Security Management in the North American Electricity Sub-Sector

A Guideline

September 2016
## Table of Contents

Preface ........................................................................................................................................ iv
Executive Summary ....................................................................................................................... v
Preamble .......................................................................................................................................... v
Introduction ................................................................................................................................... vii
  Definitions ................................................................................................................................... vii
  External References ...................................................................................................................... vii
  Additional Reference Material ..................................................................................................... vii
Security Management Program .................................................................................................... 4
  Governance ................................................................................................................................... 4
  Implementation .............................................................................................................................. 4
  Competence ................................................................................................................................. 4
  External Relationships .................................................................................................................. 4
  Internal Relationships ................................................................................................................... 4
Automated Tools .......................................................................................................................... 6
Security Strategies ......................................................................................................................... 5
  Introduction ................................................................................................................................ 5
  Security Strategy - General ........................................................................................................... 5
  Copper Theft Prevention Strategy ................................................................................................ 5
  Antiterrorism Planning Strategy .................................................................................................. 6
Security Risk Management ........................................................................................................... 5
  Definitions .................................................................................................................................. 5
  Principles of Security Risk Management ...................................................................................... 5
  Risk Strategies ............................................................................................................................ 6
  Sources of Risk ............................................................................................................................ 6
  The Risk Management Process .................................................................................................... 7
  Security Risk Management Model ............................................................................................... 8
Design Basis Threat ....................................................................................................................... 12
Physical Security .......................................................................................................................... 13
  Available Sub-Sector Resources .................................................................................................. 13
  Security Measures Selection ......................................................................................................... 13
  Guards ....................................................................................................................................... 14
  Mobile Patrols .............................................................................................................................. 14
  CCTV ......................................................................................................................................... 15
# Table of Contents

Fence Line Intrusion Detection System (FIDS) ................................................................. 16  
Intrusion Detection System (IDS) .................................................................................. 16  
Locks ............................................................................................................................. 16  
Lights ............................................................................................................................ 17  
Alarms ........................................................................................................................... 17  
LIDAR ........................................................................................................................... 17  
Fence/Wall .................................................................................................................... 17  
Personnel Security ....................................................................................................... 18  
Introduction .................................................................................................................. 18  
Access Control ............................................................................................................ 18  
Background Checks and Personnel Risk Assessments .................................................... 21  
Security Considerations for Employee Terminations .................................................... 24  
Information Security .................................................................................................... 29  
Information Asset Management .................................................................................... 29  
Information Storage ...................................................................................................... 30  
Disclosure of Information ............................................................................................. 31  
Information in Motion .................................................................................................... 32  
Information Systems Security ....................................................................................... 33  
Industrial Control Systems Security .............................................................................. 34  
Security Information Sharing and Communications .................................................... 35  
NERC CIPC .................................................................................................................... 35  
NERC CIPC’s Electricity Information Sharing and Analysis Center (NERC E-ISAC) ..... 35  
Canadian Electricity Association’s Security & Infrastructure Protection Committee (CEA SIP) .................................................................................................................. 36  
Canadian Cyber Incident Response Centre (CCIRC) .................................................... 36  
Physical Security Incident Response and Investigation ................................................ 37  
Incident Response ........................................................................................................ 37  
Investigations ............................................................................................................... 38  
Cyber Incident Response and Investigation ................................................................ 44  
Introduction .................................................................................................................. 44  
Preparation .................................................................................................................... 44  
Communications .......................................................................................................... 45  
Documentation ............................................................................................................. 45  
Composition of the Computer Incident Response Team (CIRT) ................................. 46  
Identification ............................................................................................................... 47
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Containment</td>
<td>47</td>
</tr>
<tr>
<td>Eradication</td>
<td>48</td>
</tr>
<tr>
<td>Recovery</td>
<td>48</td>
</tr>
<tr>
<td>Lessons Learned</td>
<td>48</td>
</tr>
<tr>
<td>Annex A to Cyber Incident Response Plan – Incident Handler’s Checklist</td>
<td>49</td>
</tr>
<tr>
<td>Fraud Prevention</td>
<td>51</td>
</tr>
<tr>
<td>Governance</td>
<td>51</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>51</td>
</tr>
<tr>
<td>Prevention</td>
<td>52</td>
</tr>
<tr>
<td>Detection</td>
<td>53</td>
</tr>
<tr>
<td>Investigation and Corrective Action</td>
<td>54</td>
</tr>
<tr>
<td>Qualifications, Training and Awareness</td>
<td>55</td>
</tr>
<tr>
<td>Security Leadership</td>
<td>55</td>
</tr>
<tr>
<td>Skills &amp; Experience by Position</td>
<td>56</td>
</tr>
<tr>
<td>Security Awareness Training Tools</td>
<td>59</td>
</tr>
<tr>
<td>Electricity Sub-Sector Safety Awareness Training Tools</td>
<td>59</td>
</tr>
<tr>
<td>Regulatory Compliance</td>
<td>63</td>
</tr>
<tr>
<td>NERC</td>
<td>63</td>
</tr>
<tr>
<td>NERC Critical Infrastructure Protection Standards</td>
<td>63</td>
</tr>
<tr>
<td>Change Management and Continuous Improvement</td>
<td>64</td>
</tr>
<tr>
<td>Performance Measurement</td>
<td>64</td>
</tr>
<tr>
<td>Evaluation and Review</td>
<td>64</td>
</tr>
<tr>
<td>Management of Corrective Action</td>
<td>65</td>
</tr>
</tbody>
</table>
Preface

The **North American Electric Reliability Corporation (NERC)** is a not-for-profit international regulatory authority whose mission is to assure the reliability of the bulk power system (BPS) in North America. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the BPS through system awareness; and educates, trains, and certifies industry personnel. NERC’s area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. NERC is the electric reliability organization (ERO) for North America, subject to oversight by the Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada. NERC’s jurisdiction includes users, owners, and operators of the BPS, which serves more than 334 million people.

The North American BPS is divided into eight Regional Entity (RE) boundaries as shown in the map and corresponding table below.

*The North American BPS is divided into eight Regional Entity (RE) boundaries. The highlighted areas denote overlap as some load-serving entities participate in one Region while associated transmission owners/operators participate in another.*

<table>
<thead>
<tr>
<th>FRCC</th>
<th>Florida Reliability Coordinating Council</th>
</tr>
</thead>
<tbody>
<tr>
<td>MRO</td>
<td>Midwest Reliability Organization</td>
</tr>
<tr>
<td>NPCC</td>
<td>Northeast Power Coordinating Council</td>
</tr>
<tr>
<td>RF</td>
<td>ReliabilityFirst</td>
</tr>
<tr>
<td>SERC</td>
<td>SERC Reliability Corporation</td>
</tr>
<tr>
<td>SPP RE</td>
<td>Southwest Power Pool Regional Entity</td>
</tr>
<tr>
<td>Texas RE</td>
<td>Texas Reliability Entity</td>
</tr>
<tr>
<td>WECC</td>
<td>Western Electricity Coordinating Council</td>
</tr>
</tbody>
</table>

Founded in 1891, the **Canadian Electricity Association (CEA)** is the national forum and voice of the evolving electricity business in Canada. The Association contributes to the regional, national and international success of its members through the delivery of quality value-added services.
CEA is governed by a Board of Directors comprised of senior executives from its Corporate Utility Members. CEA offers members a broad range of innovative programs and services in addition to delivering a coherent and convincing industry viewpoint to decision makers on critical policy and regulatory issues.

CEA members generate, transmit and distribute electrical energy to industrial, commercial, residential and institutional customers across Canada every day. Members include integrated electric utilities, independent power producers, transmission and distribution companies, power marketers and the manufacturers and suppliers of materials, technology and services that keep the industry running smoothly.

**Contributors to this document include:** Travis Moran, Navigant; Chris McColm, Manitoba Hydro; Mike Thebault and Sheldon Cooke, both of Emera; Jeff Pringle and Jim McGlone, both of the Department of Energy; Scott Yost, EPCOR; Shawn Eck, The Empire District Electric Company; Sandy Gosselin, Cam Fischer, and Ross Johnson, all of Capital Power; and the Canadian Electricity Association’s Security & Infrastructure Protection Committee.

Comments, suggestions, or questions about this document should be directed to Ross Johnson, CPP at rjohnson@capitalpower.com or (780) 405-5542.

**Executive Summary**

This document is a joint product between North American Electric Reliability Corporation’s (NERC) Critical Infrastructure Protection Committee, the Electricity Information Sharing and Analysis Center’s (E-ISAC) Physical Security Advisory Group, and the Canadian Electricity Association’s (CEA) Security and Infrastructure Protection Committee. This product was developed by NERC and CEA members to share and enhance industry practices that help to maintain Bulk Electric System reliability. The guideline is voluntary and does not create any mandatory obligations. It is not intended to establish new requirements under NERC’s Reliability Standards, to modify the requirements in any existing reliability standards, nor provide an interpretation of any NERC Reliability Standard.

The purpose of this guideline is to provide a framework for comprehensive security protection of the electricity sub-sector in North America. This guideline applies to owners and operators of electrical generation, transmission, and distribution facilities in North America.

**Preamble**

It is in the public interest for the North American Electric Reliability Corporation (NERC) to develop guidelines that are useful for maintaining or enhancing the reliability of the Bulk Electric System (BES). The Technical Committees of NERC; the Operating Committee (OC), the Planning Committee (PC) and the Critical Infrastructure Protection Committee (CIPC) per their charters are authorized by the NERC Board of Trustees (Board) to develop Reliability (OC and PC) and Security Guidelines (CIPC). These guidelines establish a voluntary code of practice on a particular topic for consideration and use by BES users, owners, and operators. These guidelines are coordinated by the technical committees and include the collective experience, expertise and judgment of the industry. The objective of this reliability guideline is to distribute key best practices and information on specific issues critical to maintaining the highest levels of BES reliability. Reliability guidelines are not to be used to provide binding norms or create parameters by which compliance to standards is monitored or enforced. While the incorporation and use of guideline practices is strictly voluntary, the review, revision, and development of a program using these practices is highly encouraged to promote and achieve the highest levels of reliability for the BES.
Introduction

Both Canada and the United States recognize energy - oil, gas, and electricity - as critical infrastructure. Each of these three energy components are listed as separate sub-sectors, but of the three, electricity is the one commodity that allows all other critical infrastructure sectors and sub-sectors to operate. Electricity is the critical interdependency for modern society.

Security management in the electricity sub-sector is particularly complex. Electricity sub-sector assets are concentrated in small areas and distributed over large areas; they are manned and unmanned; they involve dangerous conditions and forces that an unaware public must be protected from; and they provide a resource to the public that enables the quality of life we enjoy today.

Protection of these assets requires security managers to use every tool in the toolbox. Security managers have to consider protecting physical property, cyber assets, employees, and the public. Priorities must be established that respect the needs of the public and the organization being protected, and the protection programs that follow must be as efficient and cost-effective as possible.

This is a guideline, not a Standard. It is intended to be used by security managers in the electricity sub-sector when designing their own security management programs or as a checklist to ensure they are covering the areas they need to and that nothing is overlooked. There are a number of NERC and E-ISAC products already available, and whenever possible the reader will be steered towards them to ensure we get the maximum benefit from that good work.

Definitions

The Glossary of Terms used in NERC Reliability Standards is the source for most definitions used in this guideline. The Glossary is found here on the NERC website.

Definitions may also be found within individual sections of this document.

External References

- NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security

Additional Reference Material

- ASIS International General Security Risk Assessment
- ASIS GDL IAP 05 2007 ASIS International Information Asset Protection Guideline
• ASIS GDL PBS 09 2006 ASIS International Pre-Employment Background Screening Guideline
• ASIS GDL PSO 11 2004 ASIS International Private Security Officer (PSO) Selection and Training Guideline
• ASIS GDL WPV 09 2005 ASIS International Workplace Violence Prevention and Response Guideline
• ANSI/ASIS CSO.1-2013 Chief Security Officer – An Organizational Model, 2013
• ANSI/ASIS/RIMS RA.1-2015 Risk Assessment, 2015
• ANSI/ASIS INV.1-2015 Investigations, 2015
• ANSI/ASIS SCRM.1-2014 Supply Chain Risk Management, 2014
• Headquarters, Department of the Army, FM 3-19.30 Physical Security
• IAEA Nuclear Security Series No. 10 Development, Use and Maintenance of the Design Basis Threat – Implementing Guide
Security Management Program

Governance

General
The purpose of a security management program (SMP) is to ensure that the organization creates and maintains the policies, standards, and procedures necessary to ensure that all applicable aspects of the security domain are adequately covered.

Accountability
Governance of the SMP should include:

- Senior management accountability
- Roles and responsibilities for all aspects of the SMP, including requirements, development, review, continuous improvement, and approval
- Responsibility and resourcing for the maintenance of the SMP
- An enabling security policy that provides direction, accountability, and oversight for the SMP
- Implementation and awareness training for all employees to ensure maximum effective use of the SMP

Implementation
Implementation of a documented SMP assists the owner/operator in ensuring that all security threats to operations are effectively identified and managed.

Competence
Please see the section on Qualifications, Training, and Awareness for additional information on the qualifications and training appropriate for persons involved in the development and implementation of a security management program.

External Relationships
External relationships are important to security management to ensure that we learn from each other’s mistakes and that we share information that can be used to protect us. While our companies may compete, our security departments do not – we support each other in our efforts to ensure the safety of our people and the resilience of the Bulk Power System.

Our external relationships also include:

- NERC Critical Infrastructure Protection Committee
- NERC Electricity Information Sharing and Analysis Center
- The Canadian Electricity Association Security & Infrastructure Protection Committee
- Federal law enforcement and intelligence agencies
- Local law enforcement
- Other security partners in the sub-sector and in industry

When working with security contractors, we ensure that they are aware of their responsibilities under the security management program.

Internal Relationships
Alignment with internal organizations may be necessary when implementing a security management program. A partial list of internal stakeholders includes:
• Facilities managers
• Contingency planners
• Finance
• Human Resources
• Safety
Automated Tools

Many aspects of physical security are automated. Typical examples are:

- access control systems
- intrusion detection systems
- fence line or perimeter intrusion detection systems
- building management systems, such as heating, air conditioning and elevator control
- automated barriers and bollards
- lighting controls
- fire detection
- CCTV
- intercoms
- security alarms
- power monitoring
- ground surveillance radars
- electronic communications systems

Physical Security Information Management (PSIM) is software that combines the inputs from these systems into a single user interface to both control the sensors or inputs and provide a common operating picture.

PSIM software should provide the following capabilities:

1. **Collection** of information from input systems
2. **Analysis** of the information to determine the situation and allocate a priority
3. **Verification** of information to reduce false reporting
4. **Resolution** aids, such as Standing Operating Procedures to walk responders through the steps required to resolve the incident
5. **Recording** of information for compliance reporting, training, and investigation
6. An **audit trail** to record system inputs and the associated response

The field of computer security relies on a category of software called Security Information and Event Management (SIEM). The capabilities of SIEM systems typically include:

1. **Data aggregation** from many sources
2. **Correlation** of information to find common attributes and package the information
3. **Alerting** to notify personnel of security events
4. The use of **dashboards** to help in understanding steady and changing states
5. The gathering of information to prove **compliance**
6. **Retention** of historical data
7. **Forensic analysis** to assist in investigations

A third category of software combines both PSIM and SIEM capabilities.
Security Strategies

Introduction
There are a number of security issues common to all organizations in the electricity sub-sector. Experience has taught us that some approaches are more effective than others. It is very important that each organization take a hard look at the threats and risks that it faces and determine the strategy that would be most effective for them after considering resources, training and experience.

Security Strategy - General
At the highest level, in physical and cyber security, the strategy that we tend to employ today is:

1. **Harden our security posture** – we conduct threat vulnerability assessments to determine our security requirements, and develop and deploy security measures to achieve our security goals
2. **Security awareness** – we promote security awareness amongst our employees and contractors to reduce the risk of accidental breach while at the same time recruiting them as extra ears and eyes to watch for unusual events that could be an indicator of an adversary’s interest
3. **Reactive to proactive** – we work together in industry and professional groups and alongside law enforcement and intelligence agencies to learn of, share, and protect our organizations from threats before they show up at our gates or firewalls.

Copper Theft Prevention Strategy
Copper theft is a safety issue, and should be treated as one. Equipment can be rendered unstable by removal of the grounds, which makes it dangerous for our people to work on it. Thieves cut holes in fences, and children can be exposed to harm if they enter the site. Finally, the thieves themselves are often victims.

Copper theft can also badly impact construction schedules. Some of the copper cable used in substations and switchyards is purpose-made, and is normally not available on the shelf. It can take weeks to make new cable, and if the installation of the cable is on the construction project’s critical path then the project could be delayed.

Discuss copper theft with your safety department, and enlist their support. Ask electrical construction workers to include copper security in their safe work plans, to ensure that they have ample time in each work day to ensure that all copper cables and fittings are properly disposed of. What you would like them to do is:

1. **Clean up** all copper scrap from the worksite at the end of the day
2. **Bury all copper cable**. If there isn’t time to bury a cable before they leave at the end of the day, then they should wait until the next day to lay the cable and fill in the trench
3. **Remove all loose copper** from the worksite at the end of the day. It should go back on the truck, and be stored at the service yard overnight

The easiest way to reduce the threat of copper theft is:

- **Don’t use it**. The most commonly-stolen and accessible copper in a substation is normally the fence or equipment grounding wire. There are two options:
  - **Use non-conductive fencing**. It doesn’t need to be grounded
Use CopperWeld. This is a grounding product made of copper-clad zinc, and it has no commercial value at a recycler. If you choose to use CopperWeld, ensure that you clear it with the electrical engineers responsible for the equipment you are protecting, and put up plenty of perimeter signs to warn would-be thieves that what they are going to steal is not welcome at the recyclers’

- Bury it. If the thieves can’t see it, they will find it challenging to steal
- Mark it. Have a stamp engraved with your company name or logo, and stamp all copper fittings. Ask the company which makes your copper cable to include a strand marked with the name of your company. Inform the metal recyclers in your area and local law enforcement that your copper is marked so they will know to look for the identification mark if they see any copper they suspect may have been stolen. Most recyclers are honest, and all they ask is that we mark our copper so that they can identify it as stolen
- Work with Law Enforcement. Local law enforcement agencies may not know the threat to public safety that copper theft creates. They will need to know how to value the loss – if it is only based on the scrap price of copper, it will always be petty theft. If they understand the cost of replacement, the work involved, and the cost to customers of an outage then they can charge copper thieves more appropriately when they catch them

**Antiterrorism Planning Strategy**

As a critical infrastructure sub-sector, we may be a target of terrorists determined to interfere with the normal functioning of society and to send a message to the public that they government cannot be relied upon to protect them.

First, though, a couple of useful definitions:

- **Antiterrorism**: passive measures designed to reduce the likelihood of terrorist attack. Activities related to antiterrorism are undertaken by the private sector, or government facilities not directly involved in the counterterrorism fight
- **Counterterrorism**: those active measures undertaken by law enforcement, the intelligence community, militaries and diplomats which are designed to hunt down and neutralize terrorist groups. This is almost always within the jurisdiction of governments

The interaction between terrorist groups, antiterrorism planners, and counterterrorism forces is described in Figure 1, and explained below.
Terrorist attacks are characterized by: very short duration; routine activities of authorities; little warning; and a quickly developing threat. These characteristics compensate for the overwhelming weakness of most terrorist groups - their inability to fight a sustained battle with government forces - which drives their absolute need to achieve surprise at their objective.

The best way for a terrorist group to achieve surprise is by thorough knowledge of the objective. What security measures are in place? What is the routine? Where are the weak spots in the perimeter? Are there any gaps in security? How do they handle visitors? Couriers? Deliveries? VIPs? Are they actively watching outside the perimeter? Where is the closest law enforcement or military post? How long would it take for an organized force to arrive at the objective? What is the routine of local police? The more information that a terrorist group can collect the more certain they will be of success.

To enhance the likelihood of success, terrorist groups follow their own routine:

- **Broad Target Selection**: a list of potential targets based on the intended target of the message
- **Intelligence and Surveillance**: information collected from all sources, including cursory surveillance
- **Specific Target Selection**: a comparison of the choices from the broad target list resulting in a decision on which one to attack
• **Pre-Attack Surveillance and Planning**: the collection of detailed information needed to successfully attack the objective

• **Attack Rehearsal**: usually conducted in a remote location free of unwanted observers

• **Escape and Evasion**: often necessary even in the case of suicide bombers, as there may be other terrorists nearby the bomber acting as spotters, photographers, or handlers

The message that security managers need to send terrorists is simple: *You will not be successful here*. To do this, we need to engage terrorists during their two information collection phases (Intelligence and Surveillance and Pre-Attack Surveillance and Planning).

Antiterrorism planning follows a routine as well. There are five distinct elements:

• **Threat Vulnerability Assessment**: an honest and thorough evaluation of the likely terrorist threats to a facility or organization. This assessment is usually site-specific, so a site in an area that has a past history of terrorist groups who possess both the capability and the intentions of attacking targets similar to your own facility will have a higher threat than a facility in an area with no known history of terrorist activity. An accurate threat vulnerability depends on good relations with local counterterrorism forces, as their intelligence input is often crucial to an accurate assessment. The Design Basis Threat document available from the E-ISAC would be a useful document in this phase, but it is only a start, and you should always include liaison with local counterterrorism authorities

• **Security Measures**: a collection of measures that allow security managers to increase or decrease the application of security measures in consonance with the perceived threat level. These measures usually include static and mobile armed or unarmed security guards, closed-circuit television cameras, fences or walls, barbed or concertina wire, gates or other vehicle barriers, and procedures for access control of employees, visitors, and deliveries

• **Observation**: a systemic process, called surveillance detection, that involves watching the most likely locations that terrorists will collect information on the target from, including a mechanism for collecting useful information on unusual or suspicious activities and reporting it to someone in a position to act on it – usually security management and local counterterrorism forces. This supply of information is very important to counterterrorism, as often the first hard indicator of terrorist interest is in the targets they choose to watch. Inclusion of counterterrorism forces at this stage allows them to begin their operational cycle through countersurveillance (identifying, investigating and following surveillants) – hopefully disrupting the terrorist group long before they get to the attack itself

• **Random Antiterrorism Measures**: a collection of unannounced additions to security measures which, when implemented singly, will change the security posture of the facility in a way that cannot
be predicted by an observer. These measures are intended to introduce doubt into the terrorist planning cycle, hopefully reducing its attractiveness as a target.

- **Response Planning**: Predetermined actions to be taken in the event of discovered surveillance, attack, fire, explosion, etc. Prompt response to all unwanted or unforeseen events will enhance reaction time and effectiveness, minimizing consequences and reducing the perceived value of the target to terrorists.

To work effectively, antiterrorism planners and counterterrorism forces cannot operate in isolation from each other. Effective liaison is required - antiterrorism planners need to meet with their counterterrorism counterparts on a regular basis, sharing information.¹

Security Risk Management

Security risk management is the forecasting and evaluation of security risks together with the identification of procedures to avoid or minimize their impact.

Definitions
Threat – Actions, circumstances, or events that may cause harm, loss, or damage to your organization’s personnel, assets, or operations.

Risk – The combination of impact and likelihood for harm, loss, or damage to your organization from exposure to threats.

Resilience – The ability to prepare for and adapt to changing conditions, and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

Security Risk Management (SRM) – An analytical process that considers the operational context of the organization and the risk of unwanted events that might impact personnel, operations, and assets, with the aim of developing strategies that reduce risk by reducing the likelihood and impact of these events.

Security Risk Assessment – (SRA) A process that includes:
  - Identify those threats which could affect personnel, assets, or operations
  - Determine the organization’s vulnerability to those threats
  - Determine the risk by assessing the likelihood and impact of the threats
  - Prioritize risks
  - Identify methods and strategies to reduce the likelihood and impact of the risks

Principles of Security Risk Management

Unity of Effort
Risk management efforts should be coordinated within the organization and will all partners and stakeholders, such as government, regulators, law enforcement, and if necessary, the local community.

Transparency
Information on how risk decisions are made should be shared with all that have a valid need to know, both inside and outside the organization.

Adaptability
Risk management strategies and processes should be designed to allow for constant change.

Practicality
Risk managers cannot predict the future, nor can they eliminate all threats. They must be practical in what they choose to protect.

Customization
Solutions must meet the needs and respect the culture of the organization.
Risk Strategies
There are four general strategies for dealing with risk:

1. Accept the risk – choose to accept the risk, and budget for the consequences that are likely to flow from that decision
2. Avoid the risk – Choose not to undertake the risky activity
3. Reduce the risk – Design controls to reduce the likelihood or the impact of the risk. Any remaining risk is referred to as ‘residual risk’
4. Transfer the risk – The potential negative impact of this activity is shifted to a third party, either through insurance or contract language

Sources of Risk
Internal
Internal sources of risk include employees, contractors, or visitors. The types of activity they may be engaged in include: theft of money, equipment, or information; sabotage or vandalism; espionage, workplace violence, and collaboration with outside attackers.

External
External sources of risk include: criminals (thieves, kidnappers, vandals, saboteurs, fraudsters); terrorists, espionage, and workplace violence.

Environmental
Environmental risks generally include flooding, fire, severe storms, or earthquakes.
The Risk Management Process
This process is based on ISO 31000 Risk Management.

Diagram 1: ISO 31000 Risk Management Process
Diagram 2: Security Risk Management Model

Program, Activity or Facility Assessment

Threat Assessment

Vulnerability Assessment

Impact ↔ Likelihood

Risk

Control/Mitigation Measures
(accept, avoid, reduce likelihood, reduce impact,

Decision Making
(establish priorities, funding, resources)

Prepare and Implement Control Measures

Review and Update
Communications and Consultation
This is key to successful security risk management. You should include all stakeholders, partners, and customers. Discussions should be consistent and two-way, and include certainties, uncertainties, perceptions, and tolerance for loss.

Establishing the Context
Considerations in this step include:

- The goals and objectives of the risk management process must align with the goals and objectives of the organization
- What is the mission and values of the organization you are protecting?
- What is the scope and criticality of the risk management decision you are making – what must you protect?
- Who are the decision-makers and stakeholders?
- What is the decision timeframe?
- What are your risk management capabilities and resources?
- What is your organization’s tolerance for risk? (Warning – this must be determined by senior management)
- What is the availability and quality of the information available to you?

When you have gathered the information above, design the process by which you will determine:

- What exactly do you need to protect? Do you need to protect the entire facility, or just the critical parts? How do you determine what is critical?
- Identify the risks – internal, external, and environmental
- Conduct a risk assessment and analysis
- Select, implement, and evaluate risk management alternatives

Risk Identification
What might happen, and why?

- Consider a wide variety of risks
- Use ‘risk to’ and ‘risk from’ logic. \textit{(For example, the risk to our substations comes from copper thieves)}
- Create a broad list of potentially adverse outcomes
- Include the full range of probabilities (likely to highly unlikely) – not just the most likely risks
- Understand that you’re not going to capture them all – we make up for this ambiguity later when we design our security measures and resiliency strategies
- Develop scenarios to assess and analyze risks. Ensure that the scenario set covers the full scope of the assessment
- Scenarios should not overlap – multiple scenarios that contain the same event may lead to double-counting the risk
A scenario is a “hypothetical situation comprised of a hazard, an entity impacted by that hazard, and associated conditions including consequences…”

- DHS Risk Lexicon, 2010 Edition

**Risk Analysis**
What are the consequences?

- Gather and validate information
- Consider all internal, external, and environmental risks
  - Are there groups or individuals present with the history, capabilities, or intention to harm your organization?
  - Are there conditions present which may harm your organization?
- Assess the impact of safety, the environment, reputation, and material assets
- Rate the consequence as one of the following:
  - Insignificant
  - Minor
  - Significant
  - Major
  - Severe

**Risk Evaluation**
What is the likelihood (or probability) of the event happening?

- How often has this event happened before:
  - To your organization?
  - To similar organizations in your area?
  - To similar organizations farther away?
- Are there factors present that will make this event more likely?
- Are there factors present that will make this event less likely?
- Rate the likelihood of the event occurring from the following list:
  - Rare
  - Unlikely
  - Moderate
  - Likely
  - Almost certain

**Plotting the Results**
Plot each risk on the risk analysis table at the intersection of its consequence and likelihood. (See Table 3: Risk Analysis Table)
Table 3: Risk Analysis Table

After the risks are plotted on the risk analysis table, they are prioritized from high to low based on the score.

For example:

If the likelihood of copper theft at a substation is ‘Likely’ and the consequence is ‘Minor’ then the risk is at the intersection of the likelihood row and the consequence column is ‘Medium.’ The score for that risk is eight. (Scores are particularly useful when prioritizing alike risks – a Medium with a score of nine has a higher risk rating than a Medium with a score of five.)

If the likelihood of gunfire at a substation is ‘Moderate’ and the consequence is ‘Major,’ then the risk is ‘High.’ The score for that risk is 12.

Based on the scoring of the two threats in our example, the gunfire threat is accorded a higher priority for treatment than the copper theft threat.

Risk Treatment
Start with the highest risks, and work down the list from there.

Options include:

- Accept the risk, and the consequences that come from it
- Avoid the risk by not undertaking the risky activity
- Reduce the risk by reducing either the likelihood of it happening, or by reducing the impact if it does happen. (This is where our security measures come into play.)
• Transfer the risk by insuring against the loss, writing protection into contract language, or hiring others who are better suited to manage the risk

**Execution Phase**

**Decision time:**

• Establish priorities of work, obtain funding, determine available resources, determine timetable for implementation

• Prepare and implement control measures – security design, policies and procedures, and contingency plans

• Review and Update – periodically review your security risk assessment to ensure that no material factors or assumptions have changed
Design Basis Threat

A Design Basis Threat (DBT) is a formal document that describes the threats that an asset should be protected from. Often used in the nuclear power industry, the definition used by the International Atomic Energy Agency is “A DBT is a comprehensive description of the motivation, intentions and capabilities of potential adversaries against which protection systems are designed and evaluated. Such definitions permit security planning on the basis of risk management. A DBT is derived from credible intelligence information and other data concerning threats, but is not intended to be a statement about actual, prevailing threats.” (IAEA Nuclear Security Series No. 10 Development, Use and Maintenance of the Design Basis Threat – Implementing Guide)

A DBT for the electricity sub-sector has been completed by the E-ISAC’s Physical Security Advisory Group (PSAG). The PSAG is comprised of over 20 electricity industry security professionals from the United States and Canada, private and public sector SMEs, and the US Department of Energy. Combined, the PSAG possesses over 600+ years of physical security experience. The DBT is available to registered members through the E-ISAC Portal.

NERC members are encouraged to consult the DBT as part of their security planning process. It is not intended to cover all the facility-specific threats and assets that may need to be considered (theft, safety of personnel, workplace violence, exposure to dangerous chemicals, etc.). It is expected that owner/operators of individual facilities may need to apply protection measures beyond the DBT to cover all the hazards and threats as identified by their assessments.
Physical Security

Available Sub-Sector Resources
The NERC Security Guideline for the Electricity sub-sector: Physical Security is an excellent resource, and is available here at NERC.com. Additional information is also available from the NERC Security Guideline for the Electricity sub-sector: Physical Security Response Guideline. It is available online here.

The North American Transmission Forum has released a document called NATF Practices Document for NERC Reliability Standard CIP-014-1 Requirement R4. It covers security measures, includes a physical security plan template, and has a section on physical security technologies and resources. It is available here.

The NATF Practices Document for NERC Reliability Standard CIP-014-1 Requirement R5 covers security measures, includes a physical security plan template, and has a section on physical security technologies and resources. It is available here.

Both NATF documents are tailored for CIP-014-2 Physical Security, which is a standard which applies to certain transmission stations, transmission substations, and associated primary control centers. The NATF documents contain security information which would be of value to anyone interested in protecting electric sector assets.

Security Measures Selection
Security measures are actions, obstacles, or policies that protect an organization. The three main goals are:

- Where possible, identify and deny access to potential threat actors
- Deny unauthorized access to the facility for weapons, explosives, and dangerous chemicals
- Deter unwanted behavior and mitigate the actions of both hazards and threats

Security measures achieve these goals through a combination of one or more of the following functions:

- Access Control
- Deterrence
- Delay
- Detection
- Assessment
- Response
- Evidence Gathering

The selection of security measures for a facility should cover all of these seven functions.

<table>
<thead>
<tr>
<th>Type</th>
<th>Access</th>
<th>Deter</th>
<th>Detect</th>
<th>Delay</th>
<th>Assess</th>
<th>Respond</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guards</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Mobile Patrols</td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

Security managers should seek to deploy the least intrusive measures required by the ambient threat, and should increase measures in consonance with an increase in the threat.

Static security measures can be overcome by an adversary through careful observation, planning and preparation. Because of this, security measures should be flexible, changing, and unpredictable. If an adversary cannot predict what a facility’s security measures will be, then they will be less likely to attack.

**Guards**

Guards are the most flexible and the most expensive of all security measures. They are first-rate in situations that require assessment and decisions, and they are a very good deterrent.

Most organizations use contract security guard companies for their guard service needs. There are a number of advantages to this: if you need more guards, the company can provide them quickly; if one doesn’t show up, it is their problem, not yours; you are spared the cost overhead and person-years involved in full time employees, and the guard company is responsible for training. Guards can do the one thing that no other security measure or system can do: they can **think**.

The negative side of using guards is that they are usually poorly-paid, so there is usually a high-turnover rate and a corresponding lack of commitment; they may not have the same level of safety awareness as the rest of your employees, so their Total Recordable Injury Frequency Rate (TRIF) may be higher than your company, and may have an impact on your safety statistics; and as they are human, they are prone to mistakes like anyone else.

If you do elect to use guards, pay them as much as you can get away with, negotiate the contract carefully and hold them to it, and monitor it closely to ensure annual pay increases are passed on to the guards. Treat the guards as if they were your own employees to foster commitment, and treat them with respect. They are likely the poorest-paid people in your company, and they do important work for you.

**Mobile Patrols**

Guard patrols are done by one of three methods: by vehicle; on foot; or by CCTV camera. (Theoretically a guard post can be considered a standing patrol.) Of the three, the mobile vehicle patrol covers the most ground, acts as a greater deterrent, and is the most responsive. The advantage of a foot patrol is that they can look more closely – a cut in the fence is likely to be seen by a foot patrol, whereas since vehicle patrols are restricted to roadways there is a good chance they won’t see it.

A CCTV patrol is where the guard performs a scan of a facility using the CCTV cameras in a thorough and organized fashion. The advantage of a CCTV patrol is that it is quick; if the cameras are sited correctly, it is

<table>
<thead>
<tr>
<th>Security Measures</th>
<th>CCTV</th>
<th>FIDS&lt;sup&gt;6&lt;/sup&gt;</th>
<th>IDS&lt;sup&gt;7&lt;/sup&gt;</th>
<th>Locks</th>
<th>Lights</th>
<th>Alarms</th>
<th>LIDAR&lt;sup&gt;8&lt;/sup&gt;</th>
<th>Fence/Wall</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

<sup>6</sup> Fence Line Intrusion Detection System
<sup>7</sup> Intrusion Detection System
<sup>8</sup> Light Detection and Ranging
thorough; and it is inexpensive, as your guards aren’t burning gasoline and spending time traveling between sites. The disadvantage is that it is not an additional visible deterrent beyond that which the CCTV cameras already provide.

**CCTV**

CCTV is one of the most commonly-used security measures today. It is a powerful resource: it is used to identify people in access control systems; it’s overt presence acts as a deterrence to criminals and terrorists; it can detect security threats and breaches; it can be used in automated change detection and self-learning systems; it allows security officers to assess a suspected event to determine if law enforcement support is required; and it makes excellent evidence to support a subsequent prosecution. CCTV cameras are IP-addressable and their images can be stored on Network Video Recorders (NVR), which allows users to access CCTV images from corporate networks or remotely over the Internet. Prices on CCTV systems continue to drop as their image quality improves.

Depending on the jurisdiction, your company may be required to write a policy on the use of CCTV cameras. The following is a generic policy. If you choose to use this template, ensure that you have the finished product approved by your corporate legal department.

---

**Video Surveillance Policy**

**Purpose:**

This Video Surveillance Policy applies to operations in all locations where (PARENT COMPANY) operates in (COUNTRY). The purpose of this policy is to ensure that (PARENT COMPANY)’s use of overt and covert video surveillance is carried out appropriately, complies with applicable legislation, and is treated confidentially. (PARENT COMPANY)’s video surveillance system includes mechanical, electronic, digital or wireless systems that enable continuous or periodic video recording, observing or monitoring of space and activities. It is intended to:

- support a safe environment for (PARENT COMPANY) employees and to help protect (PARENT COMPANY)’s assets;
- discourage misconduct or unlawful behavior at (PARENT COMPANY) sites;
- assist with responding to incidents or threats; and
- assist with investigating alleged unlawful activity, misconduct or breaches of (PARENT COMPANY)’s policies.

**Use of Overt Video Surveillance**

Camera equipment, including closed-circuit television cameras or digital video recording devices, may be installed at (PARENT COMPANY) sites when (PARENT COMPANY)’s Physical Security and applicable business unit management have determined it is reasonable and necessary for the safety and security of (PARENT COMPANY) personnel and/or property.

The field of view of the surveillance camera equipment will be limited as much as is reasonably possible to ensure that only (PARENT COMPANY) sites are monitored and the camera does not monitor areas where there is a reasonable expectation of privacy, such as change rooms or washrooms.

Signs saying that video surveillance is present will be conspicuously placed near entrances to and around the perimeter of (PARENT COMPANY) sites when overt video surveillance is being used.

**Use of Covert Video Surveillance:**
Covert or hidden surveillance camera equipment will only be used if there is reasonable cause, in extraordinary circumstances and when other less invasive options are not available. The reasons for using covert surveillance will be documented and permission to proceed must first be given in writing by (PARENT COMPANY)’s Chief Executive Officer, or his or her designate. The use of covert surveillance and the collection of personal information will be limited to only what is necessary to achieve the documented purpose.

**Video Surveillance Equipment:**

Only (PARENT COMPANY) security employees, security contractors and/or employees authorized by (PARENT COMPANY) security employees will have access to equipment used to gather data through video surveillance. This equipment will be stored in a secure manner and will be placed in an access-controlled area. Data on storage devices will be deleted after 30 days unless needed for investigation or legal purposes. Obsolete storage devices will be securely destroyed by overwriting, shredding, or magnetically erasing the information.

**Access to Video Images**

Only people with a legitimate business or legal reason to view or receive the images captured by video surveillance will be given access to those images.

**Contacts**

Questions about this Policy, or how it applies, should be directed to the:

- (PARENT COMPANY)’s Senior Manager, Physical Security and Emergency Management or
- (PARENT COMPANY)’s Privacy Officer

---

**Fence Line Intrusion Detection System (FIDS)**

Fence line intrusion detection systems will detect and alarm when someone climbs or cuts the fence. They are usually connected via software to the CCTV camera system, and will point cameras at the site of the suspected intrusion.

The advantage is that if someone is trying to penetrate your fence, you will get warning and can call for law enforcement. The problem is that the intruder may not take long to get through your fence, and by the time law enforcement arrives the attacker has finished his work and left.

**Intrusion Detection System (IDS)**

Intrusion detection systems are typically found at doors and windows of permanent structures. They are similar in deployment to FIDS, and they have the same shortcomings. It is important that they be backed up by CCTV – police will usually not respond to an alarm unless a security officer has verified that it is a real, and not false, alarm.

**Locks**

Locks may be mechanical or electro-mechanical in nature. If mechanical (keyed) locks are used, then ensure that you have a good key control regime. Also, buy locks that are durable enough to protect what you want to protect – the gate of an expensive substation should not have a ten-dollar lock on it. You should specify ‘high-
security' locks with boron shackles and shackle guards. If it doesn’t cost two or three hundred dollars, then it is likely not a particularly secure lock.

Electro-mechanical locks usually use electromagnetic force to hold a door shut. They are activated by a card reader or PIN pad.

**Lights**

Lights are excellent security measures. They provide illumination for your guards and CCTV cameras, and their presence is often a deterrent in itself. They can be installed so that a proximity sensor or your FIDS turns them on, which warns a potential intruder that he may have been spotted, so he will leave the area. Have them installed by a professional consultant, as adequate illumination and coverage is important and technical in nature.

**Alarms**

Alarms can be useful as a deterrent – if an intruder triggers an audible alarm, there is a good chance that they will abandon the attack and leave. If there is no physical response to back up an alarm, though, or if it is not timely, then an attacker will learn that too, and the alarm will be less useful.

**LIDAR**

Light Detection and Ranging is a relatively new technology which uses non-visible spectrum laser light to detect and range objects. It works equally well in day or night, and in periods of reduced visibility. It functions similar to radar, and allows the operator to see an intruder before he reaches the fence line. The cost and functionality is favorable compared to FIDS. LIDAR is an emerging technology in the security field, and it may be a challenge to find a vendor.

**Fence/Wall**

A fence or wall is the most basic security measure. Most security fencing will not keep a fit and agile intruder out for more than a few seconds, but that’s not the point. A fence or wall clearly demarcates a boundary across which an outsider cannot cross without permission, so anyone found inside the fence that doesn’t belong there is subject to trespassing laws. (If there were no fence, an intruder could claim that he wandered onto the property in error, and you would have little reason not to believe him.) A fence or wall helps you keep the honest out, allowing you to concentrate on the dishonest.

There are two main differences between fences and walls. A wall costs more, but hides the interior of whatever it is you’re trying to protect, which may please the neighbors. It blocks the wind, though, which may be a consideration if you’re relying on wind power to cool your transformers. If you are protecting anything that relies on wind cooling, you will need to discuss this aspect with the engineers.
Personnel Security

Introduction
A personnel security program includes all the elements required to ensure the safety of personnel at work. This includes:

- **Access Control** – used to ensure that only trusted personnel have unescorted access to company facilities
- **Background Checks and Personnel Risk Assessments** – used to ensure that all personnel who have unescorted access to your facility are worthy of your trust
- **High-Risk Terminations** – required for the protection of Human Resources staff in the event of a high-risk termination
- **Travel Security** – personnel traveling in unfamiliar cities or countries will be at a higher risk of misfortune

Access Control

Principles of Access Control
The principles of access control are:

1. **Trusted Access**: Only persons who are trusted by the organization should have unescorted access to the facility or its information. This trust is built through the use of background check programs.
2. **Least Privilege**: Personnel should only have access to the minimum information and physical areas that they need to effectively do their jobs.
3. **Complete Perimeter Coverage**: The access control system is only as strong as its weakest point, and the access control system must consider both physical and cyber domains in order to ensure complete coverage. The back door must be protected as well as the front.
4. **Protection in Depth**: Areas of increased sensitivity or criticality may need additional layers of access control in order to ensure that only authorized personnel may gain unescorted access.
5. **Employee Engagement**: Employees must be trained and encouraged to enforce all access control policies. The most effective access control systems in the world can be instantly rendered useless by an employee holding the door open for an untrusted person.

Types of Access Control
Access control systems can be characterized by mode:

- **Passive**: Security screening of employees, contractors, and vendors. Security screening may include criminal background checks, drug use testing, and financial responsibility checks. (Please see the CEA Personnel Risk Assessment Guideline for further information.)
- **Active**: Security screening as per Passive (above) with the addition of technology and/or security guards to restrict access to designated areas to authorized personnel.

Access control systems are further characterized by type:

- **General Access Control**:
assumes that if a cleared person is escorting someone, then that person is also permitted
suitable for many employee work spaces
entry eligibility is usually proven with an access control card and an electronic card reader
this system is prone to ‘tail-gating,’ where an unauthorized person follows an authorized person through the door

• **Positive Access Control:**
  - Uses technology or security guards to ensure that every person who enters a restricted area is checked to ensure that their entry has been approved by the proper authority
  - Commonly used in sensitive or commercial areas, such as airports, cinemas, and high-security government facilities
  - ‘Tail-gating’ eliminated through the use of guard supervision, rotating entry doors, etc.

Access control may be achieved through a variety of processes and technologies. They include:

• Security guards
• Identification cards
• Turnstiles and mantraps
• Biometric readers
• Magnetic or Radio Frequency Identification (RFID) cards coupled with automated access management systems
• Locked doors with key control

**Design Considerations**
The following subjects should be considered before designing and implementing an access control system:

• **Risk:** What is the risk to the organization that is being mitigated with the access control system? Will a simple perimeter system suffice, or are there areas of increased sensitivity which will require additional protection?

• **Regulation:** Are there any regulations which require the use of access control systems, and do they impose any specific requirements which my force you adopt one approach over another?

• **Authority:** Who is the central authority for the access control system? Are they involved with:
  - Security
  - Information Systems logical access approval
  - Industrial Control Systems logical access approval
  - Background checks and Personnel Risk Assessments
  - Access Control Card issuing
  - Access control systems maintenance
  - Emergency response management
  - Payroll and/or Contractor Management (if necessary)
• **Scale:**
  - Are you protecting a single facility, several facilities, or the full enterprise?
  - How many doors or gates are you required to protect at each site?
  - Are any of the sites unmanned?
  - What kind of audit capability is required? Will you require CCTV and video storage? How long will you be required to store the audit logs and video for?
  - Will it be used to control access to a facility during a shutdown or turnaround?

• **Culture:** How effective an access control system will your company’s culture support?

• **Executive Support:** Do you have the support of your company’s executive? They will be using it as well, every day, so you must have their support.

• **Cost:** Access control systems can be very expensive. How much money are you willing to spend?

• **Time:** How much time do you have? In the case of larger, enterprise projects, can you phase it in over several years?

• **Technology:** What are the most cost-effective options available?

• **Emergency Response:** Can the access control system support emergency response measures? For example, is it necessary for the access control system to provide a ‘real-time rollcall’ of personnel remaining inside a facility in the event of an evacuation?

• **Employee or Contractor Time Management:** Will the access control system be used to determine the amount of time onsite for employee or contractor billing purposes?

**Policy and Procedure Requirements**
An organization implementing an access control system will require the following policies and procedures:

• An access control policy which details
  - Who is allowed unescorted access
  - Who is responsible for authorizing access
  - If an access control card is used, how it is to be worn
  - Actions that employees should take if they see a person who does not have a valid access control card

• A procedure for obtaining an access control card

• A personnel screening policy

• A personnel risk assessment procedure (Please see the CEA Personnel Risk Assessment Guideline for further information)

• Expiry or renewal of access

**Selection and Installation of an Access Control System**

1. Select a project team. The team should include members from Security, Information Systems, Industrial Controls Systems, Operations/Facilities, Legal, and Supply Chain Management
2. Consider and decide on the issues raised during the design considerations phase
3. Consult with similar organizations to gather an understanding of products, vendors, implementations, and challenges
4. Create a Request for Proposal and submit to at least three (preferably more) potential providers
5. The project team will consider the responding bids and choose a successful vendor
6. Supervise installation of the access control system
7. Conduct acceptance testing using the criteria developed by the project team

**Background Checks and Personnel Risk Assessments**

The process should include the examination of criminal records, identity verification, credentials, and educational verification, as well as verification of previous employment. Background checks may be done upon hiring, and may be redone periodically if required by regulation.

The following is an outline to assist in planning and implementation of a personnel risk assessment process and policy.

**Planning**

1. Identify positions in the organization that require criminal record checks and identity verification. This may include personnel that require unescorted access to facilities or electronic access to systems. Many entities choose to background check all new hires.

2. Develop mechanism to flag “risk” positions for additional scrutiny during the personnel risk assessment process. (For example, a position that involves handling cash or which confers access to confidential customer data may require more detailed credit and reliability checks.)

3. Develop policy for discussion and subject to approval (consider getting a legal opinion.)

4. Determine who will own the policy and process, such as Human Resources or Corporate Security, and determine where the information will be stored. Some entities criminal record checks will be stored in a secure location.

5. Some entities may hire external third party to conduct the criminal record checks or to conduct investigations in-house. In some entities a third party will conduct the criminal background check and Human Resources will conduct the references and education verification.

6. Provide executive management with a recommendation for implementation and/or presentation of the new policy.

7. Communicate with Human Resources and Union Representatives to discuss implementation plans/dates.

8. Communication to be sent out to all employees affected by the new policy with effective dates.

9. Ensure you are aware of any legal or regulatory restrictions, such as seven-year background
check requirements or disclosure permissions.

Process

1. Initial verification of identity of the employee or applicant can be completed by using driver’s license, passport or other government photo identification. Fingerprints may be required to confirm identity of the applicant.

2. Criminal Name Record Check from country of origin.
3. Each applicant or employee must complete a declaration of understanding and consent form in writing prior to conducting a criminal record check.
4. To comply with legal requirements the following conditions must be met;
5. You must obtain written consent from the employee to conduct a criminal background check
6. The request for a criminal record check must be pertinent to his or her position
7. The criminal record check and the written consent forms signed by the employee must be secured separately from the employee’s personnel file.
8. Develop a methodology for including risk and criteria for what is “Acceptable” and “Unacceptable” risk to the organization.
9. Reasons for “Unacceptable” risk include but not limited to crimes of serious violence such as treason, sabotage, terrorist acts, hostage taking, weapons charges, inappropriate social behavior such as sexual assault, dishonesty such as theft, sale, possession, distribution, or manufacture of illegal drugs, multiple summary convictions of any kind.
10. Notification of “Acceptable” risk is communicated to the hiring manager.
11. Notification of “Unacceptable” risk shall be communicated to HR prior to notifying the hiring manager that the person is deemed a risk.
12. Appeal process shall be offered to all current employees to be able to provide reason for reconsideration.
13. Personnel risk assessments should be updated not less than seven years after the initial assessment or for cause.
14. Self-reporting an offence, charges and convictions should be included in the policy within seven year period.
15. Follow up on may be required from time to time on individuals that identity cannot be confirmed.
Other considerations: There are some other general considerations that should be considered when conducting a PRA.

1. All policies and processes relating to personnel risk assessments and more specifically criminal records checks should also consider all legislation, regulation requirements by industry organizations, and applicable laws.

2. Consider using third party organizations that are based in the country that you are doing the check in and comply with applicable privacy legislation.

3. Consider using security incident management software to document and store all criminal background checks for security and confidentiality.

Labor Relations
The introduction of a background check process will cause concern amongst employees, whether they have a criminal record or not. Background checks are intrusive, and look into areas that most people consider private. It is vital that employees understand that their information will be treated confidentially, and that you do nothing to contradict this.

Typically, employees will want to know why you are doing the checks, what you are looking for, what you will do with the information, and where it will be stored. They will want to know what you will do if an employee ‘fails’ a background check – will there be employment consequences?

<table>
<thead>
<tr>
<th>Information</th>
<th>Use for Assessing Qualifications</th>
<th>Use for Personnel Risk Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criminal Record Check</td>
<td>N/A</td>
<td>To determine whether the individual has committed crimes that would indicate unacceptable risk in relation to the duties to be performed.</td>
</tr>
<tr>
<td>Identity Verification</td>
<td>To prevent personation, to ensure that qualifications assessed are those of the candidate.</td>
<td>To prevent personation, to ensure that the records checked are those of the individual being checked. Identity verification is typically done through a credit bureau.</td>
</tr>
<tr>
<td>Credit Check</td>
<td>N/A</td>
<td>To determine whether the individual might be subject to financial pressures that could reflect on the degree of trust that can be justified, in relation to the duties to be performed.</td>
</tr>
<tr>
<td>Educational Qualifications</td>
<td>To ensure the individual possesses the academic qualifications required by the position.</td>
<td>To ensure the individual is being truthful about background and history.</td>
</tr>
</tbody>
</table>
Security Considerations for Employee Terminations

Introduction
Employee terminations are often stressful, emotional situations. Careful planning and treating the subject with respect and dignity can reduce the chances of a difficult or violent outcome.

There are a number of security issues to take into consideration when planning the termination meeting. These include:

1. **Risk assessment**: is there any reason to believe that there will be violence before, during, or after the termination?
2. **Interview room layout**: the layout of the seating and the position of the furniture can have a direct consequence on the safety of company personnel if the terminated employee becomes violent. Is the room laid out in a manner that would allow interviewing personnel to leave the room without being blocked by the subject?
3. **Interview process**: Is your interview process well thought out - have your prepared and educated your Manager? Do you require outplacement services on site?
4. **Recovery of assets**: Do you currently know what items the employee may have in their possession – on their person, at their work station or at home? All property, including phones, need to be recovered but there may be an opportunity to negotiate for the phone and/or phone number after the fact.
5. **Safeguarding corporate property**: Have you made the correct arrangements to suspend the terminated employee’s access to systems? Are there any other remote logins to be aware of? Is there any third-party software that the person may have access to, or authentication tokens?
6. **Collection of personal property**: the subject will need some personal property immediately, such as a purse, outdoor clothing, etc., and they will need to know how they can collect the remainder of their property later. Have you made arrangements for someone to retrieve these and bring them back to the room?

Risk Assessment
People are terminated for a wide variety of reasons: business realignment, job performance, behavioral issues, violation of company policy, criminal activity, etc. The one that we should be particularly careful with is one involving a behavioral issue: if an employee starts acting aggressively towards others, or if he develops a very poor attitude, or any other major behavioral shift, we need to understand why - terminating an unstable employee can have catastrophic consequences for all. The risk assessment process is important, but predicting
a person’s reaction to traumatic events is difficult. We need to ensure our planning allows us to react to a variety of outcomes; even those we don’t think are likely.

There are a number of warning signs of violent behavior. None of these, by itself, is a sure predictor of violent behavior, but if any of these signs appear then we should be cautious if the decision is made to proceed with the termination process. They include:

1. The employee appears or has verbalized he is stressed
2. The employee believes nothing is his fault, or complains about unfair treatment
3. The employee experiences a sudden and detrimental change in appearance
4. The employee has strained work relationships, or exhibits disrespect for authority
5. The previously safety-conscious employee begins disregarding safety at work
6. The employee has a fascination with weapons, or a concealed carry permit
7. The employee is struggling with an addiction or other medical condition
8. The employee suffers from sudden mood swings – depression/mania, forgetfulness, confusion, apparent overreaction
9. The employee is more frequently absent from work
10. The employee has recently suffered a major loss or setback, such as divorce, bankruptcy, or the death of a family member
11. During the interview, indicators of potential violent behavior may include red face, sweating, restlessness, trembling, change in voice or demeanor, violating the personal space of others, and overt threats

If the decision is made to proceed with a termination of an employee whom we feel is dangerous, then the first decision to be made is whether the person should be terminated in person, or by telephone and courier. If there is a high to critical risk of violence, then the person should be told over the telephone, and their paperwork should be sent to them by courier. A mitigating circumstance in all threat levels is whether or not the person is being terminated for cause with no financial package: a person who is getting a financial settlement is less likely to be a danger than one who is not, but this is not a hard-and-fast rule.

The aim of this process is to ensure that there is no violence. If Security personnel are required to physically touch a subject during a termination interview, then it will be considered a failure of the process.

Table 4: Threat Level Analysis Factors

<table>
<thead>
<tr>
<th>Threat Level</th>
<th>Capability</th>
<th>History</th>
<th>Intentions</th>
<th>Targeting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>X</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>High</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Medium</td>
<td>X</td>
<td>X</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>X</td>
<td>O</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Negligible</td>
<td>O</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Legend: X Factor must be present O Factor may or may not be present (unconfirmed)

Adapted from Johnson, Ross: Antiterrorism and Threat Response: Planning and Implementation, CRC Press, February 2013, page 93
Table 4 provides guidance on how to determine the threat level in a termination. This table is only a guide: if you consider that the threat may be higher than the table indicates, then use the higher level. Be very cautious in assuming that the threat is lower than the table indicates. The different categories are as follows:

1. **Capability**: Does the individual have the capability (size, strength, training, or weapons) to commit a violent act?

2. **History**: Does the individual have a history of violence? Is he or she known to have gotten into fights or physical altercations? Do they have a criminal record for crimes such as assault, battery, etc.? Are they aggressive?

3. **Intentions**: Has the individual ever threatened to hurt anyone?

4. **Targeting**: Has the individual given any indication that they have targeted someone? They could be sending threatening letters, telling co-workers that they are very angry with a specific person, such as a supervisor, or exhibiting stalking behavior off-site.

If a person has the capability to commit violence, and there are unconfirmed reports of a history of violence, intentions, and the targeting of a co-worker or supervisor, then the security risk should be deemed **Critical** and they should not be allowed back on site. The facts of the case should be referred to law enforcement and then, in consultation with the police, the person should be terminated by phone and courier.

If a person has the capability to commit violence, has a history of violence, and has made generalized threats in the past, then the security risk should be considered **High** and the person should be terminated by telephone and courier.

If a person has the capability to commit violence, has a history of violence, and there are unconfirmed reports of the intention to commit violence, then the security risk should be considered **Medium**. Given the strength of the various factors, a decision should be made as to whether the person should be terminated by phone and courier, or in person, with corporate security personnel in the room during the interview.

If a person has the capability to commit violence, and there are unconfirmed reports of a history of violence (including no criminal record for crimes such as assault), and the other factors are not present either confirmed or unconfirmed, then the threat is Low, and the termination process can proceed without the presence of Security. (If the Human Resources Consultant (HRC) would feel more comfortable with Security personnel either in the room or outside the door, then they should say so and Security will accommodate.)

If the person may or may not have the capability to commit violence, then the risk is **Negligible**, and no Security presence is required unless the HRC wishes it.

**Interview Room Layout**

The room should be neat; large enough to allow enough room for people to maintain a safe distance from the subject; and should be private. The table and chairs should be arranged so that the HRC and manager can exit the room quickly if they have to without being blocked by the subject. At the same time, the subject should not feel trapped in the room by the HRC, manager, or security.
**Interview Process**

The conduct of the interview should be respectful, free of emotion, and focused on ensuring the message is delivered to the terminated employee in a timely and succinct manner. The Manager should only be present in the room long enough (under 60 seconds) to read the scripted message they have been provided by HR and then should immediately leave. The Manager should not return. The continued presence of the manager may provide a target for the subject to offset their emotions; they may hold out for hope of redemption: believe they can convince the manager that he or she is wrong, be able to save their job; and when they can’t, there is a risk it may trigger their emotional state to move from that of sadness/hurt to anger/violence. The aim is to get past the focus on the termination and to move to the phase of transition; where the HR Consultant can explain the separation package and transition services.

As the response of any individual is not tangible, continue to be aware of the warning signs of potential violence. Should the subject’s emotional state begin to escalate and security is not available the next steps are dependent on the HRC’s experience and level of comfort.

In a majority of the time, if the subject is addressed by title, (i.e. Mr. Smith) and is told that you will call 911 and rescind the financial settlement offer, most will back down. If there is ever a doubt, safety is first and foremost: CALL 911.
Assets Retrieval and Disabling of Access

Items to be retrieved/disabled from the terminated employees:

1. Cell Phone/Blackberry
2. Laptop/Tablet
3. Employee ID/Access Control Card
4. Corporate Credit Card
5. Keys to company vehicles, buildings or equipment
6. Parking Pass
7. Disable Access to Logical Business Network/Applications
8. Disable Employee ID/Access Control Card

Safeguarding Corporate Property

Prior to the termination, the manager should provide Security with the details of any special computer accounts that the subject may have, such as plant Industrial Control Systems, etc. This is critical to protecting the company – some industrial control systems may be accessible directly from the Internet, and if the subject can access them later they can damage or destroy production equipment. If the subject is a member of Information Systems, then they may have access to a number of systems critical to the company.

When the subject enters the interview room, Security will suspend their network access, corporate accounts, and building access.

The manager should go to the subject’s workstation immediately after the termination interview and power off their computer. This prevents the subject from logging on locally later if their computer was only locked (not logged off), and they gain access to it.

Collection of Personal Property

After the manager leaves the interview room, he or she should return to the subject’s workspace and recover those personal items that the subject may need immediately, such as their coat, boots, and purse. The manager should not return to the interview room, but should ask another manager or administrative staff to bring personal items to the room. If a member of security staff is available, then the items should be left with him or her. Arrangements for the remainder of their personal effects can be made as follows:

1. The manager can box up all privately-owned material and have it couriered to the subject’s home; or
2. Security personnel can escort the subject after hours while they collect their personal items. Security will examine all items to ensure that they are not corporate property. If the ownership of an item is in dispute, then it will be held aside until the manager can rule on the ownership of the property.
Information Security

Information Asset Management

**Identifying Information Assets**
The process of identifying important information assets should be sensible and pragmatic.

Important information assets will include, but are not limited to, the following [amend list as appropriate]:

- Filing cabinets and stores containing paper records.
- Computer databases.
- Data files and folders.
- Software licenses.
- Physical assets (computer equipment and accessories, PDAs, cell phones).
- Key services.
- Key people.
- Intangible assets such as reputation and brand.

The Entity must draw up and maintain inventories of all important information assets that it deems critical and needs protection. The Entity should identify each asset and all associated data required for risk assessment, information/records management and disaster recovery. At minimum it must include the following [amend list as appropriate]:

- Type.
- Location.
- Designated owner.
- Security classification.
- Format.
- Backup.
- Licensing information.

**Classifying Information**
On creation, all information assets is assessed and classified by the owner according to their content. At minimum, all information assets must be classified and labelled in accordance with the Entity’s Information Security Policy. The classification will determine how the document should be protected and who should be allowed access to it. Any system subsequently allowing access to this information should clearly indicate the classification. Information up to RESTRICTED sent via e-mail must be labelled appropriately using the Entity’s guidance procedure.
The Information Security Policy requires information assets to be protectively marked into one of four classifications. The way the document, data and information is handled, published, moved and stored will be dependent on this classification.

The classes are:

1. Public
2. Protected
3. Restricted
4. Confidential

You should refer to Information Security Policy for full details on the application of information classification.

Assigning Asset Owners

All important information assets must have a nominated owner and should be accounted for. An owner must be a member of staff whose seniority is appropriate for the value of the asset they own. The owner’s responsibility for the asset and the requirement for them to maintain it should be formalized and agreed.

Unclassified Information Assets

Items of information that have no security classification and are of limited or no practical value should not be assigned a formal owner or inventoried. Information should be destroyed if there is no legal or operational need to keep it and temporary owners should be assigned within each department to ensure that this is done.

Disposal

When no longer required and per the Information Security Policy, hard copies of RESTRICTED or CONFIDENTIAL information shall be physically destroyed by shredding with a cross-cut non-linear shredder. Floppy disks, CDs, and DVDs containing RESTRICTED or CONFIDENTIAL information shall be physically destroyed by shredding or cutting with a cross-cut non-linear shredder in a manner to prevent use. [Insert local retention policy requirements and/or procedure for destroying information here].

Acceptable Use of Information Assets

The Entity must document, implement and circulate Acceptable Use Policies (AUP) for information assets, systems and services. These should apply to all [Entity Name] Departments, Partners, Employees of the Entity, contractual third parties and agents of the Entity and use of the system must be conditional on acceptance of the appropriate AUP. This requirement must be formally agreed and auditable.

As a minimum this will include [amend list as appropriate]:

- E-mail Policy.
- Internet Acceptable Usage Policy.
- Computer and Telephone Misuse Policy.
- Software Policy.
- Remote Working Policy.
- Removable Media Policy.

Information Storage

All electronic information will be stored on centralized facilities to allow regular backups to take place.
Records management and retention guidance will be followed [provide a link to any guidance if appropriate].

Staff should not be allowed to access information until they have been trained and approved so that they understand the responsibilities for the information that they will be handling. Databases holding personal information will have a defined security and system management procedure for the records and documentation.

Files which are identified as a potential security risk should only be stored on secure network areas.

**Disclosure of Information**

**Sharing Protected, Restricted and Confidential Information with other Organizations**

Protected, Restricted and Confidential information **must not** be disclosed to any other person or organization via any insecure method including, but not limited, to the following:

- Paper based methods.
- Fax.
- Telephone.

Where information is disclosed/shared it should only be done so in accordance with a documented Information Sharing Agreement and/or Data Exchange Agreement.

Protected or Restricted information may be sent via U.S. mail or commercial delivery service. Ensure the package requires a signature receipt and has a tracking number. DO NOT mark the information classification on the outside of the package. Restricted or Confidential information may be hand-carried, provided it is protected per the Information Security Policy.

Prior to electronic transmittal, Restricted or Confidential electronic files should be encrypted using approved encryption tools such as PGP, Adobe Acrobat, TruCrypt, etc. Approval for these tools will be authorized by the IT Administrator. Electronic transmission of information from a remote location to the Responsible Entity network shall be encrypted (e.g., VPN using 128-bit Secure Socket Layers, Internet Protocol Security IPSec, or Transport Layer Security). Passwords/pass phrases associated with the encrypted file shall not be included in the same e-mail as the attachment containing the Restricted or Confidential data.

An official email legal disclaimer must be contained with any e-mail sent.

The disclosure of RESTRICTED or CONFIDENTIAL information in any way other than via Entity’s encrypted e-mail is a disciplinary offence. If there is suspicion of an employee treating RESTRICTED or CONFIDENTIAL information in a way that could be harmful to the Entity or to the data subject, then it is be reported to the [IT Security Department], and the person may be subject to disciplinary procedure.
**Information in Motion**

The sensitivity of information shared by email within the electricity sub-sector may be indicated using the Traffic Light Protocol (TLP).

<table>
<thead>
<tr>
<th>Color</th>
<th>When should it be used?</th>
<th>How may it be shared?</th>
</tr>
</thead>
<tbody>
<tr>
<td>RED</td>
<td>Sources may use TLP: RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party’s privacy, reputation, or operations if misused.</td>
<td>Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.</td>
</tr>
<tr>
<td>AMBER</td>
<td>Sources may use TLP: AMBER when information requires support to be effectively acted upon, but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.</td>
<td>Recipients may only share TLP: AMBER information with members of their own organization who need to know, and only as widely as necessary to act on that information.</td>
</tr>
<tr>
<td>GREEN</td>
<td>Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.</td>
<td>Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.</td>
</tr>
<tr>
<td>WHITE</td>
<td>Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.</td>
<td>TLP: WHITE information may be distributed without restriction, subject to copyright controls.</td>
</tr>
</tbody>
</table>

For a more detailed explanation of how the TLP system works, please see this [website](#).
Information Systems Security

Information systems security refers to an organization’s business systems, not their Industrial Control Systems.

The goal of information systems security is to ensure the confidentiality, integrity, and availability of information.

Information security policies are key to success in this area. The SANS Institute offers a number of security policy templates on their website at www.sans.org/security-resources/policies.
NERC CIP standards may apply – see NERC Critical Infrastructure Protection Standards.

NIST SP 800-82 *Guide to Industrial Control Systems (ICS) Security* is an excellent resource. It is available online [here](#).
Security Information Sharing and Communications

NERC CIPC

CIPC is responsible for:

- Coordinating and communicating with organizations responsible for physical security and cybersecurity in all electricity industry segments and other critical infrastructure sectors, as appropriate;
- Liaising with governments on critical infrastructure protection (CIP) matters;
- Coordinating with the other NERC committees and working groups to ensure the highest degree of collaboration possible;
- Establishing and maintaining an information-reporting procedure for CIP among industry segments and with governments, as appropriate;
- Developing, periodically reviewing, and revising (as appropriate) security guidelines;
- Assisting in the development and implementation of NERC Reliability Standards; and
- Conducting forums and workshops related to the scope of CIPC.

North American Electric Reliability Corporation’s Electricity Information Sharing and Analysis Center (NERC E-ISAC)

The Electricity Information Sharing and Analysis Center (E-ISAC) establishes situational awareness, incident management, coordination, and communication capabilities within the electricity sub-sector through timely, reliable, and secure information exchange. The E-ISAC, in collaboration with the Department of Energy and the Electricity sub-sector Coordinating Council (ESCC), serves as the primary security communications channel for the electricity sub-sector and enhances the sector's ability to prepare for and respond to cyber and physical threats, vulnerabilities, and incidents.

The E-ISAC:

- Identifies, prioritizes, and coordinates the protection of critical power services, infrastructure service, and key resources;
- Facilitates sharing of information pertaining to physical and cyber threats, vulnerabilities, incidents, potential protective measures, and practices;
- Provides rapid response through the ability to effectively contact and coordinate with member companies, as required;
- Provides and shares campaign analysis, which includes capturing, correlating, trending data for historical analysis, and sharing that information within the sector;
- Receives incident data from private and public entities;
- Assists the Department of Energy, the Federal Energy Regulatory Commission, and the Department of Homeland Security in analyzing event data to determine threat, vulnerabilities, trends and impacts for the sector, as well as interdependencies with other critical infrastructures (this includes integration into the DHS National Cybersecurity and Communications Integration Center);
• Analyzes incident data and prepares reports based on subject matter expertise in security and the bulk power system;
• Shares threat alerts, warnings, advisories, notices, and vulnerability assessments with the industry;
• Works with other ISACs to share information and provide assistance during actual or potential sector disruptions whether caused by intentional, accidental, or natural events;
• Develops and maintains an awareness of private and governmental infrastructure interdependencies;
• Provides an electronic, secure capability for the E-ISAC participants to exchange and share information on all threats to defend critical infrastructure;
• Participates in government critical infrastructure exercises; and
• Conducts outreach to educate and inform the electricity sub-sector.

Canadian Electricity Association’s Security & Infrastructure Protection Committee (CEA SIP)

Reporting to the Board of the Canadian Electricity Association, the Security and Infrastructure Protection Committee (SIPC) is responsible for developing and delivering security programming and policy. The Committee addresses physical security policy, cyber security policy, and emergency preparedness.

The SIPC uses an all-hazards, all-threats perspective, coordinating the industry’s interface with Canadian federal security, intelligence and policy officials, and does so in coordination with partners in other sectors and on a continental basis through the NERC CIPC.

Canadian Cyber Incident Response Centre (CCIRC)

In support of Public Safety's mission to build a safe and resilient Canada, CCIRC's mandate is to help ensure the security and resilience of the vital non-federal government cyber systems that underpin Canada's national security, public safety and economic prosperity. As Canada's computer security incident response team, CCIRC is Canada's national coordination centre for the prevention and mitigation of, preparedness for, response to, and recovery from cyber incidents on non-federal government systems. It does this by providing authoritative advice and support, and coordinating information sharing and incident response.

• Main Incident Handling mailbox: ps.cyberdo.sp@canada.ca
• Products and Notifications distribution: ps.ccirc-ccric.sp@canada.ca
• Public mailbox used to report incidents: PS.CyberIncident-CyberIncident.SP@canada.ca
• Malware intake address (malware@ccirc-ccric.gc.ca)
• CCIRC PGP key: http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/._fl/CCIRCPublicPGPKey.txt
Physical Security Incident Response and Investigation

Incident Response

Perhaps one of the most overlooked yet necessary and important pieces of the security plan implementation process is the accurate and timely identification, notification, and response to a security incident. Security incidents can mean different things to different organizations; however, they all require action within the context of any security posture. The following is a general guideline for managing an actual security incident:

Identification

- There must be clearly communicated organizational parameters regarding what constitutes a security incident.
- All employees and contractors need to receive security incident and reporting training.

Notification

- All employees need to receive training on the security incident reporting process.
- Notification Programs need to be prominently displayed throughout an enterprise’s facilities and work areas.
  - The incident notification process should be centralized and simple — one call to security operations or emergency operations center et cetera.
  - Establish one initial point-of-contact and maintain that designee until the incident management chain identifies an incident commander.
- Educate your employees to understand that any pictures taken, videos recorded, or posts made to social media sites could be considered to be evidence, and your employees must advise responding law enforcement or your security function that pictures, video recordings, or social media posts relating to the incident have been made and to save them.
- Accuracy of reported information.
  - Employees and contractors should receive training about reporting only the known and corroborated facts.
  - Refrain from providing sensationalized information i.e., an explosion is an explosion — it is not necessarily a bomb until appropriate authorities investigate.
  - Refrain from editorializing reported information “it looks like a war zone,” et cetera. Be concise and accurate as possible: who, what, when, where, how.

Response

- If it is safe and feasible to do so, provide care and removal of any victims or casualties of the incident.
- Initial first responders not involved in care or event mitigation should establish a perimeter.
  - Perimeter size will be based upon type of event — equipment accidents, explosives et cetera will require specific training.
- Maintain operational security for all persons entering and exiting perimeter.
  - Institute one-way check-point and single path system for entry and exit. (Single path refers to identifying one travel path in/out of the scene that all must use to maintain scene integrity.)
Limit the amount of personnel that enter the perimeter until security, EMS, or LEA arrives and either assumes perimeter control or releases the scene.

- Identify by name, title, and contact information any employee at the scene or who was at the scene.
- Identify any witnesses or individuals who are at the scene or were at the scene and obtain as much personally identifiable information (PII) as possible.

- **Do not handle or remove any accompanying debris (not related to casualty treatment) until provided property guidance by the appropriate incident commander, security personnel, or law enforcement.**

- Take limited photographs or video of the scene and be prepared to turn copies and/or originals over to LEA.
  - Taking limited photographs or video once the scene is secure helps to ensure that security and LEA photographs of relevant persons, places, and evidence are consistent and not in contradiction.

- The initial person providing notification should be prepared to provide your security function or LEA with the following:
  - How you received notification, to include time, date, method, and reverse contact information if possible.
  - Who was notified of the incident both within and outside of your organization and how were they notified and when.
  - Do you have an identified incident command point-of-contact and be able to provide all contact methods for this person?
  - Who was dispatched to the scene and how long was the dispatch to arrival time?
  - If there were injuries, be able to provide the name, PII, and current hospitalization or location of the injured party?
  - Will this or has this incident had an impact on customer electricity delivery?
    - If so, how many customers have been impacted and for how long?
    - Are there any critical care or critical government facilities that have been impacted?
    - What are the attendant recovery, repair costs associated with the incident? (inclusive of lost revenue due to delivery interruption)?
  - Have you experienced any threats (insider or external) that you are aware of?

**Investigations**

**Considerations:**

**Confidentiality & Privacy** – All aspects of an investigation are considered private and confidential, and shall not be discussed with anyone except those with a valid need to know.

**Source Protection** – Every measure shall be taken to protect the identity of an informant or witness if he or she requests it or has reason to expect that their identity will be protected.

**Economy of Effort** – All investigations should be carefully planned to ensure that efficient use is made of the time and resources, and to reduce disruption to the workplace.
Oversight – The investigator’s manager should approve the investigation plan and the final report, as well as receive periodic briefings during the course of the investigation.

Methodical Exploitation – All available relevant sources of information shall be collected and reviewed prior to commencing investigation.

Documentation – All information and evidence received as part of the investigation shall be properly identified, marked, and secured properly.

Presumption of Innocence – Investigations are led by facts, not assumptions or opinions. If an allegation is unfounded, then the accused shall be presumed innocent of the allegations.

Conduct of Investigations

A) Goals of an internal investigation
- Provide a sound factual basis for management decisions;
- Produce reliable documentation and evidence that can be used to support management action;
- To reveal, if any, misconduct that has occurred. This includes identification or exoneration of employees who have been suspected, or are guilty of, misconduct;
- Help prevent further wrongful actions, and assist in providing corrective measures.
- Uncover possible criminal acts that may be passed onto law enforcement for further investigation.

B) Investigator qualifications
- All investigators should have formalized training/accreditation in the area of internal investigations. Applicable certifications include ASIS International’s Certified Protection Professional or Professional Certified Investigator.
- Previous experience in investigating criminal law
- Certified Fraud Examiner, Forensic Investigator, or Professional Certified Investigator

C) Scope of investigation and strategy
- Determine how to staff the investigation;
- Determine and assign the lead investigator;
- Fully understand the allegation(s);
- Determine how many people need to be interviewed;
- Limit the number of interviews to only those required to substantiate the allegation(s);
- Determine if the investigation will stay internal, or whether law enforcement need to become involved.

There are six phases of an investigation as follows:

1. Allegation: There are often several allegations included in a single statement. Go over the allegation carefully, and if possible, ask the complainant for clarification of any points that are not clearly understood. The allegation is the keystone of the investigation: without a proper understanding of what is being alleged, it is easy to head in the wrong direction. If, during the course of an investigation, additional allegations are
discovered then this shall be reported to the Chief Compliance Officer and the Investigation Plan shall be amended.

2. **Planning**: Determine the sources of information that will be available to you during the conduct of the investigation. Develop a plan to obtain information both external (outside the site where the alleged infraction occurred) and internal (within the site of the alleged infraction, including witness statements and interviews). Review the Investigation Plan with your manager.

3. **Off-Site Collection**: Once the investigation plan is approved, collect external records such as corporate credit card usage, emails, text messages, access control records, CCTV footage, computer documents, server and workstation logs, contracts, purchase orders, invoices, receipts, telephone records, cellphone records, legal documents, or any other record that is germane to the investigation, can be legally obtained, and is available outside the site where the alleged infraction occurred. The aim is to amass as much relevant information as possible prior to the interviews of the suspect(s) and witness(es). Information collected in this phase will provide material to guide questioning in the next phase. Note that unless there is a danger of evidence being destroyed, there is no requirement to rush this phase, as the suspect should not know that an investigation has been commenced until the time that has been agreed upon with the corporate legal counsel (or equivalent) and your manager.

4. **On-Site Collection**: The major difference between off-site and on-site collection is that when the on-site collection commences the accused will normally be aware that an investigation is underway, which may impact his or her behavior or lead to the destruction of evidence. There are two types of information that can be collected in this phase – documentary and interviews. Collect all records on site that are available and germane to the investigation. Interview anyone who is in a position to contribute to the resolution of the allegations(s). Question the accused last – you should be armed with the maximum amount of information you can possibly have, and hopefully you will know the answers to most of the questions before you ask them. You should either have a witness to the interview, or the interview should be recorded by either a video camera, or a digital voice recorder. Do not make any promises to the accused during the interview that you are not in a position to keep; for example, do not promise leniency in discipline in exchange for a confession.

5. **Collation and Analysis**: All evidence should be arranged in chronological order and examined thoroughly for relevance and accuracy. Consider each allegation in turn and determine if the evidence exists to support it. The investigator shall ensure that the case file is up to date.

6. **Reporting**: The purpose of reporting is to convey the facts of the case to the person who has requested the information. The report should tell the story of the investigation: where you looked for information, who you interviewed, and what you learned. It should also state any limitations to the investigation: for example, personal financial records are usually only available to law enforcement officers, and are therefore unavailable to corporate investigators. It should clearly state whether or not the allegation was proven, and detail the evidence that led you to that conclusion. Recommendations as to policy changes may be useful, but there should be no recommendations made regarding discipline, as it is outside of the investigation scope. If there is evidence of criminal wrongdoing, then a recommendation should be made in the report that the matter be referred to the law enforcement agency of jurisdiction. The investigation report shall be sent to the person who requested the investigation.
INVESTIGATION PLAN

At a minimum, the Investigation Plan should contain:

1. The allegation(s)
2. Identifying information on the accused
3. A description of the evidence provided with the allegation, if any
4. Types and sources of relevant information available away from the site where the incident occurred
5. Types and sources of relevant information available at the site where the incident occurred
6. A general list of questions for the accused and any witnesses
7. A proposed timeline for the conduct of the investigation

Examples of situations where internal investigations may be required include, but not limited to;

- Workplace theft
- Fraud
- Workplace violence
- Illegal, degrading or damaging use of computer systems/information
- Attending work in an unfit condition
- Threats against employees, others or property
- Vandalism
- Complaints received through Manitoba Hydro’s Integrity Program
- External complaints
- Personnel risk assessments
- Criminal misconduct
- Break & Enters
- Mischief
- Conflict of Interest
- Employee Misconduct

If the decision is made to suspend an employee during the investigation, the following Items to be retrieved/disabled from suspended employees:

- Cell Phone/Blackberry
- Laptop/Tablet
- Employee ID/Access Control Card
- Corporate Credit Card
- Keys to company vehicles, buildings or equipment
- Parking Pass
- Disable Access to Logical Business Network/Applications
• Disable Employee ID/Access Control Card

**Interview Protocols**

The employee being interviewed should be treated with dignity and fairness and in a manner consistent with the value that the company places on all of its employees.

1. Where, When and How

   - Generally interviews will be conducted on-site during working hours.
   - Occasionally safety or other concerns of the complainant may justify off-site interviews.
   - Generally all interviews will be conducted in person. Two members of the investigative team should attend interviews.
   - One of the interviewers will be responsible for transcribing the interview questions and answers.
   - The notes which are taken will be limited to observations and will not include personal opinions, comments or judgments.
   - Recording devices often inhibit witnesses and should not normally be used. Should it be deemed appropriate to record the interview, such devices will only be utilized with the consent of the individual being interviewed.

2. Commencement of Interview

   - Explain to the individual being interviewed that an investigation has been initiated as a result of the receipt of a complaint of a violation of the Company’s policy (state which policy).
   - Inform the individual being interviewed that they are expected to cooperate fully with the investigation.
   - Only those details of the complaint necessary to conduct a meaningful interview will be revealed.
   - Advise the individual being interviewed that the interviewees represent the company, and not the individual employee, and that information is being collected in order to provide factual evidence to the company as a result of an allegation(s). In the event that the employee responds to this information by asking if he/she can consult legal counsel or union representation prior to the interview or have legal counsel or union representation present at
the interview, the answer should be: “You may if you wish, however, you should understand that this is not a hearing and no one has been charged”.

• Explain that as it is difficult for the interviewer to listen and take proper notes and, as a result, note taking will be the witness’ primary task. The person being interviewed will be told they will have the opportunity to review those notes and will be asked to sign a witness statement at the end of the interview.

• Explain that the investigation process is confidential, but limited disclosure may be required in order to conduct the investigation.

• Advise that there is the possibility of a legal proceeding at some point following the investigation, at which the person being interviewed may be called as a witness. Because we are not responsible for that proceeding, it must be made clear to the individual being interviewed that no promises or predictions as to whether the person being interviewed would have to testify can be made.

• The person being interviewed must be advised to keep the information discussed during the interview(s) confidential as the company intends them to be protected by solicitor-client privilege and that he/she cannot discuss it with anyone else, neither an employee nor a friend, nor a family member.

• Advise the person being interviewed that if he/she has any follow-up information recalled after the interview, including any corrections or clarifications, or any subsequent questions, he/she should contact the interviewer without delay.

• Advise the person being interviewed that there will be an investigation report provided to the company at the completion of the investigation and that appropriate action following the investigation depends on complete and accurate answers to questions asked.

• Where criminal activity may be uncovered, and criminal prosecution is an option, include the caution against verbal incrimination.
Cyber Incident Response and Investigation

Introduction

This document is based on the SANS Institute's Incident Handler's Handbook, and has been modified for use in this Guideline. The original Handbook is available at: http://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

The purpose of this document is to provide a common cyber incident response plan for all information systems and operational technology in XYZ Corporation. Please note that this is only a suggestion intended to trigger further discussion within an organization – it is not a finished plan.

Preparation

Policy

The response strategy contains six components:

1. Preparation
   a. Activities (such as the creation of this plan) intended to help prepare XYZ Corporation to respond to a security incident involving the company’s information systems or operational technology.

2. Identification
   a. How do we identify the incident?
   b. What is its severity rating – Low, Medium, or High?

3. Containment
   a. Short-term containment – the immediate steps necessary to limit the damage and prevent further damage from occurring
   b. System backup – creating a forensic image of the affected system or systems to allow investigation of the incident as close as possible to the time it occurred without further impediment to the production environment
   c. Long-term containment – temporarily restoring the affected system or systems to allow a quick return to the production environment while rebuilding clean systems in the next phase

4. Eradication
   a. Removal or restoration of affected systems

5. Recovery
   a. Return to production

6. Lessons Learned
   a. What did we learn?
   b. Who do we inform?
   c. What changes to procedures or equipment are required?
   d. Follow-up to ensure changes are made
Communications
Swift, accurate communications are key to the success of this plan.

External
Warning external parties of the incident may help to prevent a similar attack on their systems, and through their reciprocation we may learn of imminent threats to our systems in time to take preventative measures.

External parties include:

<table>
<thead>
<tr>
<th>Severity of Incident</th>
<th>Entity</th>
<th>Email Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Canadian Cyber Incident Response Centre (CCIRC)</td>
<td><a href="mailto:ps.cyberdo.sp@canada.ca">ps.cyberdo.sp@canada.ca</a></td>
</tr>
<tr>
<td>Low</td>
<td>Electricity Information Sharing and Analysis Center (E-ISAC)</td>
<td><a href="mailto:operations@esisac.com">operations@esisac.com</a></td>
</tr>
<tr>
<td>Medium or High</td>
<td>Canadian Cyber Incident Response Centre (CCIRC)</td>
<td><a href="mailto:ps.cyberdo.sp@canada.ca">ps.cyberdo.sp@canada.ca</a></td>
</tr>
<tr>
<td>Medium of High</td>
<td>Electricity Information Sharing and Analysis Center (E-ISAC)</td>
<td><a href="mailto:operations@esisac.com">operations@esisac.com</a></td>
</tr>
</tbody>
</table>

* Consider informing if there is something new or unusual about the event

Immediate Internal Response
All cyber security incidents will prompt an immediate notification between all persons responsible for managing the response and investigation process. There should be communication between information systems management and industrial control systems management as well to ensure that each side is aware of the situation.

<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
<th>Email</th>
<th>Cellphone</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Internal
Informing internal parties will help to contain the attack and allow us to restore normal operating conditions more effectively. At a minimum, the following personnel should be informed of an incident:

- Chief Information Officer
  - Executive informed by CIO as appropriate
  - Privacy Officer informed by CIO if personal or private information is compromised
- Service Desk
- Forensics & Investigations Specialist
- The senior management of the department which uses the affected application(s)
- Director of Communications

Executive
Informing the Executive in the event of a severe incident will allow them to decide if further action, such as the deployment of the Crisis Management Team and informing the Board is warranted.

Documentation
Documentation of all of the activities of the response is particularly important if there is a chance that the incident will result in:

- disciplinary action against one or more employees;
- criminal charges; and/or
• if the severity rating is High.

Documentation should seek to allow the reader to understand:
• what happened;
• who responded, and what they did;
• when it occurred;
• where it happened;
• why it happened;
• how it happened;
• which internal parties were told, and when; and
• which external parties were told, and when.

**Composition of the Computer Incident Response Team (CIRT)**
The composition and size of the CIRT is determined by:
• the severity of the incident;
• the affected system(s); and
• an estimate of the resources required to restore normal operations.

<table>
<thead>
<tr>
<th>Incident Severity</th>
<th>CIRT Leadership</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Vice President, IS &amp; CIO</td>
</tr>
<tr>
<td>Medium</td>
<td>Senior Manager (Security &amp; Contingency Planning; Infrastructure), and Manager, Industrial Controls</td>
</tr>
<tr>
<td>Low</td>
<td>Forensics &amp; Investigations Specialist</td>
</tr>
</tbody>
</table>

Typically, other members of the CIRT would be drawn from other internal stakeholders as appropriate. Any required specialists would be brought in as necessary.

Depending on the circumstances, additional non-technical may be required from Communications, Operations, Legal, or Human Resources.

**Access Control**
Prior to the investigation of any incident, an assessment must be done to ensure that the technical investigators have access to the computer systems and physical locations necessary to adequately do the job. Assessing and assigning access at the beginning of the investigation is done to ensure that the momentum of the investigation is not impaired later by access problems.

**Tools**
Logical tools used in investigations include Encase.

**Training**
Training of the cyber incident response plan will be conducted annually. Training will be chiefly through tabletop exercises. Whenever possible, real incidents will be exploited for their training value.
Identification
Cyber incidents are identified and classified. Identification refers to the type of attack, and classification refers to its level of severity.

In general, the types of attack, their potential level of severity, and their classification include:

<table>
<thead>
<tr>
<th>Type</th>
<th>Method of Attack</th>
<th>Potential Severity</th>
<th>Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disruption</td>
<td>Worm</td>
<td>Very low – easily handled by automated systems</td>
<td>Routine</td>
</tr>
<tr>
<td>Disruption</td>
<td>Virus</td>
<td>Very low – easily handled by automated systems</td>
<td>Routine</td>
</tr>
<tr>
<td>Cybercrime</td>
<td>Spyware</td>
<td>Very low – easily handled by automated systems</td>
<td>Low</td>
</tr>
<tr>
<td>Cybercrime</td>
<td>Botnets</td>
<td>Very low – easily handled by automated systems</td>
<td>Low</td>
</tr>
<tr>
<td>Cyber Espionage</td>
<td>Advanced Persistent Threat</td>
<td>High potential</td>
<td>High</td>
</tr>
<tr>
<td>or Cybercrime</td>
<td>Zero-Day Targeted Attack</td>
<td>High potential</td>
<td>High</td>
</tr>
<tr>
<td>Cyber Espionage</td>
<td>Dynamic Trojan</td>
<td>High potential depending on location</td>
<td>High</td>
</tr>
<tr>
<td>or Cybercrime</td>
<td>Stealth Bot</td>
<td>High potential depending on location</td>
<td>Medium to High</td>
</tr>
<tr>
<td>Cyber Espionage</td>
<td>Insider attack: Removal of information from corporate systems by employee or contractor using email, USB stick, etc.</td>
<td>Severity depends upon data stolen. Most severe would be proprietary information related to business development, commodity portfolio management, or personal information</td>
<td>Medium to High</td>
</tr>
</tbody>
</table>

Containment
The purpose of this stage is to limit the damage and prevent further damage while preserving evidence should it be required for prosecution, disciplinary action, or the derivation of lessons learned.

Short-Term Containment
The aim of this step is to limit the damage by isolating the affected parts of the system. It may be as simple as isolating the network segment containing infected workstations to rerouting traffic to backup servers while production servers are isolated. The determination of what is to be done in this step is the very first decision of the management of the Cyber Incident Response Team: the remaining decisions related to investigation team composition, investigation plan, notification, etc. will wait.

System Backup
A forensic image of the affected system is taken using EnCase (or a similar tool). The purpose is to capture the system as it was during the incident, allowing investigation to commence while the servers or workstations are wiped and rebuilt (if necessary). This saves both evidence and speeds return to normal production.

Long-Term Containment
In this step, affected systems are temporarily fixed to allow them to be used in production while new servers are being rebuilt. This also entails ensuring that accounts and backdoors left by the attackers or malware are
identified and removed, installation of security patches on affected and other company systems, and preventing further escalation of the incident while allowing business operations to resume.

**Eradication**
Affected systems should be removed and restored to a pre-incident state. In most cases, this means a reimaging of the affected system’s hard drive or drives to ensure all malware is removed, improving of the system’s defenses to avoid reattack, and patching exploited vulnerabilities.

**Recovery**
In this phase, the affected systems are brought back into the production environment. The decisions that will need to be made prior to recovery are:

1. Time and date of restoration of operations
2. Test plan for the restored systems
3. Duration of the monitoring period to ensure that the restored systems are fully functional
4. The tools required to test and validate system behavior

**Lessons Learned**
This area deals with the lessons learned to make the CIRT more effective, as the technology and procedures required to prevent reinfection or reattack are dealt with previously in the response process.

The minimum information that should be captured includes:

- When was the problem first discovered, and by whom?
- What was the scope of the incident?
- How was the incident contained?
- How was the malware eradicated?
- What work was performed during recovery?
- What areas were the CIRT effective?
- What areas need improvement?
- Was the cyber incident response plan followed in its entirety, or was there an ad-hoc response?
- What is the timetable for improvement, and who is responsible to ensure the changes are made?
Annex A to Cyber Incident Response Plan – Incident Handler’s Checklist

1. Preparation
   a. Are all members aware of the security policies of the organization?
   b. Do all members of the Computer Incident Response Team know whom to contact?
   c. Do all incident responders have access to journals and access to incident response toolkits to perform the actual incident response process?
   d. Have all members participated in incident response drills to practice the incident response process and to improve overall proficiency on a regularly established basis?

2. Identification
   a. Where did the incident occur?
   b. Who reported or discovered the incident?
   c. How was it discovered?
   d. Are there any other areas that have been compromised by the incident? If so what are they and when were they discovered?
   e. What is the scope of the impact?
   f. What is the business impact?
   g. Have the source(s) of the incident been located? If so, where, when, and what are they?

3. Containment
   a. Short-term containment
      i. Can the problem be isolated?
         1. If so, then proceed to isolate the affected systems.
         2. If not, then work with system owners and/or managers to determine further action necessary to contain the problem.
      ii. Are all affected systems isolated from non-affected systems?
         1. If so, then continue to the next step.
         2. If not, then continue to isolate affected systems until short-term containment has been accomplished to prevent the incident from escalating any further.
   b. System-backup
      i. Have forensic copies of affected systems been created for further analysis?
      ii. Have all commands and other documentation since the incident has occurred been kept up to date so far?
         1. If not, document all actions taken as soon as possible to ensure all evidence are retained for either prosecution and/or lessons learned.
         2. Are the forensic copies stored in a secure location?
   a. If so, then continue onto the next step.
   b. If not, then place the forensic images into a secure location to prevent accidental damage and/or tampering.
   c. Long-term containment
      i. If the system can be taken offline, then proceed to the Eradication phase.
      ii. If the system must remain in production proceed with long-term containment by removing all malware and other artifacts from affected systems, and harden the affected systems from further attacks until an ideal circumstance will allow the affected systems to be reimaged.
4. Eradication  
   a. If possible can the system be reimaged and then hardened with patches and/or other countermeasures to prevent or reduce the risk of attacks?  
      i. If not, then please state why?

   b. Have all malware and other artifacts left behind by the attackers been removed and the affected systems hardened against further attacks?  
      i. If not, then please explain why?

5. Recovery  
   a. Has the affected system(s) been patched and hardened against the recent attack, as well as possible future ones?  
   b. What day and time would be feasible to restore the affected systems back into production?  
   c. What tools are you going to use to test, monitor, and verify that the systems being restored to productions are not compromised by the same methods that cause the original incident?  
   d. How long are you planning to monitor the restored systems and what are you going to look for?  
   e. Are there any prior benchmarks that can be used as a baseline to compare monitoring results of the restored systems against those of the baseline?

6. Lessons Learned  
   a. Has all necessary documentation from the incident been written?  
      i. If so, then generate the incident response report for the lessons learned meeting.  
      ii. If not, then have documentation written as soon as possible before anything is forgotten and left out of the report.  
   b. Assuming the incident response report has been completed, does it document and answer the following questions of each phase of the incident response process: (Who? What? Where? Why? And How?)?  
   c. Can a lessons learned meeting be scheduled within two weeks after the incident has been resolved?  
      i. If not, then please explain why and when is the next convenient time to hold it?

   d. Lessons Learned Meeting  
      i. Review the incident response process of the incident that had occurred with all CIRT members.  
         ii. Did the meeting discuss any mistake or areas where the response process could have been handled better?  
            1. If no such conversations occurred, then please explain why?
**Fraud Prevention**

A fraud prevention program is typically composed of five components:

1. **Governance:** corporate policies designed to set management expectations related to fraud;
2. **Risk Assessment:** an annual survey of the enterprise where potential opportunities for fraud are identified and controls are implemented and evaluated;
3. **Prevention:** procedures are built into corporate policies that reduce the opportunity for fraud;
4. **Detection:** personnel actively search for evidence of fraud; and
5. **Investigation and Corrective Action:** instances of suspected fraud are investigated to prevent further occurrences and determine the extent, if any, of culpability of the person committing the fraud.

**Governance**

A number of policies contribute to the governance of a fraud prevention program.

- *Ethics policies* clearly lay out acceptable and unacceptable behavior. *Purchasing policies* detail the procedures used to expend funds and purchase goods, and details the levels of approval required in order to expend funds. *Accounting policies* describe in more detail how funds are managed, and *Investigation policies* describe the authority and scope of activities undertaken to determine the extent and responsibility of fraud incidents.

**Risk Assessment**

There are a number of ways to conduct a fraud risk assessment:

- **Scenarios** – a risk register of potential fraud schemes that could take place within the company. The register is assembled by a team representing all areas of the company, and is reviewed at least annually. The register includes the following:
  1. **Scenario Number** (1-59)
  2. **Fraud Scenario** (For example, ‘False outages – intentional scheme to take generation off at predetermined times so that merchant can capitalize in the market’)
  3. **Source** Where the fraud is most likely to take place
  4. **Category** (FR: Fraudulent Financial Reporting; MA: Misappropriation of Assets; UADA: Unauthorized acquisition or disposition of Assets; AA: Aiding and Abetting; SME: Financial Misconduct by Senior Management or Employees with Significant Role in Financial Reporting; and D: Deceptive disclosure)
  5. **Risk Likelihood** (L = remote chance / M = more than remote = / H= likely (Risk scores L=1 / M=2 / H=3))
  6. **Risk Impact** (L = inconsequential / M = more than inconsequential / H = material. (Risk scores / L=1/M=2/ H=3)
  7. **Risk Rating** (Computed from Likelihood X Impact scores. Score < 3 = Low risk rating / Score 3 or 4 = Moderate Risk Rating / Score 6 or 9 = high risk rating)
  8. **Comments and Additional Information** (Usually a description of the circumstances surrounding the scenario: what factors can increase the likelihood of occurrence, or how it relates to other scenarios or policies)
  9. **Current Controls** (The procedures and methods that CPC uses to prevent that particular scenario from occurring)
  10. **Control Rating** (H = strong controls/ high rating; M = moderate controls and rating; L = weak controls / low rating controls; W = Weak)
11. **Residual Risk**: ((After controls applied) L = Low residual risk as control rating equals or exceeds risk rating; M = Moderate residual risk as risk rating exceeds control rating by 1 level (High risk vs. Moderate Control or Moderate Risk vs. Low Control); H = high residual risk as risk rating exceeds control rating by 2 levels (High risk vs. Low Control).

- **Survey** – The Association of Certified Fraud Examiners (ACFE) has a wealth of information that can assist you in building all aspects of a fraud prevention program. They have an excellent fraud risk assessment tool that is available to members at [http://www.acfe.com/frat.aspx?id=6797](http://www.acfe.com/frat.aspx?id=6797).

The fraud risk assessment should be conducted annually, and the results reported to the executive or the Board audit committee. The results of the assessment are used to guide improvements to the fraud prevention program.

## Prevention

The dynamics of fraud revolve around three factors, often called the fraud triangle:

1. **Pressure** (sometimes called motivation). A fraudster must have a reason to want to steal the money or asset. Most fraudsters don’t start out as criminals – many steal from their employer because they are in desperate financial straits; or they need money to buy drugs or alcohol; or their personal life is out of control, and they think that stealing money or assets will help them regain control;

2. **Rationalization**. Few people think of themselves as criminals, and will create elaborate justifications for stealing that allow them to retain their self-respect. For example, someone who believes that they work uncompensated overtime might think it fair to take something of value from work as a form of informal payment; and

3. **Opportunity**. In order to steal money or an asset, an opportunity must exist. As employees generally understand the processes within a company the best of anyone, they will likely be the first to identify a gap in controls that can create an opportunity for fraud. Opportunities to defraud that are left untreated by management reinforce a fraudster’s rationalization: ‘if they really cared, they would close this gap,’ or ‘if I don’t take advantage of this, then someone less deserving than I will.’

We can reduce **pressure** by:

- Conducting pre-employment background screening to avoid hiring employees who:
  - have a criminal record that indicates that they are untrustworthy or have addiction problems;
  - will have access to money and have a disastrous financial history
  - have indicated untrustworthiness by lying about previous employment, education, or certifications
- Providing Employee Family Assistance programs to assist any employees who may have an addiction problem or require financial counseling
- Provide a generous benefits package to employees that includes insurance that will reduce the financial impact of illness or other medical or dental problems
- Provide employees an opportunity to create personal wealth through a generous employee savings plan

We reduce **rationalization** by:

- Ensuring that all employees read the Ethics Policy, which clearly states expectations regarding employee behavior
• Requiring the highest level of ethical behavior of all managers to set a positive example for employees
• Compensate our employees fairly and in line with industry norms
• Remind employees of the company’s ongoing interest in preventing fraud through mandatory ethics training
• Establishing a reputation for zero tolerance of fraud within the organization

We reduce the opportunity to defraud through:
• Establishing financial controls
• Always ensure at least two levels of approval for the expenditure of funds
• Eliminate the use of cash within the organization
• Identifying and removing opportunities to commit fraud through the annual review of the fraud program

Detection
The most common methods of fraud detection include:
• Tips
• Management review
• Internal audit
• Accidental discovery
• Account reconciliation
• Document examination
• External audit
• Notification by law enforcement
• Surveillance and monitoring
• IT controls
• Confession

In many cases, fraudsters can give themselves away by exhibiting one or more of the following characteristics:
• Living beyond their means
• Experiencing financial problems
• An unusually close relationship with a vendor or customer
• They have control issues or will not share their job duties (includes not taking vacation or time off)
• Going through a divorce or other family problems
• They engage in commercial scheming
• They act noticeably irritable, defensive, or suspicious
• They have a known problem with addiction

You can use automated tools such as ACL (Audit Command Language) to look for indicators of fraud. They include:
• Duplicate invoices
• Payroll deposits after termination date
• Split requisitions
• Split purchase orders
• Purchase orders where the creator is also the approver
• Vendors and employees sharing the same mailing address
• Benford analysis
Use of these automated tools are proactive, and can uncover fraud where it would have otherwise gone unnoticed.

**Investigation and Corrective Action**
Investigation of suspected fraud incidents will be generally governed by the potential scope. A simple fraud incident may be investigated using organic resources, but a more complex scheme – especially one involving large sums of money - may require the assistance of a forensic audit consultant or law enforcement agency.

The corrective action is determined through your organization’s disciplinary policies.

Further information on fraud prevention can be found on the [Association of Certified Fraud Examiner’s website](https://www.acfe.com).
Qualifications, Training and Awareness

Security Leadership

Selecting the best-qualified security leader is important to the success of an organization’s security program. The following is a list of the skills and experience that a Chief Security Officer or Security Director should have to be considered for the position.

Skills
The role of the CSO is to protect the company by: providing leadership to the company’s security team; representing the department to the Executive and the rest of the company; and ensuring that the security team evolves in organization, capability, and equipment in order to keep pace with the threat environment. The skills and experience that a successful CSO should have include:

- Leadership
- An ability to think and act both tactically and strategically
- Superior communications skills: the CSO must be the evangelist for corporate security, and must be able to present ideas clearly and simply, in writing and in person, to groups large and small
- SME level knowledge in one or more of the following disciplines: physical security, information systems security, industrial controls systems security, or business continuity management
- Using influence to achieve an end, rather than relying on the exercise of authority
- Adapting security solutions to meet the business need – not the other way around
- Comfortably discuss security issues with the Executive or Board
- Using technology to solve problems
- Managing change in both the corporate and the security environments
- Creating and fostering personal relationships within the wider security community to enhance access to information, influence regulation and legislation, and recruit personnel
- Working with personnel of diverse skill sets and backgrounds
- Planning, budgeting, and executing

Qualifications and Experience

Relevant certifications include:
- Certified Protection Professional (CPP)
- Certified Fraud Examiner (CFE)
- Certified Information Systems Security Professional (CISSP)
- Accredited Business Continuity Professional (ABCP)

A CSO should have:
- Extensive practical and leadership experience in the military, law enforcement, intelligence, or corporate security
- A university education, police or military staff college, or equivalent
• Involvement with the CEA’s Security and Infrastructure Protection Committee, and/or the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection Committee
• A thorough understanding of the protection issues associated with the Bulk Power System
• Familiarity with NERC CIP Standards and Guidelines, and the process by which they are developed
• Must be able to obtain a Level II (Canada) / Secret (US) security clearance
• Membership in a professional association, such as ASIS International or (ISC)²

Additional Information
• ASIS GDL CSO 04 2008 ASIS International Chief Security Officer Guideline 2008 Edition
• ANSI/ASIS CSO.1-2013 Chief Security Officer – An Organizational Model

Skills & Experience by Position
The following table shows the suggested skills and experience for all persons in a security department in the electricity sub-sector.
<table>
<thead>
<tr>
<th>Position</th>
<th>Certification (see legend - should have at least one)</th>
<th>Leadership Experience</th>
<th>Experience in Law Enforcement, Military, Intelligence, or Corporate Security (See Below)</th>
<th>University Education (or police/military staff college)</th>
<th>Experience with CEA SIPC and/or NERC CIPC</th>
<th>Professional Association (ASIS International, (ISC)^2, Disaster Recovery Institute</th>
<th>Written Communication Skills</th>
<th>Presentation Skills</th>
<th>SME-Level Knowledge</th>
<th>Electric Sector Background</th>
<th>Level II (Secret) Security Clearance</th>
<th>Relationship-Building Skills</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSO</td>
<td>CPP, CFE, CISSP, GSEC, CBCP, MBCP, FSyl, CSyP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Advanced</td>
<td>Advanced</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Director</td>
<td>CPP, CFE, CISSP, GSEC, CBCP, BPCP, FSyl, CSyP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Advanced</td>
<td>Advanced</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Senior Manager - Physical Security</td>
<td>CPP, CFE, FSyl, CSyP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Superior</td>
<td>Superior</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Senior Manager - IT Security</td>
<td>CISSP, GSEC</td>
<td>Yes</td>
<td>Desirable</td>
<td>Yes</td>
<td>Yes</td>
<td>Superior</td>
<td>Superior</td>
<td>Yes</td>
<td>IT Security</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Senior Manager - Business Continuity Management</td>
<td>CBCP, MBCP</td>
<td>Yes</td>
<td>Desirable</td>
<td>Yes</td>
<td>Yes</td>
<td>Superior</td>
<td>Superior</td>
<td>Yes</td>
<td>Business Continuity Management</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Manager - Physical Security</td>
<td>CPP, PSP, CFE, FSyl, CSy</td>
<td>Desirable</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Good</td>
<td>Good</td>
<td>Yes</td>
<td>Physical Security</td>
<td>Desirable</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Manager - IT Security</td>
<td>CISSP, GSEC, GCFA, GCFE</td>
<td>Desirable</td>
<td>Desirable</td>
<td>No</td>
<td>Yes</td>
<td>Good</td>
<td>Good</td>
<td>Yes</td>
<td>IT Security</td>
<td>Desirable</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Manager - Business Continuity Management</td>
<td>CBCP, MBCP</td>
<td>No</td>
<td>Desirable</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Good</td>
<td>Basic</td>
<td>Business Continuity Management</td>
<td>Desirable</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
## Skills & Experience by Position

<table>
<thead>
<tr>
<th>Position</th>
<th>Qualifications</th>
<th>Planning</th>
<th>Training</th>
<th>Awareness</th>
<th>Physical</th>
<th>Security</th>
<th>Safety</th>
<th>Desirable</th>
<th>No</th>
<th>Desirable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advisor - Physical Security</td>
<td>PSP, PCI</td>
<td>No</td>
<td>Yes</td>
<td>Good</td>
<td>Basic</td>
<td>Physical</td>
<td>Security</td>
<td>Desirable</td>
<td>No</td>
<td>Desirable</td>
</tr>
<tr>
<td>Advisor - IT Security</td>
<td>GSEC, GCFA, GCFE</td>
<td>No</td>
<td>Yes</td>
<td>Good</td>
<td>Basic</td>
<td>IT Security</td>
<td>Desirable</td>
<td>No</td>
<td>Desirable</td>
<td></td>
</tr>
<tr>
<td>Advisor - Business Continuity Management</td>
<td>ABCP</td>
<td>No</td>
<td>Yes</td>
<td>Good</td>
<td>Basic</td>
<td>IT Security</td>
<td>Desirable</td>
<td>No</td>
<td>Desirable</td>
<td></td>
</tr>
<tr>
<td>Security Administrator</td>
<td>None</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>None</td>
<td>None</td>
<td>No</td>
<td>No</td>
<td>Desirable</td>
</tr>
</tbody>
</table>
Security Awareness Training Tools

Security awareness training should be an ongoing project. There should be several forms of training to ensure that interest is maintained and all parts of the company or organization are reached. Security awareness training can take the following forms:

- Security Environment Brochure for distribution to employees (please see the end of this section for an example)
- Anti-phishing training for email security, URL security, and social engineering (this form of training is available from third-party vendors)
- Posters
- Corporate intranet newsletters
- Group presentations
- Online training

Electricity Sub-Sector Safety Awareness Training Tools

The Canadian Electricity Association has produced several videos for use in electricity sub-sector safety training. The videos are available on YouTube as follows:

<table>
<thead>
<tr>
<th>Title</th>
<th>Link</th>
<th>QR Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electricity: The Invisible Killer - Construction Industry</td>
<td><a href="https://www.youtube.com/watch?v=pnasKXQQUtQ">https://www.youtube.com/watch?v=pnasKXQQUtQ</a></td>
<td><img src="https://www.example.com/qr-code.png" alt="QR Code" /></td>
</tr>
<tr>
<td>Electricité : le tueur invisible - L'industrie de la construction</td>
<td><a href="https://www.youtube.com/watch?v=CYIOL_5JIS8">https://www.youtube.com/watch?v=CYIOL_5JIS8</a></td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td>---------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Electricity: The Invisible Killer - Emergency First Responders</td>
<td><a href="https://www.youtube.com/watch?v=ipPEVp4HRmg">https://www.youtube.com/watch?v=ipPEVp4HRmg</a></td>
<td></td>
</tr>
</tbody>
</table>
Qualifications, Training and Awareness

Security Environment

Who is the Physical Threat?

Criminals
Criminals steal tools, equipment, and copper, or vandalize our property

Disasters
Random events that impact our ability to do business: flooding, fire emergencies, pandemics, extreme weather

Protesters
Members of the public may disagree with some of our projects, and employ their legal right to protest. Extremists within these groups may threaten our people

Our Own Employees
A very few employees engage in fraud, theft, or workplace violence

Industrial Espionage
Proprietary information related to business development and technology may be used by an adversary to strip XYZ Corp of its competitive advantage and gain a competitive edge, or by a foreign power to enhance their own capacity to develop without paying the full cost

Terrorists
The threat of terrorism at our facilities is very small, but as critical infrastructure asset owners we have a responsibility to ensure that we are aware of the threat and plan accordingly

Is the Threat to XYZ Corp Real?

Our Own Employees
- XYZ Corp has been defrauded of more than $300,000 in the past four years
- Two employees were terminated for purchasing card fraud totaling over $50,000; one of them was prosecuted, convicted, and was sentenced to restitution and probation
- Two employees were terminated for theft of more than $22,000 dollars worth of metal, which they had cashed in at a metal recycler
- We terminated several members of a criminal gang at one of our facilities who were involved in a scheme to defraud XYZ Corp
- Many employees don’t wear their access control cards, making it easier for an intruder to pass as an employee and complicating efforts to protect XYZ Corp
- During a recent social engineering audit an intruder was able to gain unescorted and unchallenged entry onto XYZ Corp floors wearing an ‘escort required’ visitor badge he had stolen during an earlier incursion

Criminals
- A pickup truck was stolen from the contractor parking lot during a shutdown at one of our power plants

Disasters
- Building power outage closed the head office for several days, requiring execution of business continuity and disaster recovery plans
- Flooding required execution business continuity and disaster recovery plans

Industrial Espionage
- We have had at least one instance of what we believe to be attempted industrial espionage at one of our power plants. The attempt was thwarted by the guards

What Programs or Activities do We Use to Execute our Strategies?

Strategy 1: Hardening our Security Posture
- Wearing access control cards
- Security policies
- Electronic access control, CCTV, security fencing, and intrusion detection systems
- Background checks and personnel risk assessments
- Vehicle and bag searches
- Mobile & static guards
- Crisis Management, Business Continuity, Threat Response, Disaster Recovery, Incident response, and Emergency Site Plans

Strategy 2: Security Awareness
- Online security awareness training
- Corporate communications
- Social engineering recognition training

Strategy 3: Reactive to Proactive
- Intelligence exchanges with:
  - CEA’s Security & Infrastructure Protection Committee
  - NERC’s Critical Infrastructure Protection Committee
  - NERC’s Electric Information Sharing and Analysis Center
  - RCMP Criminal Infrastructure Criminal Intelligence
  - Canadian Security Intelligence Service
- Liaison with local law enforcement at plant and office locations
- XYZ Corp’s Fraud Assessment Group and annual Fraud Risk Assessment to the Board Audit Committee
- Prosecution of criminals whenever possible
- Sabotage reporting standards
- Internal and external audits
- Coordination of cyber and physical security strategies and programs
- Frequent risk and vulnerability assessments
NERC
Within North America, the primary source of regulation for the electricity sub-sector is the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards.

NERC Critical Infrastructure Protection Standards
Reliability standards are enforceable in all interconnected jurisdictions in North America: the continental United States; the Canadian provinces of Alberta, British Columbia, Manitoba, New Brunswick, Nova Scotia, Ontario, Quebec, and Saskatchewan; and the Mexican state of Baja California Norte.

The Standards are available on Nerc.com in this section.
Change Management and Continuous Improvement

The threat to the Bulk Electric System is continually changing, and in order to remain relevant a security management program must change too.

**Performance Measurement**

The security management staff should be constantly looking for information that will allow them to measure the effectiveness of their security management program. The types of information that lends itself to measurement include (but are not limited to):

- Reported incidents
  - Injuries to any personnel, including adversaries
  - Dollar loss related to incidents
  - Outages related to incidents
- Access control card requests
  - Cards requested
  - Cards produced
  - Average amount of time to complete request
- Background checks
  - Total background checks
  - Percentage returned ‘not clear’
  - Number of personnel risk assessments
  - Number of personnel not cleared for hire
  - Total cost of background check program
- Number of threat vulnerability assessments conducted
- Number of requests for assistance from employees or management
- Number of actual or suspected sabotage events
- Safety statistics for security staff, including contract Security Officers
- Safety Near Misses reported by Security Officers

**Evaluation and Review**

The purpose of the review is to assess the validity and effectiveness of the security management program. Reviews should:

- Be conducted
  - when there is an increase in the threat
  - annually
  - after a major security incident (internal to the company or at another similar company or organization)
  - after the acquisition or divestment of a major asset
  - after a change in senior security management
  - after a change in legal requirements
  - prior to an audit (internal or external)
  - after an audit (internal or external)
  - when considered necessary by the owner/operator
• The results of the review should be approved, at a minimum, by the senior security manager within the organization

Management of Corrective Action
Change management is a formal process to ensure that changes indicated in the Evaluation and Review are actioned. The process should include:

• who is accountable for the change management process
• who is responsible for managing the change to each section of the security management program. For example, the person responsible for changes within the physical security measures section may not be the same person responsible for changes within the industrial control systems section
• an opportunity for all stakeholders to comment on the proposed change(s)
• a decision of whether or not the change is warranted or necessary
• a determination of the budget impact of the change(s)
• an analysis of how the change(s) will be integrated into the organization
• an implementation and communication plan for the change(s)
• approval for the change at the appropriate level of management