March 2019

DETECTION AND RESPONSE TO CYBERSECURITY THREATS ON BC HYDRO'S INDUSTRIAL CONTROL SYSTEMS

An independent audit report

www.bcauditor.com

OFFICE OF THE
Auditor General
of British Columbia

CONTENTS

Auditor General's comments 4

Report highlights 6

Summary 7

- Electric power systems are a critical infrastructure 7
- Standards protect against cascading failure of electric power systems 7
- Standards don't cover all systems and devices 7

Summary of recommendations 9

Response from BC Hydro 10

About the audit 11

- Background 11
  - Cybersecurity threats to ICS and critical infrastructure 11
  - The importance of cybersecurity monitoring and incident response 12
  - BC Hydro's electrical grid 12
  - Grid interconnections—BC Hydro to other western utilities 13
  - Mandatory standards in B.C. 14
- Audit scope 15
- Audit criteria summary 15
- Audit method 17

Audit objective and conclusion 18

- Audit objective 18
- Audit conclusion 18

Key findings and recommendations 19

- Delivering power to people in B.C. 19
  - Cybersecurity incidents could threaten the local delivery of power 19
- Preparing for cybersecurity incidents 19
  - Program for cybersecurity incidents is well-developed but missing some key information 19
- Detecting cybersecurity incidents 20
  - BC Hydro is unable to detect cybersecurity incidents on some system components 20
- Responding to and recovering from cybersecurity incidents 21
  - BC Hydro responds to the cybersecurity incidents it detects 21
  - BC Hydro prepares for recovery from cybersecurity incidents 21
- Improving preparation, detection and response 22
  - BC Hydro improves its preparation, detection and response to cybersecurity incidents 22

Audit quality assurance 23

Appendix A: complete audit criteria 24

The Office of the Auditor General of British Columbia would like to acknowledge with respect that we conduct our work on Coast Salish territories. Primarily, this is on the Lkwungen-speaking people's (Esquimalt and Songhees) traditional lands, now known as Victoria, and the W̱SÁNEĆ people's (Pauquachin, Tsartlip, Tsawout, Tseycum) traditional lands, now known as Saanich.

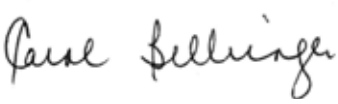
623 Fort Street
Victoria, British Columbia
Canada V8W 1G1
P: 250.419.6100
F: 250.387.1230
www.bcauditor.com

The Honourable Darryl Plecas
Speaker of the Legislative Assembly
Province of British Columbia
Parliament Buildings
Victoria, British Columbia
V8V 1X4

Dear Mr. Speaker:

I have the honour to transmit to the Speaker of the Legislative Assembly of British Columbia the report *Detection and Response to Cybersecurity Threats on BC Hydro's Industrial Control Systems.*

We conducted this audit under the authority of section 11(8) of the *Auditor General Act* and in accordance with the standards for assurance engagements set out by the Chartered Professional Accountants of Canada (CPA) in the CPA Canada Handbook – Canadian Standard on Assurance Engagements (CSAE) 3001 and Value-for-money Auditing in the Public Sector PS 5400.



Carol Bellringer, FCPA, FCA
Auditor General
Victoria, B.C.
March 2019

AUDITOR GENERAL'S COMMENTS

CAROL BELLRINGER, FCPA, FCA
Auditor General

THROUGH AN EXTENSIVE electric power system, BC Hydro provides electricity to 95% of the people in British Columbia. The system is considered "critical infrastructure" because it affects every aspect of our lives and is essential to our economy.

In this audit, we focused on how BC Hydro is managing the cybersecurity risks to its industrial control systems (ICS), which form an integral part of its electric power infrastructure. Globally, the energy sector is one of the most cyberattacked of all critical infrastructure sectors. Cybersecurity is no longer only about prevention, but also about quickly detecting and responding to attacks—because some are almost certain to get through.

We found that BC Hydro is effectively managing cybersecurity risk by detecting and responding to cybersecurity incidents on the parts of its electric power system covered by mandatory reliability standards—standards that are accepted across Canada and the U.S. However, BC Hydro needs to expand its detection efforts because the standards focus on ensuring reliable operation of the power system as a whole, but don't cover all components of the system. Any components that don't fall under the mandatory standards may be vulnerable to cybersecurity threats and should be monitored.

The components that BC Hydro isn't looking at—generally equipment of lower power capacity—may allow cybersecurity incidents to cause localized outages and, in aggregate, could have a large effect on the overall power system. The B.C. system is part of an interconnected power grid with Alberta and the western United States. The standards BC Hydro follows help to prevent a power failure in B.C. from cascading to other parts of the grid outside of the province.

For security reasons, we are not disclosing findings that could expose details of BC Hydro's power system. Instead, we provided BC Hydro with a detailed technical report that specifically outlines our findings

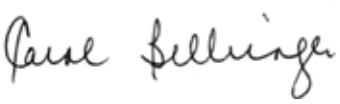
AUDITOR GENERAL'S COMMENTS

and recommendations.

We recommended that BC Hydro work on:

- assessing the cybersecurity risk to make sure appropriate detection and response measures are implemented
- maintaining an inventory of its hardware and software components, regardless of whether they fall under the mandatory standards
- implementing detection mechanisms and monitoring, in real time, for unusual activity on ICS-related systems and devices not currently under the mandatory standards

I would like to thank everyone at BC Hydro for their cooperation and support during our work on this audit.



Carol Bellringer, FCPA, FCA
Auditor General
Victoria, B.C.
March 2019

REPORT HIGHLIGHTS

BC HYDRO'S ELECTRIC POWER SYSTEM:

CRITICAL **infrastructure**

ESSENTIAL to our **lives** and **economy**

Provides electricity to **95%** of B.C.

Audit focused on **ICS cybersecurity incident detection** and **response**

BC Hydro **complies with reliability standards** accepted across North America

Following standards **protects against** MAJOR POWER FAILURES

Standards DON'T COVER **all components** of power system

BC Hydro **MONITORS FOR CYBERSECURITY INCIDENTS**, but **unable to detect** for most lower power components

Cybersecurity incidents involving lower power components could add up to cause **LOCALIZED OUTAGES**

BC Hydro needs to **EXPAND CYBERSECURITY DETECTION** to include system components outside standards

SUMMARY

Electric power systems are a critical infrastructure

Governments use the term critical infrastructure to describe processes, systems, assets and services that are essential for society and the economy to function. BC Hydro's electric power system is one such example of critical infrastructure. As part of the energy sector in the province, BC Hydro generates and provides electricity across B.C. A major power failure could cause significant interruptions and tremendous losses to businesses and people in B.C.

Cybersecurity attacks against the energy sector have increased dramatically around the globe and pose significant risk to the electric power infrastructure. But cybersecurity is no longer defined by the prevention of attacks—attackers will eventually succeed. Instead, cybersecurity is defined by how quickly an organization can detect, and respond to, an attack.

Standards protect against cascading failure of electric power systems

BC Hydro's electric power system is regulated by a set of mandatory standards designed to protect the collective power system to which BC Hydro belongs. The standards, approved for adoption by the British Columbia Utilities Commission, are largely based on the North American Electric Reliability Corporation reliability standards from the United States and set out requirements for the reliable operation of the power system. The standards are specifically aimed at reducing risk to the power system as a whole, including connections with other jurisdictions. They do this by requiring utilities to have both preventive measures—designed to prevent cybersecurity threats from being successful in the first place—and detective measures, since eventually some attacks will succeed.

Standards don't cover all systems and devices

Our audit examined whether BC Hydro was effectively managing cybersecurity risk by detecting, and responding to, security incidents on its industrial control systems operating the electric power infrastructure.

We concluded that BC Hydro is effectively managing cybersecurity risk by detecting, and responding to, security incidents on its electric power infrastructure for system components where mandatory standards apply. However, it is missing the ability to detect cybersecurity incidents on most components where the standards do not apply. As a result, a security incident that goes undetected may cause localized power outages in B.C. and increases risks to the broader system.

Even though BC Hydro is detecting and analyzing cybersecurity incidents that cover systems and devices where mandatory standards apply, it has not

SUMMARY

established monitoring and detection mechanisms for a substantial portion of its systems and devices where mandatory standards are not yet in effect. This may delay or prevent discovery and response should an incident occur.

Specifically, we found that BC Hydro:

- has a well-developed program to prepare for cybersecurity incidents, but it is missing some key information resources
- can't monitor for some cybersecurity incidents, as it is missing detection mechanisms and monitoring on some system components
- can respond to the cybersecurity incidents it detects
- has the capability to respond and recover when an incident occurs
- has processes in place to improve its responses to cybersecurity incidents

To be fully effective, BC Hydro needs to monitor for, detect and respond to cybersecurity incidents on all its systems—regardless of whether they currently fall under the mandatory standards. Building a strong capability for cybersecurity monitoring and incident response is fundamental to good cybersecurity practice.

SUMMARY OF RECOMMENDATIONS

WE RECOMMEND THAT BC HYDRO:

1. assess cybersecurity risk over its entire industrial control systems (ICS) environment to ensure appropriate detection and response measures are implemented.

2. maintain an inventory of hardware and software components, including their configuration settings, for all ICS-related systems and devices, regardless of whether they currently fall under the mandatory standards.

3. implement detection mechanisms and monitor, in real time, for anomalous activity on ICS-related systems and devices not currently under the mandatory standards.

RESPONSE FROM BC HYDRO

BC Hydro would like to thank the Office of the Auditor General for conducting the audit of Detection and Response to Cybersecurity Threats on our Industrial Control Systems (ICS) and for identifying opportunities to improve in this area.

As stated in the report, BC Hydro has a well-developed cybersecurity incident program and is able to respond to cybersecurity incidents. After investing over $30M over two years in our cyber and physical security programs, BC Hydro is operating within the mandatory standards and the legal requirements in British Columbia. BC Hydro has ongoing programs to meet anticipated compliance requirements as they become law in British Columbia.

BC Hydro also acknowledges the findings in the audit report that our cybersecurity practices need to consider all aspects of our industrial control systems, beyond those that impact the critical facilities involved in the production and distribution of power.

BC Hydro supports the recommendation that we assess cyber security risk over our entire ICS environment to ensure appropriate detection and response measures are implemented. We will extend our assessment of cyber security risks to areas of the power system not already covered by mandatory standards and legal requirements in British Columbia. We will use a risk based approach to prioritize mitigation measures where needed.

We also support the recommendation that we maintain an inventory of hardware and software components, including their configuration settings, for all ICS related systems and devices regardless of whether or not they currently fall under the mandatory standards. Based on the risk assessment, we will conduct a gap analysis and follow a risk based approach to develop mitigation plans for those areas not already inventoried.

Finally, based on the above risk assessment and wherever technically possible, we agree to extend detection mechanisms and real time monitoring for anomalous activity on ICS related systems that are not currently under the mandatory standards.

Our customers can be confident in our ability to provide reliable, affordable, clean electricity throughout B.C. This audit and its recommendations support us in achieving that mission.

ABOUT THE AUDIT

BACKGROUND

British Columbia Hydro and Power Authority (BC Hydro) is the largest public utility in the province. It generates and delivers electricity to over four million people across B.C., enabling social and economic well-being, as well as a myriad of life-enhancing conveniences.

BC Hydro produces electricity and delivers it to consumers through a sophisticated network of physical infrastructure (e.g., generators, transmission and distribution lines, substations, poles, and transformers) along with control devices (e.g., circuit breakers) and systems (e.g., software that controls the flow of electricity).

ABOUT BC HYDRO

BC Hydro is a provincial Crown corporation under the responsibility of the Ministry of Energy, Mines and Petroleum Resources.

BC Hydro's strategic direction emphasizes electrical safety and reliability to help meet its goal to "safely keep the lights on" throughout B.C.

Delivering electricity is complex and highly dependent on industrial control systems (ICS). ICS is a collective term for different types of computerized control systems, including devices, systems, networks and controls that operate and automate industrial processes. ICS are used in nearly every industrial sector, such as the energy, transportation, water treatment and manufacturing industries.

ICS devices range from sensors that collect electricity flow data, to transformers that regulate electricity voltage, to circuit breakers that can open and close circuits. BC Hydro uses thousands of interconnected ICS devices to automate and control the flow of electricity at its 30 hydroelectric generating plants and 300 transmission and distribution stations.

Cybersecurity threats to ICS and critical infrastructure

Governments describe critical infrastructure as systems and services that are essential for the functioning of a society and economy. Public Safety Canada lists the following as its ten critical infrastructure sectors on its website:

- energy and utilities
- information and communication technology
- finance
- manufacturing
- food
- safety
- government
- transportation
- health
- water

ABOUT THE AUDIT

Today's electric power ICS are becoming more advanced and interconnected than ever before. Many ICS that were previously used in isolated environments are now accessible to allow users to remotely monitor and control processes.

The increased integration of information technology (IT) and ICS provides greater grid reliability and efficiency, but it also introduces new vulnerabilities and new risk. Cybersecurity threats in an environment of increased interconnection have a correspondingly greater potential to cause more disruption to the power grid.

Cybersecurity threats have proliferated in recent years. Threats against traditional IT targets (e.g., financial systems) continue to grow, but, increasingly, the attackers—cyber criminals, activists and nation-states—are shifting their focus to ICS in critical infrastructure sectors. Advanced ICS in critical infrastructure sectors have become attractive targets for cybercrime. The energy sector is one of the most attacked infrastructures.

If a cybersecurity threat succeeds in causing a major power failure, it could cause significant interruptions and tremendous losses to businesses and people in B.C. The degree of impact may range from minor disruptions to life threatening. A large-scale *lights out* puts a community at risk when all of the services requiring electric power go down, too—e.g., heat, water supply, transportation and communication.

The importance of cybersecurity monitoring and incident response

Cyberattacks are now stealthy, multi-pronged and persistent, and it is only a matter of time until the advanced attackers get in. This is why it is important for organizations to:

- recognize the inevitability of attacks
- be proactive
- have effective means to detect a breach when it happens
- react quickly to limit the impact of the attack

Building a strong capability for cybersecurity monitoring and incident response is fundamental to good cybersecurity practice.

Cybersecurity success is no longer defined by the ability to prevent attacks, but by how quickly organizations can detect and respond to the attacks. This is an important shift. Organizations that overestimate their ability to prevent attacks often learn about successful attacks long after they have happened and the damage has been done.

BC Hydro's electrical grid

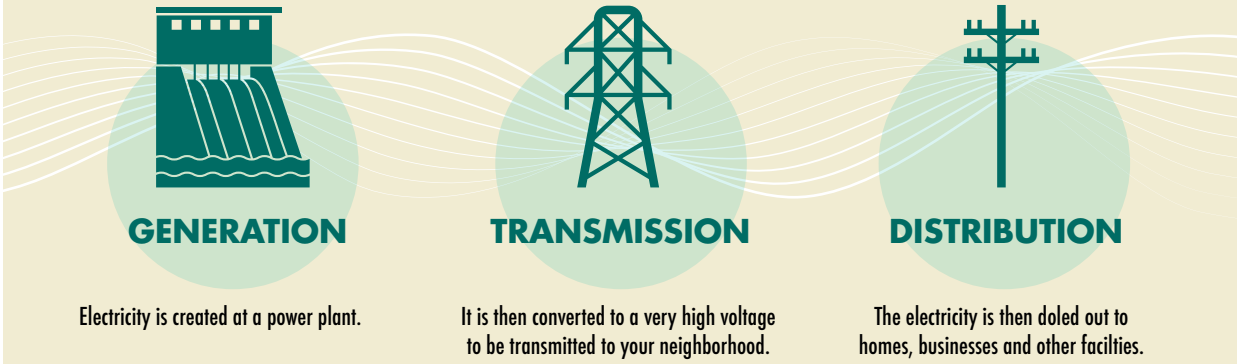
BC Hydro's electrical network, or *grid*, comprises three distinct functions (see Exhibit 1):

- **generation** of electricity at hydroelectric dams and other generating stations
- **transmission** of electricity over long distances through high-voltage transmission lines to local distribution stations
- **distribution** of electricity to commercial and residential consumers by first reducing the voltage, then delivering it via local distribution lines

BC Hydro centrally controls all three functions to balance electricity supply with demand, while maintaining grid stability.

ABOUT THE AUDIT

Exhibit 1: The three functions of an electric utility



Source: energy.gov, modified by the Office of the Auditor General of British Columbia

Grid interconnections—BC Hydro to other western utilities

North America's electric power system is made up of four distinct power grid regions (see Exhibit 2).

Even though electric utilities within a given region operate independently, they are interconnected with one another. This helps ensure that a steady supply of electricity can be available to meet all demand within the region.

B.C.'s electrical grid is in the western interconnection region (see Exhibit 2) and is interconnected with the grids of Alberta, 14 western states in the United States, and the northern portion of the Baja California state in Mexico. The interconnections of all the grids allow transmission of power throughout the western region and enables BC Hydro to ensure electrical energy is continuously available in B.C. The interconnections also allow supply and demand to be balanced throughout the western interconnection region.

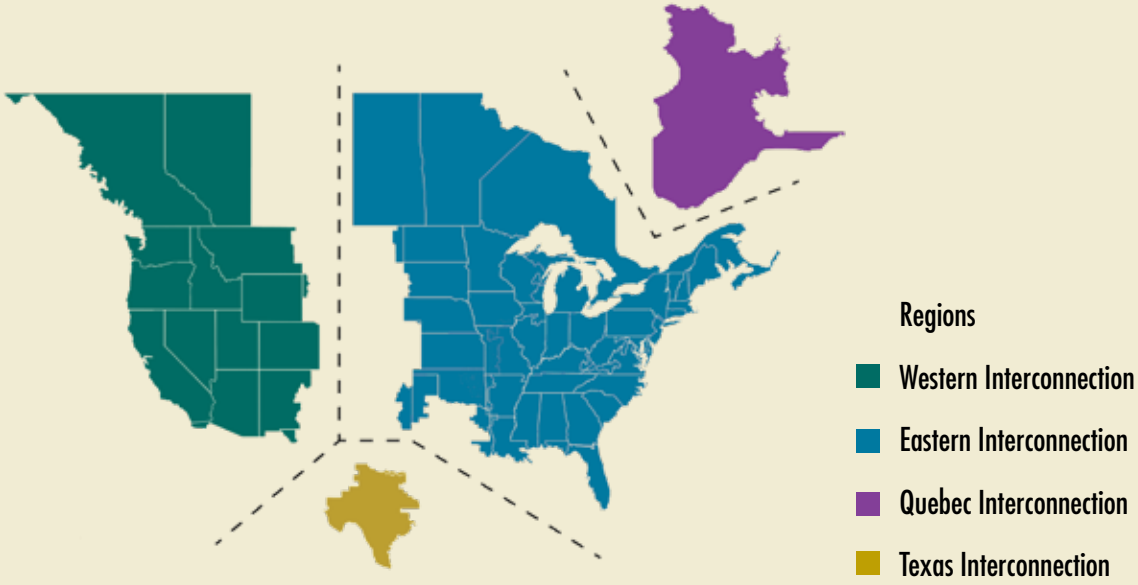
A side effect of the interconnectivity is the possibility that a large failure in one part of the grid can cascade through to multiple utilities, causing widespread power outages, which happened during the North America blackout of 2003. Over 50 million people were without power in the most widespread blackout in history.

To prevent such cascading failures, a common set of standards—the North American Electric Reliability Corporation (NERC) reliability standards—was created.

The NERC reliability standards do not apply to all components of the electrical grid. The standards focus on the planning, operation and maintenance of those grid components that operate at higher voltage and power levels. These standards are meant to ensure the reliable operation of the electrical grid as a whole, including interconnections between electric utilities in the four grid regions (e.g., between BC Hydro and Alberta Electric System Operator). The

ABOUT THE AUDIT

Exhibit 2: North America's electric power grid regions



Source: nerc.com, modified by the Office of the Auditor General of British Columbia

NERC reliability standards include some ICS security requirements. These are also focused on the larger grid and system control centres, rather than on local parts of the grid in B.C.

Mandatory standards in B.C.

Some components of BC Hydro's electric power infrastructure are subject to the standards, and some are not. Through the authority of the British Columbia Utilities Commission, B.C. adopted the Mandatory Reliability Standards (the standards), which are largely based on the NERC standards from the United States. B.C.'s standards set out planning and operating requirements for the power grid and include cybersecurity requirements for ICS. However, they do not apply to all ICS operated by utilities (e.g., BC Hydro). For example, the standards apply to ICS that, if unavailable, would adversely affect the reliable operation of the larger power grid in the western interconnection region. They do not apply to those facilities used to handle lower levels of electric power.

Systems and devices that fall under the standards are generally dealing with greater quantities of electric power—quantities large enough that disturbances to them could affect the reliable operation of BC Hydro's major system components and interconnections to other utilities in the western interconnection region.

Systems and devices that affect smaller quantities of electrical energy are not subject to the standards. These systems and devices are of less importance to the reliability of the larger grid, but, nonetheless, are important to the reliability of local parts of the B.C. grid—an area not yet addressed by the standards.

ABOUT THE AUDIT

ORGANIZATIONS RESPONSIBLE FOR MONITORING COMPLIANCE WITH STANDARDS

The North American Electric Reliability Corporation (NERC), a standard-making body in the United States, was established for the purpose of developing and enforcing standards for power grid reliability in North America.

The Western Electricity Coordinating Council (WECC), a regional entity established in the United States, is responsible for developing standards as well as monitoring compliance with the NERC mandatory standards for the western interconnection region (B.C. belongs to the western interconnection region).

However, in B.C., it is the British Columbia Utilities Commission that monitors B.C. utilities for compliance with the standards. It does this by engaging WECC to administer compliance and monitoring activities on its behalf.

AUDIT SCOPE

Our audit focused on BC Hydro's ICS, which form an integral part of its electric power infrastructure. All ICS components housed in the control centre and at sites for power generation, transmission and distribution across the province were in scope for the audit.

Some components of BC Hydro's power infrastructure within our scope were subject to mandatory standards and the related compliance audits conducted by the Western Electricity Coordinating Council (WECC). Because of the overlap in audit areas for cybersecurity incident detection and response, we limited the extent of testing for these ICS components in our audit.

CYBERSECURITY INCIDENT

For the purposes of this audit, we defined a cybersecurity incident as any event or situation with the potential to threaten the security of the IT (traditional computing devices) and ICS components that form a part of BC Hydro's electric power system.

AUDIT CRITERIA SUMMARY

We developed our audit objective and criteria based on the four-part National Institute of Standards and Technology (NIST) cybersecurity framework and the incident response guide (see Exhibit 3).

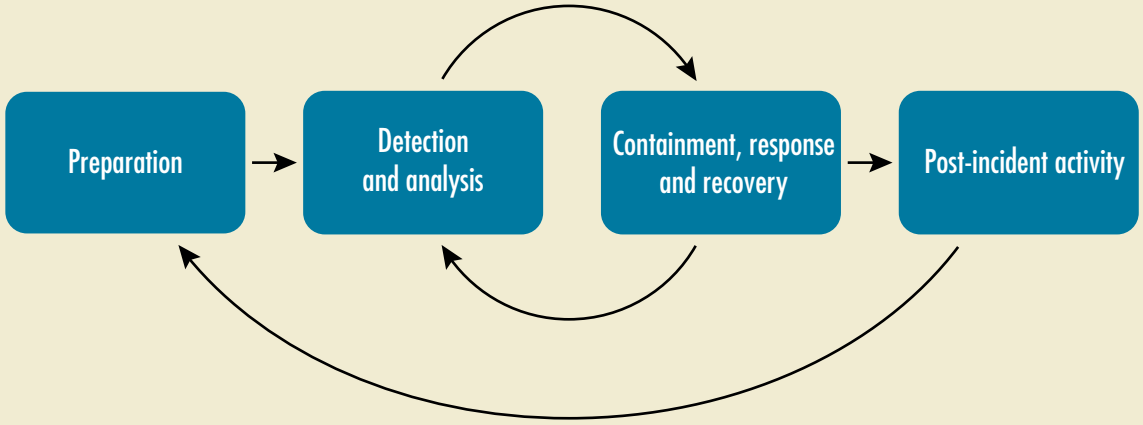
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

The National Institute of Standards and Technology (NIST) is an agency of the United States Department of Commerce with a mission to promote innovation and industrial competitiveness.

NIST first published its Cybersecurity Framework in 2014. Originally aimed at operators of critical infrastructure, the guidance on how to respond to cybersecurity incidents can now be used by any private sector organization.

ABOUT THE AUDIT

Exhibit 3: NIST-based cybersecurity framework on incident response and basis for the audit lines of enquiry



Incident response phase	Lines of enquiry
Preparation	There should be a program established to detect and respond to cybersecurity incidents that impact the electric power infrastructure.
Detection and analysis	Cybersecurity incidents, which may impact the electric power infrastructure, should be detected and analyzed.
Containment, response and recovery	Cybersecurity incidents should be contained, responded to and recovered from to minimize impact to electric power infrastructure and restore systems to normal operation.
Post-incident activity	Post-cybersecurity incident activities should be used to improve incident response capability for protecting the electric power infrastructure.

Source: Office of the Auditor General of British Columbia, based on the NIST cybersecurity framework

In Appendix A, we provide a list of control-based audit criteria for each line of enquiry.

ABOUT THE AUDIT

AUDIT METHOD

We carried out our audit work between January 2018 and October 2018. The period we looked at was from September 2017 to May 2018. The audit report is dated March 8, 2019, the date on which the audit team finished obtaining the evidence used to determine the findings and conclusions of the report.

Our work involved:

- interviewing BC Hydro staff on incident detection and response practices related to the protection of the electric power infrastructure
- visiting BC Hydro's system control centre, two generating stations and two transmission and distribution stations to observe and evaluate the control environment
- reviewing policies, procedures and other documentation from BC Hydro and the British Columbia Utilities Commission for supporting evidence of control implementation
- verifying processes to confirm effectiveness of controls implemented
- reviewing and assessing the compliance audit work reported by WECC to confirm results

AUDIT OBJECTIVE AND CONCLUSION

AUDIT OBJECTIVE

THE OBJECTIVE OF OUR AUDIT was to determine whether BC Hydro was effectively managing cybersecurity risk by detecting, and responding to, security incidents on its industrial control systems operating the electric power infrastructure.

AUDIT CONCLUSION

BC Hydro is effectively managing cybersecurity risk by detecting, and responding to, security incidents on its electric power infrastructure for system components where mandatory standards apply. However, it is missing the ability to detect cybersecurity incidents on most components where the standards do not apply. As a result, a security incident that goes undetected may cause localized power outages in B.C. and increases risks to the broader system. To be fully effective, BC Hydro needs to address cybersecurity risk to its entire electric power infrastructure.

Specifically, we found that BC Hydro:

- has a well-developed cybersecurity incident program, but it is missing some key information resources needed to prepare for incident handling
- can't monitor for some cybersecurity incidents as it is missing detection mechanisms and monitoring on some system components
- can respond to the cybersecurity incidents it detects
- has the capability to respond to, and recover from, cybersecurity incidents
- has processes in place to improve its responses to cybersecurity incidents

KEY FINDINGS AND RECOMMENDATIONS

DELIVERING POWER TO PEOPLE IN B.C.

Cybersecurity incidents could threaten the local delivery of power

Undetected cybersecurity incidents present risk to BC Hydro, and to people and businesses in B.C., so it is important to be proactive and have effective means to detect an attack and respond quickly to limit its impact. The degree of impact may range from minor disruption to life threatening.

BC Hydro's electric power system must comply with the mandatory standards—this is important for the reliable operation of major components of the electrical grid in B.C. and for interconnections between other utilities in the western interconnection region.

Complying with the standards means that BC Hydro is effectively managing the cybersecurity risk for most of its industrial control systems (ICS) related systems and devices (those that fall under the standards), but not all. Specifically, BC Hydro cannot be certain of its level of cybersecurity risk until it assesses risk for its entire ICS environment—not just the systems that fall under the mandatory standards.

BC Hydro has mechanisms to detect and respond to cybersecurity incidents. However, detection and monitoring are missing for many of the ICS-related systems and devices that do not fall under the standards. BC Hydro relies on these systems and devices for power delivery within the province, so the lack of monitoring increases the risk of localized disruption.

RECOMMENDATION 1: *We recommend that BC Hydro assess cybersecurity risk over its entire industrial control systems (ICS) environment to ensure appropriate detection and response measures are implemented.*

PREPARING FOR CYBERSECURITY INCIDENTS

Program for cybersecurity incidents is well-developed but missing some key information

An incident response program helps organizations respond to incidents effectively and efficiently. Substantial planning and resources are required to handle incidents successfully.

We determined whether BC Hydro has:

- a formal incident response process for handling incidents

- dedicated tools and resources for communication of incidents and coordination of incident responses
- a complete inventory of hardware as a foundation for incident detection and response
- mitigation software for quickly restoring systems and recovering from an incident

We found that BC Hydro:

- has established a formal incident response program
- maintains a complete inventory of all its system components where mandatory standards apply, but not for most of the components where the standards do not apply
- has all the expected tools and resources needed in preparation for incident handling and system recovery
- has up-to-date system software for quickly recovering from an incident

BC Hydro can't monitor for some cybersecurity incidents, as it has not maintained a complete inventory of all its system components in preparation for incident handling. This could slow down recovery from cybersecurity incidents.

RECOMMENDATION 2: *We recommend that BC Hydro maintain an inventory of hardware and software components, including their configuration settings, for all ICS-related systems and devices, regardless of whether they currently fall under the mandatory standards.*

DETECTING CYBERSECURITY INCIDENTS

BC Hydro is unable to detect cybersecurity incidents on some system components

Early detection of incidents is important because the consequences of an attack become more severe as time goes on. Attackers often use footholds gained on one device or system to begin attacking others, so accurately detecting and assessing possible incidents helps reduce the likelihood that an incident will expand. It also allows for prioritization and allocation of response resources. To aid in detection and assessment, normal behaviour of systems must be documented so the systems can be compared against current activity.

We determined whether BC Hydro:

- has detection mechanisms and monitors for cybersecurity incidents, in real time, to promptly detect anomalous activity
- has documented normal system behaviour as a comparison tool
- is able to analyze and validate incidents to plan its response

We found that BC Hydro:

- has tools and processes to identify and detect anomalous activity, and monitors, in real time, system and network activity for cybersecurity events affecting system components where mandatory standards apply, but not for all components where the standards do not apply

- has documented expected system activity to help detect cybersecurity events—again, for system components where the mandatory standards apply, but not for those components where the standards do not apply
- analyzes and validates incidents

Because essential detection and monitoring mechanisms were not in place for all system components, BC Hydro cannot know if some of its systems have been compromised.

RECOMMENDATION 3: *We recommend that BC Hydro implement detection mechanisms and monitor, in real time, for anomalous activity on ICS-related systems and devices not currently under the mandatory standards.*

RESPONDING TO AND RECOVERING FROM CYBERSECURITY INCIDENTS

BC Hydro responds to the cybersecurity incidents it detects

Prompt response to incidents helps limit the impact and provides time to develop a tailored remediation strategy. During our audit, BC Hydro responded promptly to thousands of cybersecurity incidents by prioritizing its response based on the type and severity of incidents.

We determined whether BC Hydro:

- gathers and preserves evidence for analysis
- has containment strategies for remediation
- responds to incidents it detects
- tests its responses to ensure they are adequate

We found that BC Hydro:

- gathers and preserves evidence for analysis
- has incident response plans that include containment and remediation strategies
- follows its response processes and procedures
- tests its responses by categorizing, interpreting and investigating incidents

BC Hydro prepares for recovery from cybersecurity incidents

We could not examine all of BC Hydro's recovery capabilities in this audit because none of the incidents that happened during our examination period required more than a simple recovery.

We determined whether BC Hydro:

- executes and maintains recovery procedures to enable timely restoration of systems and to ensure staff are prepared when incidents happen

We found that BC Hydro:

- tests its recovery processes and plans regularly

KEY FINDINGS AND RECOMMENDATIONS

IMPROVING PREPARATION, DETECTION AND RESPONSE

BC Hydro improves its preparation, detection and response to cybersecurity incidents

An important step that is often overlooked after a cybersecurity incident is a feedback process. Feedback allows organizations to review the effectiveness of their incident-handling process and helps them identify areas for improvement in the response process.

We determined whether BC Hydro:

- has a feedback process to improve future incident detection, response and recovery strategies to protect the electric power infrastructure

We found that BC Hydro:

- has a feedback process and improves its incident detection, response and recovery activities

AUDIT QUALITY ASSURANCE

We conducted this audit under the authority of section 11 (8) of the *Auditor General Act* and in accordance with the standards for assurance engagements set out by the Chartered Professional Accountants of Canada (CPA) in the *CPA Canada Handbook* – Canadian Standard on Assurance Engagements (CSAE) 3001 and Value-for-money Auditing in the Public Sector PS 5400. These standards require that we comply with ethical requirements and conduct the audit to independently express a conclusion on whether or not the subject matter complies in all significant respects to the applicable criteria.

The office applies the CPA Canadian Standard on Quality Control 1 (CSQC) and, accordingly, maintains a comprehensive system of quality control, including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements. In this respect, we have complied with the independence and other requirements of the code of ethics applicable to the practice of public accounting issued by the Chartered Professional Accountants of BC, which are founded on the principles of integrity, objectivity and professional competence, as well as due care, confidentiality and professional behaviour.

APPENDIX A: COMPLETE AUDIT CRITERIA

We developed our audit objective and criteria using the following good practice guides:

- NIST Framework for Improving Critical Infrastructure Cybersecurity
- NIST 800-61R2 Computer Security Incident Handling Guide

Audit criteria	
Line of enquiry 1:	There should be a program established to detect and respond to cybersecurity incidents that impact the electric power infrastructure.
1.1	BC Hydro should have a formal cybersecurity incident handling program to help minimize the impact of incidents since not all incidents can be prevented.
1.2	BC Hydro should have communication tools and facilities dedicated for responding to cybersecurity incidents to allow timely and coordinated response.
1.3	BC Hydro should have prepared information resources, such as an inventory of hardware, software and their configurations to identify and analyze incidents.
1.4	BC Hydro should have incident analysis hardware and software so that resources needed for analysis and recovery are ready to handle incidents.
1.5	BC Hydro should have incident mitigation software so that appropriate software needed to restore systems and recover quickly is available.
Line of enquiry 2:	Cybersecurity incidents, which may impact the electric power infrastructure, should be detected and analyzed.
2.1	BC Hydro should employ tools to identify common precursors (i.e., early indicators) of attack.
2.2	BC Hydro should have defined processes to help analyze and validate incidents.
2.3	BC Hydro should appropriately document and prioritize incidents.
2.4	BC Hydro should detect anomalous activity in a timely manner and determine the potential impact of events.
2.5	BC Hydro should monitor, in real time, the information systems and devices to identify cybersecurity events and verify the effectiveness of protective measures.
2.6	BC Hydro should maintain and test detection processes and procedures to ensure timely and adequate validation of anomalous events.

APPENDIX A

Audit criteria	
Line of enquiry 3:	Cybersecurity incidents should be contained, responded to and recovered from to minimize impact to electric power infrastructure and restore systems to normal operation.
3.1	BC Hydro should gather and preserve evidence for analysis.
3.2	BC Hydro should identify the source of cybersecurity attacks to limit impact.
3.3	BC Hydro should have containment strategies for remediation.
3.4	BC Hydro should follow response processes and procedures to ensure timely response to detected cybersecurity events.
3.5	BC Hydro should coordinate response activities with internal and external stakeholders, as appropriate.
3.6	BC Hydro should conduct testing to ensure adequate response and support recovery activities.
3.7	BC Hydro should perform activities to prevent expansion of an event, mitigate its effects and eradicate the incident.
3.8	BC Hydro should execute and maintain recovery processes and procedures to ensure timely restoration of systems or assets affected by cybersecurity events.
3.9	BC Hydro should coordinate recovery activities with internal and external stakeholders, as appropriate.
Line of Enquiry 4:	Post-cybersecurity incident activities should be used to improve incident response capability for protecting the electric power infrastructure.
4.1	BC Hydro should have a feedback process to improve future incident detection, response and recovery.
4.2	BC Hydro should retain evidence of incidents and response based on retention requirements for post-event analysis.

AUDIT TEAM

Morris Sydor,
Deputy Auditor General

Ada Chiang,
Director, IT Audit

John Bullock,
Senior IT Audit Specialist

Greg Morhart,
IT Audit Manager

SUBJECT MATTER EXPERT

Jason Grimbeek

OFFICE OF THE
Auditor General
of British Columbia

Location

623 Fort Street
Victoria, British Columbia
Canada V8W 1G1

Office Hours

Monday to Friday
8:30 am – 4:30 pm

Telephone: 250-419-6100
Toll free through Enquiry BC at: 1-800-663-7867
In Vancouver dial: 604-660-2421

Fax: 250-387-1230

Email: bcauditor@bcauditor.com

Website: www.bcauditor.com

This report and others are available at our website, which also contains further information about the office.

OFFICE OF THE
Auditor General
of British Columbia