakeholders of the organization is a critical element during any type of incident or event. Organizations must establish a common communication plan including escalation thresholds that will ensure appropriate engagement from key stakeholders, ranging from technical support staff to senior leadership teams.

Communication needs will vary for each level of an organization based on the state of emergency, and it is imperative that meeting rooms or conference bridges be designated for emergencies. Alternate forms of communication channels should also be established to facilitate coordination efforts across appropriate levels within the organization.

The organization should maintain the capability to relocate emergency management staff to alternate work locations (if possible), in the instance that primary locations become compromised or made unavailable.

An organization should maintain the understanding that cyber incidents may impact the same digital systems which are relied on for communication under normal circumstances. For example, the underlying network itself may be affected and/or isolated to reduce the spread of a digital virus for protection of other systems, or software collaboration tools may be linked to compromised system administrator accounts, rendering them inaccessible.

The plan should provide several reliable and secure communication *alternatives* for CSIRT participants at each level. It should include specific instructions available for each alternative in the event that the primary communication methods become unavailable during the incident (i.e., the internet or e-mail system is shut down).

Examples of alternative communications include, but are not limited to:

1. A secure web portal on public internet with separated authentication systems;
2. Secondary and tertiary Internet connections, such as cellular or satellite;
3. E-mail with predetermined incident response distribution lists;
4. Internet-based collaboration systems and/or audio conference bridges;
5. Mobile phones;
6. Land lines (or POTS, "plain old telephone service");
7. Satellite phones; and
8. VHF/UHF radio systems.

The organization should define specific protocols and procedures for local site staff, and designate a local Incident Commander (i.e., person on the ground), in case the communication with central incident command becomes impaired.

Certain thresholds must also be defined, and the delegated decision authority for various conditions should be clearly identified for an autonomous remote cyber security incident response. The CSIRT should establish predetermined communication templates, and offer appropriate guidance on the type and level of information to be provided to each of the following forums: technical teams, middle managers, senior leaders, industry partners, CERT, public etc. Appropriate review and approval protocols should also be established to allow information to be released to other participants, partners, and stakeholders, as they relate to the incident and the potential resulting impact.

Step 6: Determine Necessary Response Actions

The main objective for this step is to determine the nature of any cyber incident or event that occurs in an ICS environment, and to outline appropriate responses aimed at prioritizing the safety of people and the reliability of industrial operations during an incident. The following information should be considered when establishing or conducting cyber incident responses within an industrial setting.

Note: This guide assumes that ICS networks, including SIS (Safety Instrumented System), are already properly segmented from business networks, and that Incident Response tools have been tested to ensure safety of use on the ICS, and that a defensible cyber position has been established and tested.

Triaging the Threat(s)

ICS incident response personnel need to quickly triage and identify the scope of an incident as soon as it occurs. This includes first understanding what type of threat(s) are being dealt with, the behavior of the threats, potential vectors, and the potential goals of the threat. This will help in determining the appropriate response actions needed. Forensic data will be quickly collected (2-5 hours) and analyzed (2-5 hours) to determine the nature of the threat, and how to approach containment and eradication steps. Analysis of the data would consist of dynamic malware analysis and static property file analysis, with more detailed reverse engineering occurring at a later stage. Evidence should also be collected from critical ICS assets first, usually prioritizing:

- PLCs (checking if ladder logic was recently changed and identifying the deltas from previously obtained digital hashes of project files);
- Data Historian account or process changes (Data Historians are a hot spot used for adversaries to pivot from);
- Microsoft Windows HMIs; and
- Remote access logs (such as RDP, VPNs, etc.).

> "ICS incidents are rarely short, and it may take days or weeks to defend against future attacks."

In addition, determine if additional resources (internal and/or external) are required to defend through the attack. ICS incidents are rarely short, and it may take days or weeks to defend against future attacks. Personnel count, shifts and logistics should be considered based on your current security team, as well as any outsourced incident response services to augment your response capabilities.

Establishing a Defensible Cyber Position for ICS Incident Response

Tools used for ICS incidents include data acquisition software/hardware for forensic analysis of operating systems, engineering field device data and network traffic captures, and are key to any effective defensive strategy. It is important to test any tool prior to an actual incident occurring, not only to assess the capability, but also to assess the impact. The goal of a defensible cyber position is to isolate operations as much as possible when feasible, to ensure there is a reduced impact of potential threats to operations. This could mean disconnecting from IT business networks, an OT DMZ or business applications, or segmenting within an ICS (i.e., disconnecting process A from process B). It is important to test a defensible cyber position prior to execution, perhaps through an incident-handling exercise through part of a scheduled test. A subset of the defensible cyber position could lead to operations running in manual operations – without the assistance of stand-alone Windows-based HMIs, but rather working from built-in

HMIs such as those embedded into ICS assets via on-device panels, or running in full manual operations with disconnected network segments to further isolate ICS plant network(s).

Communications During Incident Response

During an incident, an analysis and/or impact assessment should be presented to key stakeholders of the ICS process, with seasoned process engineering staff in the room to provide the impact analysis. Stakeholder engagement is essential to ensure the coordination and feasibility of response, if security recommendations are to affect and/or change ICS operations as the incident(s) unfold. This allows all parties involved to establish a clear understanding of the incident, and allows for necessary communication that can help to ensure the safety of all on site(s).

Note: **Containment** can occur safely, yet **eradication** may have to wait until the next scheduled operations outage. If this is the case, additional monitoring may be required to ensure that threat remain contained.

Scoping & Environment Changes

The Initial Triage will ideally provide indicators of compromise (IOCs). These may include command and control IPs, ports and protocols used by the threat, or file behaviors or indicators and process information that can in turn be used for defensive and preventative action. IOCs are used to block operations (if not impede them), to scope out any potentially impacted assets/networks, and to identify any threat vectors. IOCs and any identified behaviors from the triage analysis should be used directly to apply countermeasures on all applicable cyber security layers. These countermeasures could include blocking ports on switches on the plant floor, adding FW rules to deny IOCs, disabling (i.e., further hardening) services that are not in use currently, segmenting networks logically, or completely disconnecting remote access during an incident response. All actions taken should consider the potential impact that they will have on operations and the safety of the site workers and the plant.

Making the Decision to Affect Operations

Disruptions of ICS operations should only occur when there is an imminent threat to the system, or when a threat exists that affects loss of control, loss of operations monitoring, disruption to operations, or the ability to manipulate operations. Facility stakeholders and/or primary decision-makers should always be in the room prior to changes in the ICS process site(s). Consider logical changes before considering physical changes. For

example, consider changes such as implementing additional firewall rules, disabling the RDP (Remote Desktop), and/or adding tighter ACL (access control lists) before considering disconnecting physical cables, unless equipment being disconnected or changed is already a part of your tested defensible cyber position.

Step 7: Determine How the CIRP Will Fit With a Crisis Management Plan

The primary purpose of this step is to leverage any Corporate Crisis Management Plan (CMP) or Emergency Response Plan (ERP) that may already exist within your organization, and link it with the Joint IT/OT CIRP.

As stated earlier in this document, these plans, should they exist, may also provide a good starting point for the development of a Joint IT/OT CIRP. By implementing integration points between the CIRP, the corporate CMP and site ERP, the organization will have an improved response capability during an incident.

The following should be considered when conducting a review of existing CMP and ERP within an organization:

1. Review definitions for what constitutes a crisis or emergency
    - Incorporate new definitions if OT cyber incidents are not adequately covered already
    - Modify existing content if an aspect of the OT environment is missing
2. Review roles and responsibilities within the crisis management plan
    - Ensure that there is an OT Cyber Breach Coordinator who can act as a liaison between the CIRP and the Crisis Management Team;
    - If an IT Cyber Breach Coordinator exists, negotiate options within the plan; and
    - Add new responsibilities to existing roles to further assist capacities in the event of an OT cyber incident.
3. Review how the CMP and ERP are invoked
    - Update the CIRP with information on how to escalate an OT cyber security incident to the crisis management plan; and
    - Update the corporate CMP and ERP to include context on what to expect during an OT Cyber Security Incident Response.

4. Include the Crisis Management and Emergency Response Teams on any updates to the plans, options including:
    - Table-top exercises; and
    - Training meetings.

The CIRP should work together with the CMP or EMP. This will ensure that all the necessary internal and external partners are properly considered, and that their roles and responsibilities will be adequately covered. Depending on the severity level of the incident, a cyber security incident can be a type of crisis or an emergency. Even though the cyber security IRP has its own remediation steps, many of the roles and responsibilities within the CMP are required, such as Legal Counsel consultation and Public Relations consultation.

It is possible for a cyber security attack scenario to create unsafe conditions at a facility, which could create a crisis. A CMP should have a process in place to safely shut down the facility if this occurs. In order to achieve this, individuals with specific knowledge of facility's safety requirements will be required to properly respond to cyber security incidents of this magnitude. The crisis management team is given the authority to make business decisions associated with the impact of the incident. Whether the CIRP is a standalone document or part of the CMP, both should be designed to work harmoniously together.

Maintaining the Joint IT/OT CIRP

Establishing a joint IT/OT CIRP is not a "set it and forget it" type of exercise. Once a plan is in place, it will need to be continually maintained in order to remain relevant.

Assuming dual leadership, as is typically the case with IT and OT leadership, the custodians of the response plan should reside in both environments, and advocate for one another's role. In order to achieve this, the following approach is recommended:

- Have regular incident response review meetings to keep IRT members informed of recent events and incidents;
- Keep management informed of the meetings and their outcomes, and give them a sense of your preparedness. Share meeting outcomes with management and subject matter experts (SMEs);
- If you have built a response team matrix of SMEs from various areas within your organization and these team members may be activated at any time, it will be important to rotate them through your weekly or bi-weekly meetings, to ensure that they maintain their situational awareness of the environments that they support;
- Be prepared to exercise your plan;
    - Run regular communication checks with your responders/ SMEs. Be creative; you may have all the contacts accurately documented, but they may not be available to respond, or their designated alternates may not be aware of their expected availability;
    - Conduct periodic table-top exercises to validate procedures and communications (less frequent, but on a regular basis so as to allow for greater participation);
    - Be prepared to educate new members of the organization (as required); and

> “A fatal flaw in any exercise allows for learning of the same lessons again during an actual incident.”

- After an exercise, ensure that relevant findings are captured in a “Lessons Learned” document, and that actions are taken to ensure weaknesses and vulnerabilities are resolved and/or addressed. A fatal flaw in any exercise allows for learning of the same lessons again during an actual incident.

- Clearly delegate an authority to change the plan when necessary, and define what must be communicated and to whom, as well as when it should occur; and
- Communicate. Prepare checklists. Promote the plan and inform others of its whereabouts (with access controls of course). Keep a printed copy with controlled access.

Conclusion

This guideline has been created with the intent of providing organizations currently utilizing OT with the necessary understanding of the importance of implementing an IRP that can better target the unique implications affecting OT systems. By applying this guideline in the context of a particular organization that has already been equipped with IT functionalities and capabilities, it will allow for better preparation and defense against future cyber related threats and incidents that may arise in both information and operational technologies.

This guideline's analysis of the types of OT assets that may be vulnerable to cyber threats within an organization helps educate organizations on the importance of ensuring that OT systems are sufficiently protected. It also offers important information and guidelines to consider that will equip IRTs with sufficient capabilities that are needed to address and mitigate the risks associated with OT cyber incidents. By providing a range of factors that an organization must consider based on unique organizational features and operational circumstances, organizations can be better prepared for future cyber related OT incidents that IT-specific IRPs are incapable of adequately addressing.

Glossary

Centralized Approach – A model of structuring an organization's incident response capabilities, based on the size, structure and unique specifications of that organization. Requires the CSIRT to dedicate all of their time and resources towards incident response within the organization.

Chief Information Officer (CIO) – The senior executive tasked with managing and overseeing the IT strategy and other computer systems utilized and relied upon by an organization.

Chief Risk Officer (CRO) – The senior executive tasked with identifying, managing and mitigating internal and external risks to the organization.

C-I-A Triad – The three components associated with network security. Requires network systems to include elements of confidentiality, integrity, and availability.

Crisis Management Plan (CMP) – An pre-defined process that an organization follows when addressing a crisis or incident.

Crisis Management Team (CMT) – The elected bodies of an organization tasked with overseeing the Crisis Management Plan and mitigating the risks associated with cyber threats and incidents.

Cyber Incident Response Plan (CIRP) – A pre-defined process that an organization will refer to during and prior to cyber incidences that threaten any technological systems or resources utilized by the organization.

Cyber Security Evaluation Tool (CSET) – A product developed by the Department of Homeland Security that assists organizations in protecting their cyber assets.

Cyber Security Incident Response Team (CSIRT) – A team of dedicated incident responders that are tasked with addressing and mitigating both IT and OT cyber incidents if and when they occur within an organization.

Chief Security Officer (CSO) – The senior executive responsible for the physical security of an organization, who oversees the protection of its people, assets, infrastructure and technology.

Decentralized Approach – A model for structuring an organization's incident response capabilities, based on the size, structure and unique specifications of that organizations. Allows incident responders to have

roles outside of the CSIRT, where they are only called upon for incident response in the event of an incident.

Distributed Control Systems (DCS) – Systems that use multiple controllers, computers, and sensors across an infrastructure or plant to facilitate control.

Emergency Response Plan (ERP) – A pre-defined process that an organization follows in the event of emergencies. Includes required actions, resources, procedures and protocols.

Human Machine Interface (HMI) – Provides a textual or graphical view of a system and its operations, allowing for more extensive monitoring, control, status reporting and other functions.

Incident Response Plan (IRP) – A plan that helps you prepare for and prevent security incidents.

Incident Response Team (IRT) – An incident response team is a group of people—either IT staff with some security training, or full-time security staff in larger organizations—who collect, analyze and act upon information from an incident.

Industrial Control System (ICS) – Control systems associated with instrumentation utilized for industrial process control. Include devices, systems, networks and controls used to operate and/or automate industrial processes.

Indicators of Compromise (IOCs) – Computer signatures that identify potentially malicious activity on a system or network.

Information Technology (IT) – The application of hardware and software to maintain and resolve organizational network and computer systems.

Network Mapper (NMAP) – A free open-source network scanner used to discover hosts and services on a computer network by sending packets and analyzing the responses.

Operational Technology (OT) – The application of hardware and software designed to manage, monitor and control industrial operations and assets.

Plain Old Telephone Service (POTS) – A standard and basic telephone service that offers connection to the telephone network for many residential and small businesses throughout the world.

Programmable Logic Controller (PLC) – A specialized computer device used for ICS, typically relied on for automation of industrial electrochemical processes in the control of machinery.

Remote Desktop Protocol (RDP) – A protocol designed to facilitate the remote control of networked hosts.

Safety Instrumented System (SIS) – A system responsible for ensuring the safety of a plant or organization that identifies when risky conditions occur and acts accordingly to avoid accidents inside and outside the facility.

Security Operations Centre (SOC) – A centralized unit within an organization that deals with technical and security issues.

Senior Leadership Team (SLT) – A team of executive officials of an organizations, including those at the highest levels of management who are responsible with managing and overseeing its operations.

Supervisory Control and Data Acquisition (SCADA) System – A collection of multiple computers, interfaces, systems, and networking configuration used to govern and control an ICS environment or plant.

Turbine Control Systems (TCS) – Unique control systems designed for turbine control.

Ultra High Frequency (UHF) – A commonly used radio frequency more suited for indoor environments, often used by schools, warehouses and retail stores.

Very High Frequency (VHF) – A commonly used radio frequency more suited for outdoor environments, often used for outdoor professions such as forestry and oil.

Virtual Private Network (VPN) A private network that gives you online privacy and anonymity by creating a private network from a public internet connection. VPNs mask your internet protocol (IP) address so your online actions are virtually untraceable. Most important, VPN services establish secure and encrypted connections to provide greater privacy than even a secured Wi-Fi hotspot.