Deloitte.

CYBER THREAT & RISK ASSESSMENT

BC Hydro

Private and confidential

September 17, 2021

TABLE OF CONTENTS

EXECUTIVE SUMMARY

INTRODUCTION

In its FY22 Revenue Requirements Application (RRA), BC Hydro outlined increases in its capital and operating budgets to enhance its cybersecurity program and to augment its security team in order to address evolving cybersecurity threats to critical infrastructure and the bulk electric system (BES). In its Decision and Order (G-1187-21) the British Columbia Utilities Commission (BCUC) approved the increases to BC Hydro's cybersecurity budget, but also issued two directives to BC Hydro regarding its cybersecurity program. The first, Directive 8, mandated that BC Hydro was to "undertake a Cyber Risk Assessment of all of its cyber assets and to notify the BCUC of any action that has been or needs to be taken on any immediate or time-sensitive concerns".

Through its second directive (Directive 9), the BCUC ordered BC Hydro to "develop a company-wide, comprehensive Cyber Security Plan that encompasses BC Hydro and its subsidiaries and third parties with whom it interfaces". This plan is to be completed within one year of the issuance of the decision and is to be informed by the cyber risk assessment report delivered under Directive 8.

BC Hydro engaged Deloitte to conduct a cyber risk assessment in support of its response to Directive 8. This document outlines the objectives, scope and approach for this assessment as well as a series of observations and recommendations designed to build upon BC Hydro's enterprise cyber security program and improve its cyber risk posture. As indicated in the Concluding Statement below, opportunities for improvement were identified; however no "immediate or time-sensitive concerns" were noted within the scope and timeframe of this assessment.

SCOPE

BCUC's Directive 8 ordered that BC Hydro undertake a cyber risk assessment of its cyber assets. Given the compressed timeline for the review, a risk-based approach was taken to focus on asset categories that are most commonly targeted by threat actors, namely: 1) corporate IT assets (including certain systems and assets which support MRS compliance), 2) operational technology (OT) assets covered under the Mandatary Reliability Standards (MRS), and specifically, the Critical Information Protection (CIP) standards and 3) OT assets that are not covered under the MRS CIP standards.

APPROACH

This project was delivered over seven weeks between July and September, following the approach outlined below.

Threat and risk assessment

Organizations within the energy and resources (E&R) industry (and the electric power sector in particular) are increasingly being targeted by malicious actors because of the intellectual property they hold, their susceptibility to ransomware and related extortion models due to the critical services they provide and their importance to national and economic security. These motivating factors, in combination with the inherent complexity of the OT and IT environments used to deliver services, make cyber security a critical risk mitigation capability.

In order to conduct this assessment, it was first necessary to identify key cybersecurity threats and risks that are relevant to the broader power sector, and more specifically to BC Hydro. This enabled a risk-based assessment of cyber capabilities at BC Hydro in the context of specific threat scenarios, with a focus on corporate IT assets and OT assets. Key threat scenarios were selected based on available threat intelligence and a review of relevant bulletins and advisories issued by the Canadian Centre for Cyber Security for the Canadian Electricity Sector. The key threat scenarios considered in this assessment include:

1. **Major Ransomware Outbreak** – A major ransomware outbreak within BC Hydro's network results in service disruption and data loss, with the threat actor threatening data exposure should the ransom not be paid.
2. **Espionage by Advanced Persistent Threat (APT)** - An Advanced Persistent Threat (APT) group embeds themselves into BC Hydro systems to steal intellectual property and/or to position malicious tools to be used at a later date to potentially disrupt the electric system.
3. **Supply Chain Attack Introducing Compromised Software** - A cyber-attack on a supplier of equipment, software or services to BC Hydro results in a backdoor being established into BC Hydro's network, providing cybercriminals with access to key systems to launch further attacks.
4. **Insider Attack Facilitating Data Leakage** - The accounts of an insider with access to sensitive information (either by malicious insider intent or by compromise of an employee's account) is used to access and exfiltrate data, resulting in a data breach.
5. **Business Email Compromise (BEC)** - An attack launched through targeted emails to BC Hydro employees leads to financial fraud.
6. **Compromise of Exposed Network Services** - A successful compromise of external network services leads to unauthorized access to BC Hydro systems.

Capability assessment

An assessment of cyber capabilities was conducted, based on interviews with BC Hydro representatives and on review of documentation (including a review of recently completed audits and reviews of BC Hydro's cyber program and capabilities). This was a point-in-time assessment, based on available information and management's representation of BC Hydro's control environment. This review was aligned to the NIST Cybersecurity Framework (CSF), and created an integrated view of cyber capabilities based on prior targeted assessments while also evaluating BC Hydro's enterprise cyber program for its IT, MRS OT and non-MRS OT environments.

The assessment reviewed the design of capabilities in place within BC Hydro's cyber program but did not include testing of the effectiveness of cybersecurity controls due to the breadth of the scope and the time available. Further, it was focused on BC Hydro's internal, enterprise security program and did not include a review of BC Hydro's subsidiaries or third-party relationships.

Validation and reporting

Upon completion of the capability assessment, results were validated with the appropriate stakeholders at BC Hydro and a final report (this document) summarizing threats, observations and recommendations was prepared. The objective of this report was to quickly identify strengths, gaps and opportunities for improvement to be considered in BC Hydro's strategic planning exercise in response to Directive 9. BC Hydro has indicated that, in response to Directive 9, it will conduct a detailed analysis of these recommendations, evaluate viable options to address them, and develop an implementation roadmap outlining an enterprise cybersecurity strategy with timing, costs and anticipated outcomes.

OBSERVATIONS AND RECOMMENDATIONS

Cybersecurity threats are constantly evolving in response to changing motivations and capabilities of threat actors (nation states, organized crime organizations, terrorist organizations, etc.) and due to the continual evolution of malicious tools and techniques used by these actors. As a result, cyber risks are not static and it is not always possible to fully mitigate cyber risk or reduce it to "low", even with significant investment. However, effective cyber programs focus on implementing capabilities and controls that can reduce both the likelihood of a cyber incident, and also to mitigate the impact of an incident should it occur.

This report contains observations and recommendations for improvement of BC Hydro's IT and OT cyber programs based on our assessment of relevant cyber threats, cyber security capabilities within BC Hydro's IT and OT environments, and on a review of recent internal and external assessments of BC Hydro's cyber security controls. The observations are intended to highlight the strengths of the existing program as well as gaps or opportunities for improvement to enhance the risk posture of BC Hydro relative to its ever-evolving cyber threat landscape. The recommendations described in this report are intended as an input into BC Hydro's more detailed enterprise cyber strategic plan being developed in response to Directive 9.

This report includes 40 recommendations integrated from prior reviews and audits together with recommendations arising from our interviews and document review as part of this assessment. As they were validated with BC Hydro, BC Hydro noted the status of their work related to these recommendations as "in flight" (projects already underway), "planned" (formally part of BC Hydro's cybersecurity roadmap) or "under consideration" (considered but not currently part of BC Hydro's 3-year cybersecurity workplan). BC Hydro noted that 50% of the recommendations are "in flight" or "planned", and the remaining 50% are "under consideration". The table below illustrates the breakdown of the recommendations by environment and by implementation status.

Table 1 - Count of recommendations by environment and implementation status

		BC Hydro indicated status		
Environment	# of recommendations	In-flight	Planned	Under consideration
Enterprise	10	1	4	5
Corporate IT	15	8	5	2
MRS OT	6	0	1	5
Non-MRS OT	9	0	1	8

Detailed findings and recommendations are contained within the body of this report. However, a summary of the key themes arising from the assessment is provided below.

Enterprise governance of cybersecurity – BC Hydro's cybersecurity initiatives are currently delivered by specialists working within its corporate IT and OT environments. BC Hydro has recently introduced changes to the cybersecurity team's organization and governance model that will enhance coordination and alignment of cyber activities between these environments. BC Hydro should continue to implement this new model to ensure an enterprise view of cyber risks, priorities and initiatives that spans the IT and OT environments. A formal enterprise cyber governance model will help to ensure a common and consistent approach to threat and risk assessment across the organization, coordination and alignment regarding cyber initiatives, effective and meaningful reporting and clear roles and responsibilities with respect to the delivery and oversight of the cyber program. Enhanced cyber governance across these environments also helps to address emerging cyber risks associated with increased interconnectedness of OT and IT environments.

Asset management – although asset management capabilities were identified for both the IT and OT environments, the importance of a combined view of assets (including data assets and data flows) and their related cyber risks is important to adequately understand and manage BC Hydro's cyber risk at an enterprise level. Deloitte recommends continuing to formalize asset management processes, giving consideration to adopting a single configuration management database and supporting monitoring process across BC Hydro.

Privileged access management – the management of privileged accounts, including rotation of shared accounts and PINs, was observed to be addressed in a number of ways across BC Hydro's OT and IT environments. The planned use of a formal privileged access management (PAM) solution within Corporate provides an opportunity to consolidate these approaches under one enterprise-grade solution that can reduce the risk of privileged account compromise or abuse across BC Hydro's environments.

Security event monitoring – security incident and event management (SIEM) capabilities within the Corporate environment are being expanded and improved within BC Hydro as part of a current in-flight initiatives. While security monitoring is in place within the OT environments, this is focused predominantly on compliance driven monitoring and audit use cases. BC Hydro should consider expanding the use of its Corporate SIEM solution to the OT environments where possible. In addition, expansion of this solution to include further network anomaly detection and the inclusion of specialized ICS monitoring solutions could further increase BC Hydro's threat identification.

Continued expansion of vulnerability management – BC Hydro has implemented patch and vulnerability management practices and processes across the IT and OT environments. In addition, there are planned improvements to processes to actively test the environment's security. However, there are opportunities for improvement, including the addition of red teaming processes, expanded threat hunting and more regular penetration testing.

CONCLUDING STATEMENT

Through this assessment and previous audits and reviews, a number of strengths related to BC Hydro's cyber program (across IT and OT environments) have been identified. Several recommendations for improvement have also been identified that could further strengthen the program and enhance cyber capabilities for its IT and OT environments. With respect to Directive 8, "immediate or time-sensitive concerns" was interpreted as representing critical, open vulnerabilities or weaknesses presenting a current or imminent risk to BC Hydro's operations. Within the scope and timeframe of this assessment, no such concerns were noted. As a next step, it is recommended that BC Hydro utilize this integrated list of recommendations to inform a more detailed enterprise cyber planning exercise (to support its response to Directive 9) and update/refine its cyber strategy to further improve its cyber risk posture.

GLOSSARY OF TERMS

Table 2 - Glossary of terms

Threat	Description
Active Directory (AD)	A Microsoft directory service that is used to manage computers and other devices on a network
Advanced Persistent Threat (APT)	A covert cyber-attack on a computer network where the attacker gains and maintains unauthorized access to the targeted network and remains undetected for a significant period
Business Email Compromise (BEC)	Cyberattack that is designed to gain access to critical systems through email-based fraud or impersonation of a business email address
CA IDM	BC Hydro Identity Governance and Administration (IGA) solution
Canadian Centre for Cyber Security (CCCS)	A Canadian government program that is responsible for monitoring threats and coordinating the national response to any cyber security incident
Centre for Internet Security (CIS)	A community-driven non-profit organization, responsible for the CIS Controls® and CIS Benchmarks™ which are globally recognized best practices for securing IT systems and data
Command & Control (C2) Server	A computer that is used by attackers to maintain communications with compromised systems within a target network
Cyber Security Incident Response Plan (CSIRP)	A systematic and documented plan for approaching and managing situations resulting from security incidents or breaches
Cybersecurity & Infrastructure Security Agency (CISA)	A Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future
Distributed Denial of Service (DDoS)	A cyber-attack performed in an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources
Data Loss Prevention (DLP)	A cybersecurity solution that is used to detect and prevent data leaks
De-Militarized Zone (DMZ)	A network area (a subnetwork) that is between an internal network and an external network which contains and exposes an organization's external-facing services to an untrusted, usually larger, network such as the Internet
Electricity Information Sharing and Analysis Centre (E-ISAC)	A trusted leader and source of security information within the electricity industry in collaboration with the Department of Energy, the Department of Homeland Security, and the Electricity Subsector Coordinating Council
Endpoint Detection and Response (EDR)	A category of tools used to detect and investigate threats on endpoint systems
Industrial Control System (ICS)	An information system used to control industrial processes such as manufacturing, product handling, production, and distribution through integration of hardware and software with network connectivity
Information Technology (IT)	An application of technology to solve business or organizational problems on a broad scale
Intellectual Property (IP)	A category of property that includes intangible creations of the human intellect
Internet of Things (IoT)	A network of physical objects or "things" that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet
Industrial Internet of Things (IIoT)	Interconnected sensors, instruments, and other devices networked together with computers' industrial applications, including manufacturing and energy management
Internet Protocol Address Management (IPAM)	A methodology implemented in computer software for planning and managing the assignment and use of IP addresses and closely related resources of a computer network
Local Area Network (LAN)	A network contained in one physical location, such as a building, office, or home
Managed Defense and Response (MDR)	Advanced managed security services that is designed to rapidly identify and limit the impact of security incidents
NetFlow	A protocol for collecting, aggregating and recording traffic flow data in a network

Threat	Description
Network Access Control (NAC)	The process of restricting unauthorized users and devices from gaining access to a corporate or private network through policy enforcement on devices and users of corporate networks
Operational Technology (OT)	The use of hardware and software to detect or cause a change, through the direct monitoring and/or control of industrial equipment, assets, processes, and events
Red Teaming	The practice of testing the security of systems by adapting an adversarial perspective
Privileged Access Management (PAM)	Access management strategies and technologies that are focused exclusively on privileged account access control and management
Security Information and Event Monitoring (SIEM)	A security tool that analyzes the data collected across endpoint, network and cloud assets against security rules and advanced analytics to identify potential security issues within an enterprise
Software Development Life Cycle (SDLC)	A process for designing, developing, and testing high quality software
Supervisory Control and Data Acquisition (SCADA)	A control system that is designed to collect, analyze, and visualize data from industrial equipment
Tactics, Techniques, and Procedures (TTPs)	Patterns of activities or methods associated with a specific threat actor or group of threat actors
Transport Layer Security (TLS)	A cryptographic protocol designed to provide communications security over a computer network
User and Entity Behavior Analytics (UEBA)	A cybersecurity process that uses machine learning and deep learning to model the behavior of users on corporate networks and highlights anonymous behavior that could be the sign of a cyberattack
Virtual Desktop Infrastructure (VDI)	A virtualization technology where a desktop operating system is run and managed in an on-premise or cloud data center
Virtual Private Network (VPN)	A service that creates a safe, encrypted online connection that ensures secure data transmission across shared or public network
Web Application Firewall (WAF)	An application firewall that filters, monitors, and blocks HTTP traffic to and from a web service
Wide Area Network (WAN)	A computer network that covers a broad area (e.g., internet, any network whose communications links cross metropolitan, regional, or national boundaries over a long distance)

INTRODUCTION

BACKGROUND

BC Hydro's FY22 and FY23-25 Revenue Requirements Applications (RRA) outline significant increases in investments and expenditures related to cyber security both for its corporate systems and systems related to the Bulk Electric System (BES) covered by the Mandatory Reliability Standards (MRS). These investments and expenditures include increased funding and resources for BC Hydro's corporate cyber security program and are intended to address remediation and enhancement projects as well as additional headcount to deliver and sustain these programs[1].

This additional investment in cyber security is driven by a rapidly evolving global threat landscape related to critical infrastructure (including recent cyber security incidents in relevant industries), changes in the NERC Critical Infrastructure Protection (CIP) standards, earlier penalties associated with non-compliance to NERC CIP requirements, direction from the British Columbia Utilities Commission (BCUC) in its last RRA decision (FY20-FY21), and results from recent internal and external audits and assessments (including an audit by the BC Office of the Auditor General).

In its decision regarding the FY22 RRA (Decision and Order G-187-21[2]), the BCUC approved the proposed increases in budget for BC Hydro's MRS and non-MRS cyber security programs. However, the BCUC also noted concerns related to the state of BC Hydro's overall cyber security posture. Specifically, the BCUC noted that: "while portions of BC Hydro's operations that are part of the North American BES are protected by MRS, the Panel remains concerned that other areas such as distribution, back-office systems, and other assets that are not protected by MRS provide potential cyber security vulnerabilities". Given recent attacks highlighting the potential vulnerability of critical infrastructure to attacks targeting corporate assets, the BCUC noted that "the Panel considers that BC Hydro should afford the same or similar level of protection across all of BC Hydro's cyber assets" to the protection offered under the MRS requirements.

In its RRA decision, BCUC directed BC Hydro to undertake "a cyber risk assessment of all of its cyber assets" and to notify the BCUC of any action that has been taken or needs to be taken on any immediate or time sensitive concerns. This directive was issued on June 17, 2021. The assessment was to be completed, with a report submitted to BCUC, within three months of the decision date (by September 17, 2021). In the same decision, the BCUC directed BC Hydro to "develop a company-wide, comprehensive Cyber Security Plan that encompasses BC Hydro and its subsidiaries and third parties with whom it interfaces" within one year of the decision (i.e., by June 16, 2022). The decision further notes that the cybersecurity plan should be informed by this cyber risk assessment.

OBJECTIVES

In response to the BCUC's directive, BC Hydro engaged Deloitte to support a risk assessment of its cyber program, covering its corporate information technology (IT) and operational technology (OT) environments. The goal was to integrate results of previous assessments of specific elements of BC Hydro's technology environment and assess the organization's overall enterprise cybersecurity program in light of a rapidly evolving cyber threat landscape. Specifically, the objectives of this cyber risk assessment were to:

- Review BC Hydro's threat landscape and develop an updated list of threats relevant to North American power and utilities entities
- Conduct an enterprise-level cyber assessment to identify capabilities in place to address identified threats. This assessment was aligned to the NIST Cybersecurity Framework (CSF), with reference to NERC CIP standards where appropriate
- Building on findings from interviews and document review, as well as recent audits and reviews of BC Hydro's cybersecurity program, provide an integrated assessment of BC Hydro's security risk posture and program relative to threats
- Provide recommendations to address any identified gaps

SCOPE

In scope

Previous cyber assessments and audits have focused on individual components of BC Hydro's cybersecurity program to address questions regarding cyber risks and strengths or gaps related to existing cyber controls. Each assessment has resulted in a series of findings and recommendations, many of which are currently being addressed by BC Hydro. However, to address the directive issued by the BCUC for a "cyber risk assessment of all of its cyber assets", this review was designed to provide an integrated view of BC Hydro's cyber program and risk posture across both Corporate and operational (OT) environments. This scope reflects the fact that threats and risks related to critical infrastructure (including power infrastructure) are rapidly evolving, that there is increasing integration of IT and OT environments and that an attack on any element of BC Hydro's technology environment could have significant implications for residential and commercial power customers in BC and for the Bulk Electric System more broadly.

This assessment therefore focuses on three categories of IT assets within BC Hydro's technology environment (see Table 3): the Corporate IT environment (addressed through BC Hydro's corporate cybersecurity program), the OT environment that is subject to the NERC mandatory reliability standards (addressed by BC Hydro's MRS compliance program) and the OT environment associated with power infrastructure that is currently not subject to the NERC standards. Given the broad scope and short timeframe of this assessment, it was not possible to assess controls or capabilities in place at individual facilities or for individual systems. Rather, the report focuses on the capabilities in place as part of BC Hydro's cybersecurity program for these three categories of assets, and also addresses the extent to which these three elements of the program are aligned to address key enterprise cyber threats and risks. This assessment reviewed the design of BC Hydro's cybersecurity program and did not include an audit of the program's operating effectiveness (i.e., where controls are tested based on statistically-representative samples).

[1] hxxps://www.bcuc.com/Documents/Proceedings/2020/DOC_60299_B-2-BCH-F22-RRA-Application.pdf
hxxps://www.bcuc.com/Documents/Proceedings/2021/DOC_64005_B-2-BCH-F23-F25-RRA-public.pdf

[2] hxxps://www.bcuc.com/Documents/Other/2021/DOC_63154_G-187-21-BCH-F2022-RRA-Final-Order-Decision-Public_Redacted.pdf

Table 3 - Description of IT and OT scope categories included in this assessment

Scope	Scope Description	Illustrative assets/locations
Corporate Information Technology	• Information technology assets, systems, and applications which are connected to corporate networks and/or managed by BC Hydro's information technology department • Also includes BC Hydro's Corporate offices and related facilities • Includes systems which are corporate-network connected, but support the OT environment (e.g. CCTV feeds to monitor physical site access points) and includes systems which are used to support MRS compliance processes (e.g. SigmaFlow, business applications which support Generation and Supply Operations)	• Corporate finance, HR, productivity and related systems • Dunsmuir Offices • Victoria District Office

MRS Operational Technology	• Bulk Electric System Cyber Systems which are categorized as high, medium or low impact (according to the impact rating criteria contained within CIP-002-5.1a)
	• These assets are subject to NERC mandatory reliability standards (specifically to the Critical Infrastructure Protection standards) and cybersecurity is managed under BC Hydro's MRS program. This includes:
	  o BES Cyber Systems (BCS) and BES Cyber Assets (BCAs); Protected Cyber Assets (PCAs); Electronic Access Control and Monitoring Systems (EACMS); and Physical Access Control Systems (PACS).
	  o Transient Cyber Assets (TCA) and Removable Media (RM) that connect to BCAs or PCAs or a network within an Electronic Security Perimeter (ESP) at 'High Impact' and 'Medium Impact' BES Facilities.
	• 53 facilities are rated as High or Medium impact and 133 are rated as Low impact
		• Ruby Creek capacitor station
		• Mica generating station
		• Cathedral Square substation

Non-MRS Operational Technology	• Approximately 150 BES cyber facilities that are not covered under BC Hydro's MRS program • While non-MRS OT networks may represent a lower risk to the Bulk Electric System overall, a failure associated with non-MRS OT could impact local electric system operations resulting in operational and reputational impacts to BC Hydro and inconveniences to its customers • Field smart metering infrastructure was not specifically assessed given the relatively compressed timeframe for this review.	• Sea Island substation

Not in scope

In its Decision and Order, the BCUC also directed that BC Hydro "develop a company-wide, comprehensive Cyber Security Plan that encompasses BC Hydro and its subsidiaries and third parties with whom its interfaces" within one year of the decision (i.e., by June 17, 2022). The decision further notes that this cybersecurity plan should be informed by this cyber risk assessment. With this in mind, the following are excluded from the scope of this assessment:

- BC Hydro subsidiaries
- BC Hydro's third-party service providers

APPROACH

This project was delivered over seven weeks to align with the submission date outlined in the BCUC's Decision and Order. The scope and assessment activities were aligned to the BCUC request to undertake a "cyber risk assessment of all of its cyber assets" and included the following activities:

- Understanding the BC Hydro attack surface and threat landscape
- Gathering and reviewing documentation related to BC Hydro's control environment, including prior assessments (see appendix A for list of documents reviewed)
- Assessment of the global threat landscape with a focus on the Energy and Resources sector
- Confirmed relevant threats and risks to BC Hydro
- Conducted working sessions with BC Hydro stakeholders to identify cyber capabilities related to the threats and risks (see appendix B for list of working sessions conducted and stakeholders involved)
- Assessed cyber program covering BC Hydro's core environments (IT, MRS OT and non-MRS OT) against threat and risk scenarios using NIST's cybersecurity framework
- Validated observations and recommendations for each of the threat scenarios

This report provides prioritized recommendations to address gaps identified during the assessment, taking into consideration the relative risk, timelines to implement and the degree of risk mitigation they will deliver. The recommendations from this report will be an input into BC Hydro's follow up cyber security planning, per Directive 9.

BC HYDRO CYBER THREAT LANDSCAPE

DRIVERS OF CYBER RISK

The power and utilities sector faces ongoing and persistent cyber threats, driven by a number of key characteristics which increase the overall inherent risk of attack, and the attractiveness of the sector to a range of threat actors. These drivers are highlighted below.

Level of interconnection and interdependence

The functioning and the resilience of the North American electric system is enabled by its highly interconnected nature. This supports dynamic management of demand and energy supply, a functioning electricity market and pricing and improves the resilience of the overall system to natural and human-caused disruptions. However, this level of interconnection and interdependence can also increase the risk of the system to targeted and coordinated cyber attacks. Cyber weaknesses within the ecosystem of generation, transmission and distribution providers (and their key suppliers) can result in increased risk to the bulk electric system overall if not properly managed, particularly when combined with rapid grid modernization efforts being implemented across the electricity value chain. The inherent risks to the sector has been well documented by regulators, intelligence agencies and cybersecurity service providers over the past 10+ years[3,4,5,6,7,8,9] and these risks have driven the significant focus of energy sector regulators on cyber resilience through the mandatory reliability standards (and in particular, the Critical Infrastructure Protection standards).

The threat of collateral damage

The level of reliance on third parties, and the interconnectedness into a broader network of IT services place modern organizations such as BC Hydro at risk of collateral damage. The 2017 NotPetya virus was one such example – the attack was directed at accounting software from Ukraine, potentially attempting to disrupt Ukraine's supply network, but quickly spread and caused collateral damage to a multitude of organizations around the world.

Extensive physical footprint

The highly distributed nature of typical electric power systems (from distributed generation systems to the transmission and distribution infrastructure required to move and deliver power to consumers and the network infrastructure to support operations) creates an inherently large and complex attack surface. Managing physical and cyber security effectively across such a distributed and complex environment can be logistically and administratively challenging, requiring effective coordination and prioritization of security operations and monitoring, as well as risk management involving multiple business units and suppliers. Additionally, the field teams and equipment operators are not traditionally trained to identify and contain a cyber incident. Their roles have been operating physical systems which have high availability and reliability requirements, and not scanning removable media for malware or identifying anomalous network behavior. This convergence of physical and cyber security with operational interfaces can be a technical and cultural challenge for OT organizations.

As complex ecosystems in electricity supply become more integrated and sophisticated, comprising computation, networking, and physical operational processes, having the capability to provide a coordinated, proactive, and effective response to cyber threats across an entire business becomes increasingly essential.

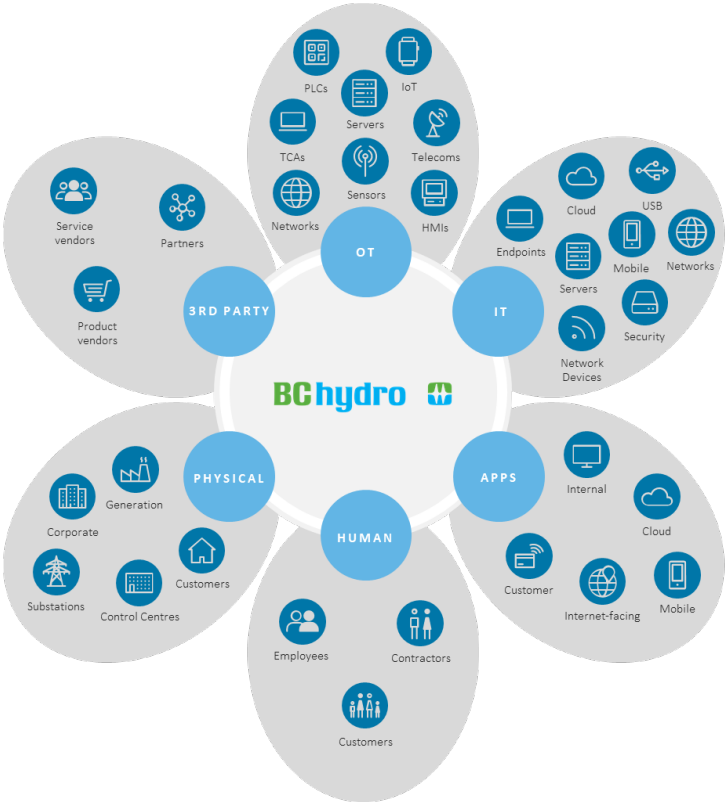

Figure 1 – BC Hydro's Attack Surface

[3] US Government Accountability Office, 2012. Cybersecurity: Challenges in securing the electricity grid
[4] Idaho National Laboratory Mission Support Centre, 2016. Cyber threat and vulnerability analysis of the US electric sector.
[5] Deloitte, 2018. Managing cyber risk in the electric power sector – emerging threats to supply chain and industrial control systems.
[6] World Economic Forum Centre for Cybersecurity and Electricity Industry Community, 2019. Cyber resilience in the electricity ecosystem: principles and guidance for boards.
[7] US Government Accountability Office, 2019. Critical Infrastructure Protection – Actions needed to address significant cybersecurity risks facing the electric grid.
[8] US Department of Homeland Security, 2020. Homeland threat assessment.
[9] Canadian Centre for Cybersecurity, 2020. Cyber threat bulletin: the cyber threat to Canada's electricity sector.

Extensive use of legacy technology

Legacy OT and IT within the generation, transmission and distribution facilities of most electric systems is common, introducing increased risk of un-remediated vulnerabilities within these environments. Risks arise from the fact that these technologies were often not originally designed with security controls in mind, and because of their distributed nature, may not be as easily inventoried and managed. Further, because distributed operational technologies are often not connected via internet protocol or telecommunications networks, it is difficult to remotely monitor these environments for vulnerabilities and/or malicious activity (although this lack of connection can also reduce their exposure to cyber threats).

Grid modernization and digitalization

Grid modernization and digitization is leading in some instances to increasing network connectedness of elements across the power grid (from generation through to consumers), increasing convergence of IT and OT environments and the proliferation of Internet of Things (IoT) devices connected to the electric system. While these developments increase the functionality and resilience of the grid in many ways, they also significantly increase the scale and complexity of the attack surface, requiring constant updates to threat models and relevant controls to mitigate evolving cyber risks.

Increasingly capable threat actors

As noted above, organizations in the electric utility sector are often targeted by a range of threat actors as they represent high-value targets for Intellectual Property (IP) theft, extortion and for broader intelligence, geopolitical and military purposes. Externally, organized crime, nation states and terrorist organizations represent the most significant threat to the bulk electric system. However, insiders and third-party suppliers that are technically and/or operationally integrated into an organization's IT and/or OT infrastructure also represent a significant risk as observed through several recent compromises.

Additionally, threat actors have an ever-growing financial motivation to conduct extortion type campaigns. In 2020, the average ransom payment was over $300,000 USD, growth of over 171% year on year[10]. With average ransom payments growing at such a rapid pace, threat actors are looking for any foothold into a network to attempt to exfiltrate data, deploy ransomware, and demand payment.

IT / OT DICHOTOMY

The drivers identified above highlight that connected digital technologies have both enabled efficiencies across the energy sector and added a new dimension of risk. Increased levels of connectivity and dependence, the proliferation of internet of things (IoT) devices and the digitization of customer support and experience platforms are expanding the cyber-attack surface for threat actors. Simultaneously, the technology which enables these operational efficiency drivers is not equally designed. While OT technology has evolved in the past decade in terms of improving cyber security posture, the inherent technology profile is different to that of its IT counterpart. These technologies are critically related and interconnected, but are defined differently with respect to cyber risks, challenges, and priorities, as reflected below:

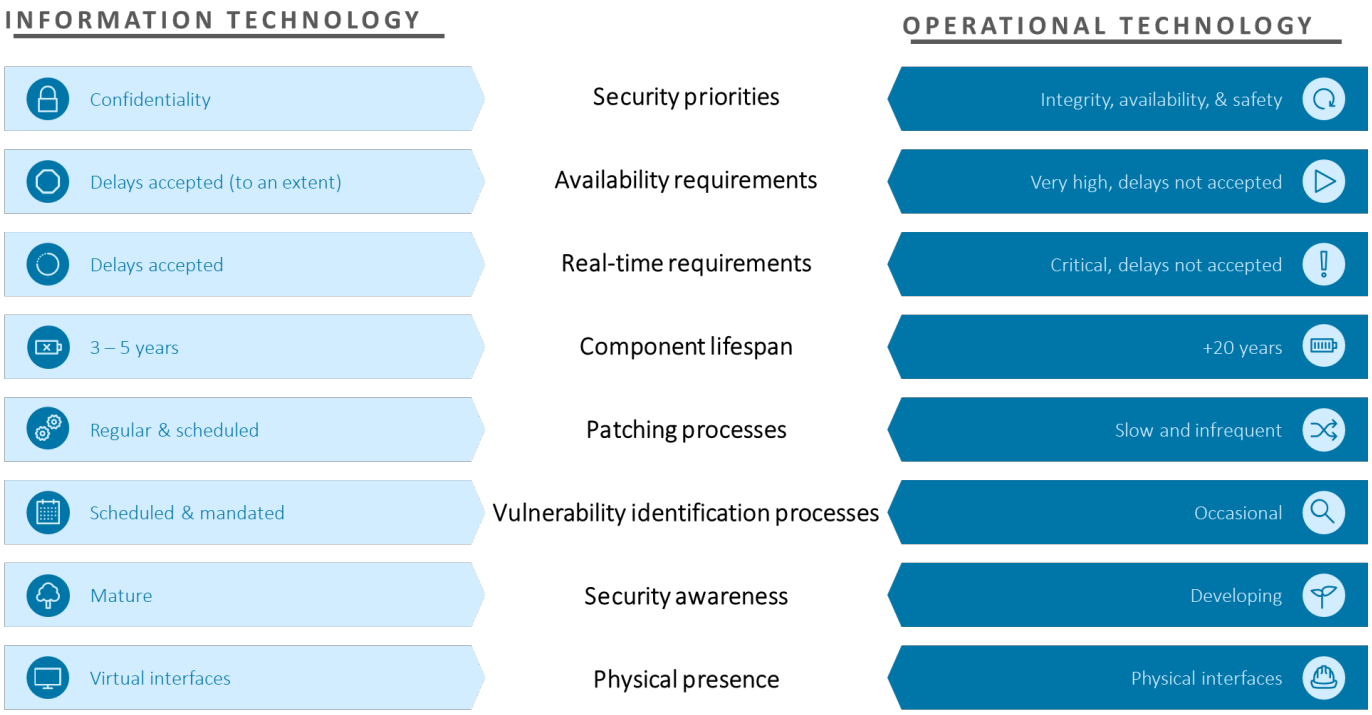

Figure 2 – IT / OT Dichotomy

[10] Unit 42, 2021. Ransomware Threat Report.

BC HYDRO: GENERATION, TRANSMISSION, AND DISTRIBUTION

BC Hydro serves 2.1 million customer accounts throughout the province. It generates over 49,000 gigawatt hour of electricity annually, using predominantly hydro-electric dams, before transporting it across the province (and through interconnections, to western North America through the Bulk Electrical System (BES)), and finally distributing it to customers (including residential, industrial, and commercial customers). The BES Western Interconnection is a network of high-voltage transmission lines that connects British Columbia with other utilities in western North America, including those in Alberta, Washington State, Oregon and California. Facilities, infrastructure, and supporting systems which facilitate the transmission of electricity along the BES are covered under a regulatory framework called Mandatory Reliability Standards (MRS).

Generation, transmission, and distribution are described in further detail on the following page, and a simplified view of the process, along with a summary of relevant BC Hydro assets, is provided below:

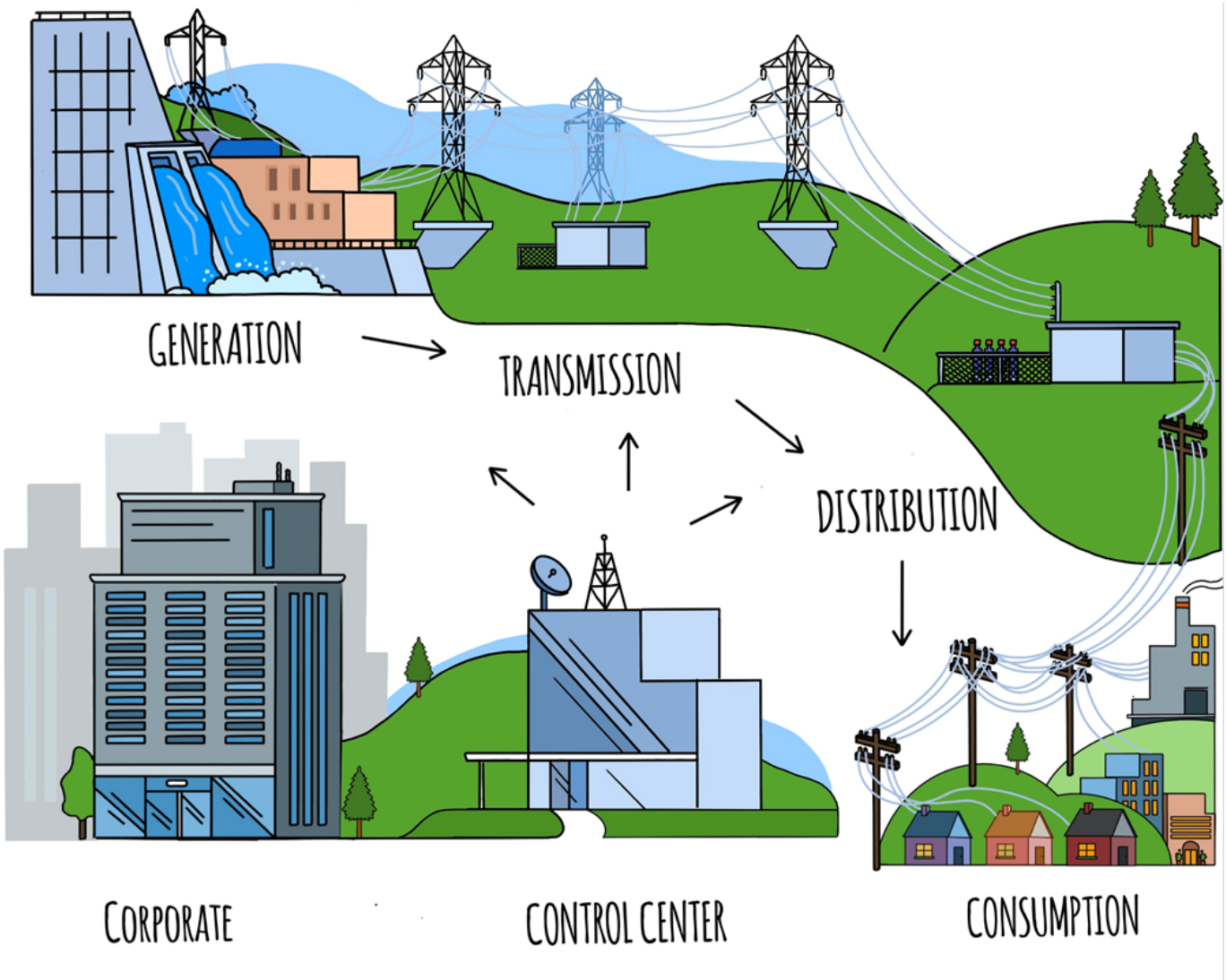

Figure 3 - Simplified illustration of the generation, transmission and distribution of electricity by BC Hydro

PHYSICAL AND CYBER ASSETS RELATED TO GENERATION, TRANSMISSION, DISTRIBUTION

31 generating stations	300+ substations	55,000+ KMs of distribution lines	18,000+ KMs of transmission lines
4 major datacenters	8500+ workstations	2600+ servers	400+ applications
50+ corporate office locations	186 MRS sites	6000+ employees	2.1+ million customer accounts

Generation

In BC, more than 90% of generation is hydroelectric generation, using moving water to spin turbines. Electricity generation relies on local control equipment to manage output, and wide area networks to manage load and frequency to the electrical system. Generation station sensors continuously feed data to control rooms, which use that data to tune output and send commands to generator equipment.

The cyber-attack surface for generation is considered to be more focused on gaining access to the local control system, which can be achieved through local physical access, remote access, the introduction of malware, or pivoting through a trusted communication path in the organization's networks. Additionally, the attack surface is further expanded through the risk of an attack on wide area control systems, which depend on ICS/SCADA, that could have serious impacts on power stability emanating from a generation facility.

Transmission

Once electricity is generated it is stepped-up in voltage and transported. Transmission systems have substation transformers, transmission towers, and control centers to manage the delivery of power from generation resources to the distributed system loads. Similar to generation, cyber threats to utilities responsible for transmission depend on several variables, such as network configuration within a substation and means of communicating data, and substation and transmission tower physical security.

Controllers and other devices found in control rooms are often sources of vulnerabilities which could serve as entry points to networks. Without protective controls in place, a threat actor who is able to breach substation networks could disrupt, desynchronize, or impact data communications necessary for protection and control, causing load instability. Substation networks without detection capabilities to identify intrusions and malicious data injection could allow an attacker to manipulate multiple substations over time without discovery. Additionally, physical access to a substation could result in significant damage via malware introduction to computers and devices, manipulation of protective relays, and destruction of physical equipment.

Distribution

Distribution and local delivery of electricity is not generally considered part of the BES, meaning cyber security control implementation can vary in terms of coverage and effectiveness. However, cyber security threats to distribution infrastructure could lead to outages that would cause impacts to BC energy consumers. Such impacts to certain distribution substations (highly visible substations, or substations serving critical or vulnerable customers) would cause significant reputational impacts to BC Hydro. While distribution attack surfaces may be smaller and potential impacts may be lower, cyber security controls are subject to lower oversight, and therefore may present a certain amount of risk.

Corporate

Corporate infrastructure supports BC Hydro's business operations, but also enables services which very closely interface with OT infrastructure and processes. Examples include telemetry and analytics reports for water levels, weather, or environmental factors which are critical inputs to OT operations. This data must transit along complex networks amongst thousands of connected devices and systems.

On the other side of energy production is the millions of consumers and customers of BC Hydro. These customers integrate with BC Hydro systems every day through self-service portals which contain personal information and banking information to facilitate customers receiving electricity in the right place at the right time. Additionally, loss of data and/or inability to communicate both internally or externally to suppliers or customers for billing purposes would inhibit BC Hydro's ability to conduct business. Associated recovery and restoration efforts would be resource intensive and costly. Further, the continual evolution of the grid through the introduction of new customer-facing services (e.g., smart meters, electric vehicle charging stations, etc.) means that the attack surface is also evolving, requiring a dynamic cyber program to identify and respond to new risks as they arise.

All of the systems, devices, processes, and employees that make this happen now work largely remotely. Remote connected workforces add additional and emerging attack surfaces which are constantly being subjected to exploit attempts (such as Virtual Private Network (VPN) gateway exploits).

TOP THREAT SCENARIOS BASED ON GLOBAL THREAT INTELLIGENCE

According to the Canadian Centre for Cyber Security (CCCS)[11], the majority of cyber threats against the Canadian electricity sector have largely consisted of fraud and ransomware, as well as espionage and intellectual property theft. While there are several notable recorded cyber incidents against North American – and global – Power and Utilities organizations, the CCCS notes that it is unlikely that state-sponsored threat actors will intentionally seek to disrupt the Canadian electricity sector in isolation. However, it does also note the increasing likelihood that the Canadian electricity sector could be adversely impacted by an attack on US infrastructure due to the high level of connectivity between the US and Canadian electricity grids, and/or as a result of the business process dependencies between traditional IT systems, and industrial control systems. Other cyber threats that affect the Canadian electricity sector include supply chain / third party attacks, and attacks on vulnerable industrial control systems components.

The following set of six threat scenarios were assessed for BC Hydro, in order to evaluate the cyber capabilities in place and to understand the current residual risk posture. The threats have been informed and chosen by using industry risk assessment reports authored by the Canadian Centre for Cyber Security (CCCS), the Cybersecurity and Infrastructure Security Agency (CISA), Deloitte's Threat Intelligence team, and other top energy sector and utilities cyber risk assessment reports. While some threats may have a number of potential vectors and impacts, this report has focused on specific scenarios that provide the broadest coverage of cyber capabilities and that best align to the above-mentioned industry insights. This threat information has been related to BC Hydro's environment through consultation with BC Hydro's cyber security leadership team.

Table 4 - Summary of cyber threat scenarios and rationale for inclusion in this assessment

Threat Scenario	Why were these threat scenarios selected for this assessment?
 **T.01** **Major Ransomware Outbreak** *Ransomware is installed onto key BC Hydro systems, blocking access to data and key systems. Attackers threaten to publish the data unless a ransom is paid.*	**Description:** Ransomware is a type of cryptovirology malware that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid and has become one of the most visible and devastating cyber threats impacting organizations today. Ransomware refers to the category of attacks in which threat actors deploy data-encrypting malware to an organization's network, rendering systems and data unusable until a ransom amount is paid. Ransomware operators have also shifted tactics to not only encrypt data and render systems unusable, but also to steal data and threaten to leak it to the public if the ransom is not paid; a tactic known as double extortion (with increasingly complex triple extortion models also now being utilized by some threat actors). Ransomware has been seen actively targeting and successfully extorting critical industries such as energy and resources, health care, and the public sector, most recently the Colonial Pipeline ransomware attack. More broadly, at the time of writing, there were 70+ E&R organizations, hundreds of Canadian organizations, and over 1500 American organizations with exfiltrated data listed on public ransomware breach pages. **Potential Impacts:** *Disclosure and theft of information assets; loss of data; disruption of services.*
 **T.02** **Espionage by Advanced Persistent Threat (APT)** *APT threat actors infiltrate an organization's network to obtain sensitive or proprietary information and/or to position malware for future disruptive actions.*	**Description:** The E&R sector is a high-value target for states with Advanced Persistent Threat (APTs) capabilities. APT groups attempt to steal information, centering on information related to natural resource exploration and energy deals. APT groups may also engage in destructive and disruptive actions against an adversary's energy industry. These capabilities were first observed in the now infamous Stuxnet attack against the Natanz uranium enrichment plant in Iran in 2010. Since then, other states have worked to develop similar capabilities to target western states. Deloitte Threat Intelligence (Deloitte TI) has identified several APT's known to specifically target the E&R sector, based on the current geopolitical climate. In particular, four of these are known to focus on the sector directly: *Sandworm Team (Russian APT)* - active since at least 2009, most notable attacks include 2015/16 targeting of Ukrainian electrical companies and 2017's NotPetya attacks; *RedEcho (Chinese APT)* - active since at least 2020, most notable attacks include 2020 attacks on 10 Indian power sector organizations and 2 seaports; *Dragonfly 2.0 (Russian APT)* - active since at least 2015, noted as targeting the power, energy, and water distribution IT networks to steal information and conduct reconnaissance on operational networks; and *Threat Group 3390 (Chinese APT)* - active since at least 2010; noted as targeting organizations in aerospace, government, defense, technology, energy, and manufacturing sectors). **Potential Impacts:** *Disclosure and theft of critical information assets; disruption of services.*

[11] Canadian Centre for Cybersecurity, 2020. Cyber threat bulletin: the cyber threat to Canada's electricity sector.

Threat Scenario	Why were these threat scenarios selected for this assessment?
 **T.03** **Supply Chain Attack Introduces Compromised Software** *Malicious software is introduced into the network by an upstream supply-chain attack.*	**Description:** Managing risk across the extended supply chain is often challenging. There may be many different third parties that must be considered whether it's a supplier that provides a specific software product, or embeds software into a larger system, these connected components increase the risk and attack surface that expose organizations such as BC Hydro to cyber threats. Threat actors may not directly target one organization, and instead use vulnerabilities in supply-chain networks to access many victims and paralyze multiple networks simultaneously. The 2020 SolarWinds attack is one of the most prolific cyber-attacks in recent history due to its magnitude and sophisticated nature. Attackers were able to evade mature cyber defenses, remaining undetected for months. Similarly, in July 2021 attackers used a zero-day exploit in Kaseya's Virtual System/Server Administration (VSA) software to plant malicious code which would then be distributed to VSA customers[12]. As impacts from these events continue to unfold, leaders should consider programmatic changes to prepare for a future in which similar attacks are increasingly common. **Potential Impacts:** *Alteration of critical system components resulting in disclosure and theft of information assets or disruption of services.*
 **T.04** **Insider Facilitates Data Leakage** *An insider with access to BCH's environment provides access to BCH's network a criminal organization.*	**Description:** The risk of insider threats has increased as encrypted and anonymous messaging services, and dark web and underground communities become more accessible (including to employees with privileged access to sensitive information or systems). Insider threats could originate from disgruntled employees, individuals in difficult financial positions or seeking financial gain, individuals that have fallen victim to extortion, or an actual "plant" implemented by a nation-state actor or criminal organization. Threat actors have been observed offering large sums of money to employees willing to help them breach and encrypt networks. Most recently, In June 2021, LockBit ransomware announced the launch of its new LockBit 2.0 ransomware-as-a-service (RaaS) operation. Among new features such as faster, automated encryption, the new model included a Windows wallpaper placed on encrypted devices to offer "millions of dollars" to corporate insiders who provide access to networks where they have an account. On August 11, 2021, Deloitte TI observed a multinational consulting firm on LockBit 2.0's ransomware site. **Potential Impacts:** *Disclosure and theft of information assets; disruption of services; Unauthorized disclosure and theft of confidential client data*
 **T.05** **Business Email Compromise** A cyber-criminal perpetrates financial fraud by compromising BC Hydro email accounts.	**Description:** Social engineering continues to be the top attack pattern leading to cyber security breaches today[13]. Unsurprisingly, phishing and business email compromise (BEC) account for the majority of social engineering attacks. According to the FBI's 2020 Internet Crime Report, the FBI received over 19,000 business email compromise complaints in 2020, with adjusted losses of over $1.8 billion. In Canada, between 2016 and 2019 there was an estimated $45 USD million lost[14] to business email compromise. In 2019, two government organizations in Canada were affected by business email compromise scams, one resulting in a loss of over $1m and the other in a loss of over $500,000. In 2020, the RCMP reported that they were investigating a BEC attack on the Government of the Northwest Territories; the undisclosed amount was reportedly recovered. The Canadian Centre for Cyber Security (CCCS) assesses that cyber threat actors will continue to use business email compromise to defraud organizations in Canada and around the world. Further, Deloitte has observed an increase in BEC scams targeting Canadian organizations. **Potential Impacts:** *Financial fraud; unauthorized access to systems; disclosure and theft of confidential company and client data*
 **T.06** **External Network Service Compromise** *A threat actor compromises an external / internet-accessible service providing access to internal systems.*	**Description:** Attacks on exposed servers were the third most common attack type in 2020, with attackers exploiting stolen credentials and known vulnerabilities to gain access (IBM). The most commonly exploited vulnerabilities in the last year were in products such as Citrix NetScaler, Pulse Secure Connect VPN, Fortinet VPN, Apache, Microsoft Windows Server, and Microsoft Exchange. The COVID-19 pandemic and "work from home" shift has driven organizational assets away from controlled spaces and into homes and public locations, increasing the reliance on remote working technologies like VPN, cloud, and remote desktop and significantly increasing the attack surface of most organizations. Additionally, OT/ICS/SCADA systems are increasingly being connected and accessed remotely. The increasing use of industrial internet of things (IoT) devices and cloud services in industrial systems has also increased the attack surface. Threat actors are conducting continuous scanning activity to locate and exploit poorly configured, networked devices, which could lead to unauthorized access to control systems and the broader technology environment. Most recently in the E&R sector threat actors have gained access to E&R organization networks after conducting vulnerability scans and conducting SQL injection attacks against the organization's websites. In a recent incident, once inside the network the threat actors compromised at least 50 systems and stole over four gigabytes of data from a business unit responsible for the exploration and later production of fossil fuels. **Potential Impacts**: *Unauthorized access to systems; disclosure and theft of confidential company and client data; disruption of services*

[12] European Union Agency for Cybersecurity, 2021. ENISA Threat Landscape for Supply Chain Attacks.

[13] Verizon, 2021. 2021 Data Breach Investigations Report.

[14] Better Business Bureau, 2019. The Explosion of Business Email Compromise (BEC) Scams

THREAT SCENARIOS ASSESSMENT

INTRODUCTION

This assessment was focused around the six threat scenarios described above in order to assess BC Hydro's cyber capabilities relative to high-priority threats and cyber risks. Each threat scenario could have multiple impacts and/or outcomes, but this assessment has specifically designed impacts and outcomes in such a way to ensure they are unique and to avoid repetitive analysis across multiple threat scenarios. In the following section, each of the threat scenarios is described in the context of BC Hydro's operating environments. BC Hydro's cyber program was assessed against these threat scenarios evaluating a variety of cyber security capabilities (based on the NIST CSF). This assessment was based on the results of previous cyber audits and reviews and on further consultation with BC Hydro stakeholders and review of documentation related to BC Hydro's enterprise cybersecurity capabilities.

THREAT SCENARIO ASSESSMENT STRUCTURE

In the following section, each of the six threat scenarios, and BC Hydro's related cyber capabilities and opportunities for improvement, are described in greater detail. Table 5 below outlines the information provided for each threat scenario.

Table 5 - Overview of threat scenario and assessment details

Section	Description
Risk Rating Summary Table	Provides a tabular summary of inherent and residual risk rating values per environment (see inherent risk values and current residual risk values definitions in the table below). Residual risk values take into consideration the assessment of expected capabilities related to each threat scenario. They represent an adjusted relative risk rating based on the extent to which the capabilities reduce the inherent risk. This rating is based on the assumption that the capabilities identified within the reviewed material and interviews are implemented as designed and are operating effectively, as no assessment of effectiveness was performed as part of this assessment.
Summary Observation	Provides a summary of the risk, as justified by a short description of the threat scenario, controls assessed as in place or planned, and areas for improvement or additional consideration.
General Description	Provides a summary view of the characteristics of a given threat scenario, and possible impacts to the organization
Key Vectors	Provides a listing of possible methods a threat actor could leverage to initiate a given threat scenario. Cyber-attack vectors may be more common among certain threat actors or threat actor groups.
Expected Capabilities	Provides a view on which NIST Cybersecurity Framework (CSF) category capabilities would reduce inherent risk associated with a given threat scenario should they be delivered at a mature level (Capability Maturity Model Integration (CMMI) Level 3 – Defined, or greater). Quantitative assessment of expected capabilities was out of scope of this assessment.
Capability Assessment	Provides a listing of identified capabilities, observations for immediate action, observations to improve BC Hydro's control environment, and observations for further consideration for a given threat for each of the three in-scope environments (i.e. corporate IT, MRS OT, and non-MRS OT). Identified capabilities are based on a point in time review of available documentation and management's assertion of implemented controls.
Recommendations	Provides a summary view of actionable recommendations which apply to protecting BC Hydro's environment from a given threat. Further details regarding recommendations can be found in the Recommendations section.

For each of the threat scenarios, **relative risk ratings** have been assigned for each of the in-scope environments (Corporate IT, MRS OT, and Non-MRS OT). Risk rating values (HIGH, MODERATE, LOW) are meant to align to BC Hydro's existing Enterprise Risk Management and Cyber Security risk matrices. Risk values have been relatively assigned based on qualitative assessments of operational, financial, safety, environmental, and reputational impacts and likelihood of threat scenario occurrence, as informed by current threat intelligence.

Risk Definition	
Inherent Risk Values	**Inherent risk values** represent a relative ranking of risk likelihood and impact values to each environment (corporate IT, MRS OT, and non-MRS OT), without the application of BC Hydro's existing cyber security controls. Inherent risk values are informed by energy and resources sector threat landscape assessments within BC Hydro's environmental context, in the absence of controls.
Current Residual Risk Values	**Current Residual risk values** take into consideration the assessment of expected capabilities related to each threat scenario, and represent an adjusted risk based on these capabilities being in place. This rating is based on the assumption that the capabilities identified within the reviewed material and interviews are implemented as designed and are operating effectively, as no assessment of effectiveness was performed as part of this review.

Note that in some instances, BC Hydro's "Current Residual Risk" is rated as "Moderate". Typically, where the impact of an event is "High", the residual risk rating cannot be reduced to "Low" even with effective controls and capabilities in place. This reflects the need for continual monitoring and response to "high impact" risks whether they are related to cybersecurity, financial outcomes, health and safety or other domains. Further, given the very dynamic nature of cybersecurity risks and the ever-evolving motivations of threat actors and their respective tools and tactics, it is not necessarily possible to reduce such risks to "Low". Given

the complexity of organizations like BC Hydro and the evolving cyber threat landscape, certain threats may continue to require a high degree of management and oversight, and the ongoing refinement of cyber capabilities, and it may not be possible to reduce such risks to "Low" levels even with mature execution of all expected capabilities. Within the context of the critical infrastructures cyber landscape, certain threat likelihoods and/or impacts must be continually evaluated, and may not be practicably reduced, in which case organizations must reasonably accept certain risks and must plan and respond to the changing threat landscape accordingly.

In the interpretation of the results below, it should be noted that Deloitte did not perform any procedures regarding the operating effectiveness of controls or processes and, accordingly, do not express an opinion thereon. Because of the inherent limitations of internal control, including the possibility of collusion or improper management override of controls, material misstatements due to error or fraud may occur and not be detected. Also, projections of any evaluation of the internal control to future periods are subject to the risk that the internal control may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

SUMMARY OF CURRENT RESIDUAL RISK OUTCOMES

The following table provides a summary of the risk ratings associated each of the threat scenarios for the Corporate IT, MRS OT and Non-MRS OT environments within this section of the report. Further detail associated with each threat and corresponding inherent and residual risk can be found in the section below. It is understood that BC Hydro will evaluate and determine its response to these risks as part of their response to Directive 9.

Table 6 - Threat Scenario Risk Rating Summary

Threat Scenario	Environment	Inherent Risk	Current Residual Risk
T.01 – Major Ransomware Infection	Corporate IT	High	Moderate
	MRS OT	Moderate	Moderate
	Non-MRS OT	Moderate	Low
T.02 – Espionage by Advanced Persistent Threat	Corporate IT	High	Moderate
	MRS OT	Moderate	Low
	Non-MRS OT	Low	Low
T.03 – Supply Chain Attack Introduces Compromised Software	Corporate IT	High	Moderate
	MRS OT	High	Moderate
	Non-MRS OT	Moderate	Moderate
T.04 – Insider Facilitates Data Leakage	Corporate IT	High	Moderate
	MRS OT	High	Moderate
	Non-MRS OT	Moderate	Low
T.05 – Business Email Compromise	Corporate IT	Moderate	Low
	MRS OT	Low	Low
	Non-MRS OT	Low	Low
T.06 – External Network Service Compromise	Corporate IT	High	Moderate
	MRS OT	High	Low
	Non-MRS OT	Moderate	Moderate

T.01 MAJOR RANSOMWARE OUTBREAK

	Relative Risk Assessment			
Environment	Inherent Likelihood	Inherent Impact	Inherent Risk	Current Residual Risk
Corporate IT	MODERATE	HIGH	HIGH	MODERATE
MRS OT	LOW	HIGH	MODERATE	MODERATE
Non-MRS OT	LOW	MODERATE	MODERATE	LOW

✳ SUMMARY OBSERVATION

What does this mean for BC Hydro?

Traditionally there are fewer reported cases of threat actors introducing ransomware directly to ICS environments, given the physical presence requirements and controls which limit the impact radius within OT networks. However, this is still considered an important risk to monitor, as OT processes could be disrupted due to business processes and workflows which rely on information from corporate IT environments. Network architecture, privileged access, and privilege escalation vulnerabilities could enable a sophisticated threat actor to gain wide-spread access within the corporate environment. Should ransomware enter corporate networks, the extent of data encryption, exfiltration and operational disruption could be extensive.

During this assessment, Deloitte identified strengths in existing programs which provide BC Hydro with protective and detective controls that reduce the risk of this threat materializing, such as the use of Splunk for SIEM and the introduction of Mandiant EDR and MDR services as well as planned/inflight programs to address recommendations identified through previous assessments (Mandiant Ransomware Assessment, OAG ICS Assessment, and Siemens ICS Assessment).

✳ THREAT SCENARIO DESCRIPTION

What is the threat scenario?

Ransomware has become one of the most visible and devastating cyber threats impacting organizations today. Ransomware refers to the category of attacks in which threat actors deploy data-encrypting malware to an organization's network, rendering systems and data unusable until a ransom amount is paid. From the emergence of CryptoLocker in 2013, to the global WannaCry and Petya/NotPetya attacks of 2017, to the proliferation of human-operated and "big game hunting" ransomware is indiscriminately disrupting organizations today and has become a booming, lucrative criminal industry. Recent advancements in the "ransomware-as-a-service" and "initial access brokers" business models have further lowered the barrier to entry.

Human-operated ransomware – the norm today - involves hands-on-keyboard attackers using credential theft and lateral movement methods, traditionally associated with targeted attacks and advanced persistent threats (APT), to infiltrate networks, access and steal data, and deploy ransomware. These types of attacks often start with a phishing email (and often in conjunction with "commodity" malware which can be "banked" for a later time and purpose), by scanning and exploiting vulnerable systems (e.g. an unpatched VPN server), or by abusing legitimate (albeit insecure) services (e.g. remote desktop exposed to the internet). Once inside, these attackers are proficient at understanding preventative and detective controls and adapting their attacks to suit the situation. Ransomware operators have also shifted tactics to not only encrypt data and render systems unusable, but they also steal the data and threaten to leak it to the public if the ransom is not paid; this is known as the double extortion strategy, which was used in over half of ransomware attacks in 2020[15].

The ransomware threat landscape is not limited to large private businesses. Ransomware has been seen actively targeting and successfully extorting critical industries such as energy and resources, health care, and the public sector. Nation state actors have been documented conducting reconnaissance exercises against power and utilities companies both to steal valuable intellectual property (IP) and to evaluate future attack paths. Alleged Russian activity against the Ukraine in 2015 using Black Energy malware is a prime example. Further, while recent ransomware incidents against energy and utilities sector organizations have largely been limited to IT environments, due to critical dependencies and business workflows between the two otherwise separate environments, OT environments have been taken offline while incident response processes are underway (as was the case with Colonial Pipeline in 2021).

Environment-Specific Scenarios	
IT	*A threat actor conducting a broad phishing campaign coerces a BC Hydro employee to download and execute malware on their corporate workstation. The threat actor escalates privileges, compromises the domain, and deploys ransomware.*
MRS OT	*A threat actor uses valid internal access (obtained through social engineering of a BCH employee or contractor) goes to a NERC CIP site and plugs in a device (e.g. laptop or portable storage) which transfers ransomware to the connected systems.*
Non-MRS OT	*A threat actor gains physical access to an unoccupied substation facilitating power supply to a small community. The threat actor is able to gain access to the local area network inside the substation via an unsecured server cabinet and deploys ransomware.*

✳ KEY VECTORS

Key vectors typically used in this threat scenario

Phishing – Credential Theft	Scan and Exploit	Unpatched Software
Phishing – Malware	Supply Chain Compromise	Legacy Software
Network Exposure	Human Error / Misconfiguration	Insider Threat
	Social Engineering	

[15] IBM Security, 2021. X-Force Threat Intelligence Index.

T.01 MAJOR RANSOMWARE OUTBREAK

✳ EXPECTED CAPABILITIES

What is required to protect against this threat scenario?

Risk Assessment	Awareness & Training	Security Continuous Monitoring
Supply Chain Risk Management	Data Security	Mitigation
Access Control	Info. Protection Processes & Procedures	Recovery Planning

✳ CAPABILITY ASSESSMENT

How effectively does BC Hydro execute against this threat scenario?

Corporate IT

Identified Capabilities

- A formal cyber security training and awareness program, enabled through a learning management system
- FireEye EDR and Mandiant MDR deployed on all BC Hydro workstations and servers (IT) providing 24x7 coverage
- Traditional McAfee antivirus product is used for application restrictions and some custom macro / script blocking
- Email protection provided by IronPort, Cisco AMP, and Cisco Threat Grid to conduct malware detection, sandboxing, and analysis
- Use of McAfee Global Threat Intelligence (GTI) providing reputation-based protection services
- Workstations and servers are hardened according to the CIS Benchmarks hardening standards
- A vulnerability and patch management program has been established
- A system backup and restoration program
- Cisco Umbrella is deployed for DNS filtering and monitoring, and monitoring and protection of off-network laptops
- Centralized audit logging and Security Information and Event Monitoring (SIEM)
- End users do not have local administrative privileges by default
- Defined cyber security incident response procedures, and established incident response retainers and cyber insurance
- BC Hydro subscribes to industry and regional threat intelligence including E-ISAC, CCCS, and NERC information sharing committees
- Commitment to threat risk reduction through corporate environment ransomware focused assessment and remediation actions underway
- Cyber insurance and incident response retainer.

Observations for Immediate Action

- None.

Observations to Improve Control Environment

- Lack of a tiered administration model to manage privileged access and reduce privileged account footprint (although PAM controls are underway)
- Active Directory configuration weaknesses, including weaknesses in removal of common attack paths and user account security
- Network segmentation not fully in place to isolate higher-risk traffic on the corporate network (e.g. access to servers, workstation to workstation)
- Backup infrastructure is not segregated from the Corporate Active Directory and could be compromised by a ransomware attacker
- Insufficient 24/7 dedicated security monitoring and response capability
- Current coverage of vulnerability scanning may not be adequate to identify vulnerabilities (active project underway to expand this with Tenable)
- Lack of regular, full-scope penetration testing and/or red teaming.

Additional Observations for Consideration

- Large-scale response and recovery technical procedures are not defined to support a major, cross-environment ransomware outbreak

Residual Risk Summary

While many good security practices were noted which reduce the likelihood of a major ransomware incident in the Corporate IT environment, BC Hydro should continue to focus on improving capabilities to prevent lateral movement and privilege escalation, and improve detection, response, and recovery capabilities to reduce the extended impact of a successful infection. While the likelihood of initial infection has been reduced, the impact of a major infection would be severe; as such, the residual risk of a major ransomware infection is assessed to be ***MODERATE.***

T.01 MAJOR RANSOMWARE OUTBREAK

MRS OT

Identified Capabilities

- The NERC CIP compliance program ensures that minimum cyber security controls are in place to protect high impact systems and maintain the resilience and reliability of the grid. Several existing capabilities were noted which were in place which address the risk of ransomware, including:
  - Cyber security risk assessment processes
  - Vulnerability identification processes
  - Security hardening and configuration management
  - Physical and logical access controls
  - Segmentation between IT and OT environments, including network and domain segmentation and an intermediate access zone
  - The use of dedicated, hardened "green laptops" for physical access at MRS OT facilities.
- MRS teams are included in CSIRP and teams participate in IR simulations

Observations for Immediate Action

- None.

Observations to Improve Control Environment

- Insufficient 24/7 dedicated cyber security monitoring and response capability (cybersecurity capability is limited outside of office hours)
- The current security monitoring solution is largely focused on compliance-driven use cases (rather than proactive threat detection)
- Privileged access management is not formally managed through a PAM solution (with the exception of some key check out procedures)

Additional Observations for Consideration

- Lack of network access controls to prevent connection of unauthorized devices

Residual Risk Summary

The segmentation of the MRS OT environment coupled with the capabilities implemented as part of the NERC CIP compliance program, which benefit from ongoing reporting, significantly reduce the likelihood of a major ransomware outbreak either starting in the MRS OT environment OR reaching the MRS OT network from Corporate IT environment. However, what is currently unclear is what the impact would be if such an event did occur within the MRS OT environment, or what the relative effect would be on MRS OT if the Corporate IT environment was to be completely incapacitated for an extended period of time. The residual risk rating of a major ransomware infection in MRS OT is assessed to be ***MODERATE****.*

NON-MRS OT

Identified Capabilities

- Change management processes deter against and identify unauthorized changes to systems through approval and documentation requirements
- Individuals are required to take security clearance-based awareness and training
- OT environments are included in the CSIRP
- Serial firewalls have been implemented in substations with connectivity which block administrative commands to the network
- Non-MRS OT systems are beginning to adopt workflows and controls which align to existing NERC compliance requirements.

Observations for Immediate Action

- None.

Observations to Improve Control Environment

- Cyber security capabilities for non-MRS OT lag behind those for MRS systems, including the following key areas:
  - User access reviews
  - Password vaulting
  - Least-privilege access management
  - Lack of active monitoring of events and alerts
  - Configuration baseline management and reviews
  - Lack of active or passive vulnerability scanning
  - Tested cyber incident response plans

Additional Observations for Consideration

- None.

Residual Risk Summary

Due to non-MRS OT systems locations, fewer external routable connectivity capabilities, the ability to directly impact broader operational processes and technologies is reduced, however there is potential for lateral movement from the corporate network with lower levels of monitoring in place within the non-MRS OT network. This results in a residual non-MRS ransomware risk assessment of ***LOW.***

T.01 MAJOR RANSOMWARE OUTBREAK

✳ RECOMMENDATIONS

For additional information refer to Recommendations section

Note: Definitions of the Value, Complexity and Priority ratings is contained within the Recommendations section of this report.

ID	Recommendation title	Environment	Value	Complexity	Priority
REC-GEN-04	Expand SOC resourcing	All	HIGH	HIGH	HIGH
REC-GEN-05	Consolidate SIEM	All	HIGH	HIGH	HIGH
REC-COPR-02	Continue securing backups	Corp IT	HIGH	HIGH	HIGH
REC-CORP-03	Continue vulnerability management expansion	Corp IT	HIGH	MEDUIM	HIGH
REC-CORP-05	Continue AD hardening	Corp IT	HIGH	MEDIUM	HIGH
REC-CORP-06	Expand network security toward zero trust	Corp IT	HIGH	HIGH	HIGH
REC-NONREG-02	Implement configuration monitoring	Non-MRS OT	HIGH	HIGH	HIGH
REC-NONREG-04	Implement the planned vulnerability scanning and penetration testing program	Non-MRS OT	HIGH	MEDIUM	HIGH
REC-GEN-06	Expand and consolidate PAM	All	HIGH	HIGH	MEDIUM
REC-CORP-11	Implement enterprise red teaming	Corp IT	HIGH	LOW	MEDIUM
REC-CORP-12	Complete addition of CSIRP playbooks	Corp IT	HIGH	MEDIUM	MEDIUM
REC-REG-03	Implement consolidated PAM	MRS OT	HIGH	HIGH	MEDIUM
REC-NONREG-05	Implement consolidated PAM	Non-MRS OT	HIGH	HIGH	MEDIUM
REC-NONREG-06	Adopt consolidated SIEM	Non-MRS OT	HIGH	HIGH	MEDIUM
REC-NONREG-07	Expand use of jump hosts	Non-MRS OT	MEDIUM	MEDIUM	MEDIUM
REC-REG-06	Expand network security towards zero trust	MRS OT	MEDIUM	HIGH	LOW

T.02 ESPIONAGE BY ADVANCED PERSISTENT THREAT

	Relative Risk Assessment			
Environment	Inherent Likelihood	Inherent Impact	Inherent Risk	Current Residual Risk
Corporate IT	MODERATE	HIGH	HIGH	MODERATE
MRS OT	LOW	MODERATE	MODERATE	LOW
Non-MRS OT	LOW	LOW	LOW	LOW

✳ SUMMARY OBSERVATION

What does this mean for BC Hydro?

Advanced Persistent Threat (APT) groups use sophisticated TTPs to enter, maintain presence within, laterally move within, and escalate privileges within, a network. The energy sector, especially North America's connected grid system, is known as a high value target for APT groups looking to exfiltrate valuable information or position for subsequent attacks on the electrical grid. The Canadian Centre for Cyber Security, in their September 29th 2020 Bulletin, assessed that cybercriminals will almost certainly continue to target the Canadian electricity sector to extract ransom, steal intellectual property and proprietary business information, and obtain personal data about customers.

OT environments have a lower risk of APT threats as a result of their reduced attack surface, where it would be more complex to persist within and exfiltrate data. However, recent smart grid advancements have increased this threat likelihood targeting OT environments. In addition, given the sensitive nature of data stored in corporate networks, and the sophistication of APT threat actor TTP's, the risk of APT threat actors is high in corporate IT environments.

During this assessment, we identified controls within the corporate IT environment that could reduce the risk of APT threat actors maintaining a presence. In addition, we identified controls that segregate the OT environments. However, given the advanced nature of these attacks and the motivation of threat actors, the impact of such a threat materializing continues to remain high, and the likelihood cannot be entirely removed through controls.

✳ GENERAL DESCRIPTION

What is this threat scenario?

Espionage activities often come from sophisticated threat actors such as APT groups attempting to obtain intellectual property and information about the ICS within a utility (such as BC Hydro). This intellectual property and information can be used by a sponsoring government or organization and can be used as an indirect route to access power supply networks, and especially connections to the US power grid. Canadian power companies can be of particular value to threat actors attempting to conduct espionage because of the connectedness of the North American power grid.

APT groups will leverage sophisticated exploitation techniques to gain initial access and spend months (if not years) maintaining an undetected presence with the intent of collecting valuable industrial and corporate information (not necessarily customer information for extortion, but more often information that would allow for control of systems or functions within an organization or communications intelligence passing through an organization) and pre-positioning additional cyber and exploitation tools as a contingency for possible follow-on activities.

Environment-Specific Scenarios	
IT	*A threat actor sends a targeted email with a malicious Word document attached to a BC Hydro corporate procurement email account which appears to be an invoice. Upon opening the Word document an embedded macro runs which is able to make alterations to the environment to establish a connection with a malicious server (i.e. C2 server).*
MRS OT	*A threat actor is able to leverage established corporate network access to obtain credentials for a valid user with remote access to BC Hydro NERC INTERMEDIATE domain and EMS production servers. Once multi-factor RSA authentication mechanism is defeated and they are able to get inside using the harvested credentials, the threat actor is able to establish persistent access for themselves.*
Non-MRS OT	*A threat actor is able to gain physical access to an unoccupied substation. Inside the substation the threat actor is able to catalogue key systems, view SCADA and HMI systems, and make note of other physical security barriers for future evasion and exploitation of other substations and sites.*

✳ KEY VECTORS

How could this threat scenario materialize?

Scan and exploitation	Supply chain compromise	Unpatched software
Legacy software	Spear-phishing	Network exposure

✳ EXPECTED CAPABILITIES

What is required to protect against this threat scenario?

Risk Assessment	Awareness & Training	Security Continuous Monitoring
Supply Chain Risk Management	Data Security	Mitigation
Access Control	Info. Protection Processes & Procedures	Recovery Planning

T.02 ESPIONAGE BY ADVANCED PERSISTENT THREAT

✳ CAPABILITY ASSESSMENT

How effectively does BC Hydro execute against this threat scenario?

Corporate IT

Identified Capabilities

- Strong functional zone network segmentation to limit a threat actors' ability to move across IT and OT networks
- Vulnerability management processes remediate exploits within systems which could be used by sophisticated threat actors
- Mandiant active threat hunting on endpoints with FireEye EDR
- Threat intel is received and reported upon from established sources
- Identity governance processes apply strong controls around the creation of identities, and they access permissions inside of systems.

Observations for Immediate Action

- None.

Observations to Improve Control Environment

- Penetration testing currently conducted on project-by-project basis (approved penetration testing plan to be implemented in FY22)
- Privileged access governance, limited processes to restrict capabilities associated with privileged accounts
- NetFlow monitoring and analysis are not performed
- Threat hunting is limited to endpoints.

Additional Observations for Consideration

- NAC and device detection capabilities are immature and do not enable real time identification and response to rogue devices establishing connections, and does not position BC Hydro for deployment of zero trust architectures
- No use of deceptive techniques such as decoy devices, systems, files, accounts, etc.
- Data leak prevention capabilities are not established which would detect or prevent critical information from being exfiltrated from online locations.

Summary

In summary there are some strong foundational capabilities which would prevent a sophisticated actor from entering BC Hydro networks and establishing a presence to conduct intellectual property theft and espionage. However, there is a lack of detective-type controls which would identify if a sophisticated threat actor were successful in bypassing security controls and establishing a presence within the network.

The likelihood of the event has been reduced with expected foundational preventative controls, but BC Hydro's lack of detective controls to identify sophisticated threat actors in the network, and lack of protective controls (i.e. DLP, encryption, etc.) on sensitive customer and operational/energy infrastructure information stored on BC Hydro corporate networks in combination with the nature of this sophisticated threat actor results in a residual risk rating of MODERATE.

MRS OT

Identified Capabilities

- Vulnerability management is defined and robustly applied across MRS environments to ensure that patches are applied in a timely manner
- A penetration testing strategy has been developed to identify vulnerabilities in systems and processes
- Network segmentation prevents threat actor movement and limits data exposure
- Both physical and logical access is controlled at defined security perimeters
- Access governance processes are executed.

Observations for Immediate Action

- None.

Observations to Improve Control Environment

- The penetration testing strategy has not yet been implemented (to be implemented FY22)
- Monitoring does not leverage a robust set of use cases to detect advanced threats.

Additional Observations for Consideration

- Threat hunting is not performed which would identify an established malicious presence inside of BC Hydro networks.

Summary

The MRS OT environment has reduced exposure to a sophisticated threat actor from gaining and establishing a persistent presence inside the network based on network segmentation controls and authentication requirements when moving across security perimeters. These can limit the movement of a threat actor. The MRS OT environment therefore is assessed as having a residual risk rating of LOW.

T.02 ESPIONAGE BY ADVANCED PERSISTENT THREAT

NON-MRS OT

Identified Capabilities

- OT environments are included in CSIRP and teams participate in incident response simulations
- Authentication requirements enforced for remote access.

Observations for Immediate Action

- None.

Observations to Improve Control Environment

- Patch identification is not delivered across the environment, and as a result many systems could be vulnerable to exploitation
- Access governance controls and processes, such as password rotation and nonrepudiation *(i.e. assured attribution of an event to a specific individual)* of authentication events is not executed effectively
- Limited log capture across environment
- Security monitoring and detection processes are limited.

Additional Observations for Consideration

- None.

Summary

The non-MRS OT environment does not provide a robust set of controls which would prevent a sophisticated threat actor from obtaining access to the environment. However, the OT environment design does not provide an easily exploitable attack surface. Many systems are not routable, and many devices operate in such remote and small sites on legacy equipment that intellectual property and data contained with the environment would be limited in value to a threat actor. As a result, the residual risk rating is assessed as ***LOW.***

✳ RECOMMENDATIONS

For additional information refer to Recommendations section

Note: Definitions of the Value, Complexity and Priority ratings is contained within the Recommendations section of this report.

ID	Recommendation title	Environment	Value	Complexity	Priority
REC-GEN-09	Implement network anomaly analysis	All	MEDIUM	LOW	HIGH
REC-CORP-06	Expand network security towards zero trust	Corp IT	HIGH	HIGH	HIGH
REC-REG-02	Implement ICS specialized detection	MRS OT	HIGH	MEDIUM	HIGH
REC-NONREG-03	Implement patch deployment cadence	Non-MRS OT	HIGH	MEDIUM	HIGH
REC-GEN-06	Expand and consolidate PAM	All	HIGH	HIGH	MEDIUM
REC-GEN-08	Expand threat hunting	All	HIGH	HIGH	MEDIUM
REC-CORP-08	Complete CyberArk Implementation	Corp IT	HIGH	HIGH	MEDIUM
REC-CORP-09	Execute penetration testing strategy	Corp IT	HIGH	HIGH	MEDIUM
REC-NONREG-05	Implement consolidated PAM	Non-MRS OT	HIGH	HIGH	MEDIUM
REC-NONREG-06	Adopt consolidated SIEM	Non-MRS OT	HIGH	HIGH	MEDIUM
REC-CORP-13	Implement deceptive detection tactics	Corp IT	HIGH	LOW	LOW
REC-CORP-15	Implement data leak prevention controls	Corp IT	MEDIUM	HIGH	LOW
REC-NONREG-09	Implement ICS specialized detection	Non-MRS OT	MEDIUM	MEDIUM	LOW

T.03 SUPPLY CHAIN ATTACK INTRODUCES COMPROMISED SOFTWARE

	Relative Risk Assessment			
Environment	Inherent Likelihood	Inherent Impact	Inherent Risk	Current Residual Risk
Corporate IT	MODERATE	HIGH	HIGH	MODERATE
MRS OT	MODERATE	HIGH	HIGH	MODERATE
Non-MRS OT	MODERATE	MODERATE	MODERATE	MODERATE

✳ SUMMARY OBSERVATION

What does this mean for BC Hydro?

Supply chain attacks can originate from deep inside a third parties value chain[16]. Even organizations with mature cyber programs are not immune to this threat. To effectively treat the associated risk, organizations must operate robust controls across all cyber capability categories. Even with controls in place to protect against this threat, the sophistication of the threat actor deploying associated techniques, makes effective protection challenging.

BC Hydro has reduced their attack surface through restricting and limiting the level of access permitted to third parties, and through the implementation of processes to configure and monitor systems within their environment. In addition, the visibility into threats obtained from threat intelligence and their use of BitSight provides for a more rapid response to any identified threat at a sector level. Opportunities for improvement exist for BC Hydro to maintain an inventory of all third parties and implement additional and ongoing assessments of their cyber capabilities.

✳ GENERAL DESCRIPTION

What is this threat scenario?

Hardware and software vendors, and managed service providers (MSPs) provide critical products and services to utilities organizations and enable effective management of a complex technology environment. A supply chain compromise occurs when products are deliberately exploited and altered prior to use by a target organization, causing backdoored software which appears to be legitimate to be introduced to a target organization.

Highly sophisticated cyber threat actors (or APTs) will target supply chain linkages and MSPs and leverage their trusted relationship as an intermediary for obtaining unauthorized access to networks or systems through malware execution. Protecting against these threats can be challenging for mature organizations[17] due to limited visibility into how third parties and MSPs are protecting themselves from cyber-attacks. As attackers target vulnerabilities within the supply chain, BC Hydro has limited visibility into embedded malware, rendering certain detective and protective controls ineffective. BC Hydro must rely on suppliers to protect against threat scenario vectors such as malware infection, social engineering, credential stuffing/brute-force attacks, etc.

Environment Specific Scenarios	
IT	*A threat actor is able to corrupt software updates from a valid BC Hydro software vendor with malware. Upon deployment of the software update to BC Hydro workstations, the malware is inserted onto all related workstations.*
MRS OT	*A threat actor is able to infiltrate networking service providers. Upon infiltration of the service provider team managing BC Hydro firewalls, the threat actor is able to make configuration changes which enable them to gain access to OT networks.*
Non-MRS OT	*A threat actor is able to place a sophisticated exploit into an OT system which enables a threat actor to establish a remote connection and make commands to site systems by bypassing the serial firewall.*

✳ KEY VECTORS

How could this threat scenario materialize?

SDLC	Patching	Phishing / Spear-phishing
Physical access	Logical / Electronic access	

✳ EXPECTED CAPABILITIES

What is required to protect against this threat scenario?

Supply Chain Risk Management	Maintenance	Info. Protection Processes & Procedures
	Security Continuous Monitoring	

[16] hxxps://www.nytimes.com/2016/11/16/us/politics/china-phones-software-security.html

[17] CISA, 2021.Defending Against Software Supply Chain Attacks.

T.03 SUPPLY CHAIN ATTACK INTRODUCES COMPROMISED SOFTWARE

✳ CAPABILITY ASSESSMENT

How effectively does BC Hydro execute against this threat scenario?

Corporate IT

Identified Capabilities

- Performing a risk-based due-diligence of third parties with baseline controls from major cyber security frameworks such as NIST and ISO
- Ongoing third-party passive scanning using BitSight platform to provides insights into third party external cyber risk posture
- Testing vendor supplied patches before implementation
- Use of separate non-production environment for release of new systems and system updates
- Including major third parties (TELUS) in cyber security exercises, i.e. incident simulation exercise
- Adhering to vendor best practices and CIS controls for middleware/application hardening
- Maintaining standards for approved list of software, hardware and cloud services
- Leveraging threat intelligence to monitor for and identify emerging threats in industry supply chains.

Observations for Immediate Action

- None.

Observations to Improve Control Environment

- Current vendor directory is focused on procurement management and does not include relevant cyber security information including assigned access, scope of responsibilities, key contacts, etc.

Additional Observations for Consideration

- There is a level of risk associated with concentration of management of critical infrastructure (domain services e.g. AD, cryptography infrastructure e.g. RSA, access control jump hosts e.g. NERC INTERMEDIATE, etc.)

Summary

The corporate IT environment has controls in place which reduce the likelihood of a supply chain attack causing disruptions and service outages. Given the nature of these threats there is a level of uncertainty when applying due diligence and cyber security controls to vendors and suppliers. These threats can be deeply embedded in supply chains where detection can be challenging. While BC Hydro's controls can reduce this risk, the characteristics of this threat scenario result in residual risk rating for corporate IT of MODERATE.

MRS OT

Identified Capabilities

- Performing a risk-based due-diligence of third parties with baseline controls from major cyber security frameworks such as NIST and ISO
- Ongoing third-party passive scanning using BitSight platform to provide insights into third party external cyber risk posture
- Testing vendor supplied patches before implementation
- Vendor leverage the non-persistent VDI environment for access, which is limited to a small subset of vendors (QA only)
- Vendor solutions are maintained internally, with little reliance on vendor expertise
- Use of separate non-production environment for release of new systems and system updates - the MRS environment leverages a separate domain. Separate environments are maintained for Development, Training and QA (in one zone) and a separate zone for Production and Electronic Security Perimeter domains
- Access controls for NERC CIP confidential information sharing, and access to physical environments
- Configuration integrity monitoring through SigmaFlow
- Leveraging threat intelligence to monitor for and identify emerging threats in industry supply chains.

Observations for Immediate Action

- None.

Observations to Improve Control Environment

- MRS monitoring is compliance focused and may not detect supply chain based threats
- No penetration testing (penetration testing strategy is developed and to be implemented FY22) to identify vulnerabilities in systems and processes
- Current vendor directory is focused on procurement management and does not include relevant cyber security information including assigned access, scope of responsibilities, key contacts, etc.

Additional Observations for Consideration

- There is a level of risk associated with concentration of management of critical infrastructure (domain services e.g. AD, cryptography infrastructure e.g. RSA, access control jump hosts e.g. NERC INTERMEDIATE, etc.)

Summary

Despite the number of controls in place this continues to be one of the top threats faced by organizations. Vulnerabilities in vendor supplied OT hardware and software could persist without BC Hydro's knowledge. Prevention of this kind of threat demands vigilance when introducing new hardware and software into the environment, and BC Hydro has several relevant capabilities in place. However, the nature of this threat, and the complexity in preventing and detecting it, result in a residual risk rating of MODERATE.

T.03 SUPPLY CHAIN ATTACK INTRODUCES COMPROMISED SOFTWARE

NON-MRS OT

Identified Capabilities

- Performing a risk-based due-diligence of third parties with baseline controls from major cyber security frameworks such as NIST and ISO
- Ongoing third-party passive scanning using BitSight platform to provides insights into third party external cyber risk posture
- Testing vendor supplied patches before implementation
- Use of separate non-production environment for release of new systems and system updates
- Leveraging threat intelligence to monitor for and identify emerging threats in industry supply chains.

Observations for Immediate Action

- None.

Observations to Improve Control Environment

- No vulnerability scanning or penetration testing (strategy is developed and to be implemented FY22) to identify vulnerabilities
- Inconsistent patching program
- Lack of configuration standards, and system integrity monitoring
- Current vendor directory is focused on procurement management and does not include relevant cyber security information including assigned access, scope of responsibilities, key contacts, etc.

Additional Observations for Consideration

- Third party management of certain critical infrastructure (domain services e.g. AD, cryptography infrastructure e.g. RSA, access control jump hosts e.g. NERC INTERMEDIATE, etc.)

Summary

Despite the number of controls in place this continues to be one of the top threats faced by organizations. Without proper vigilant controls in place, vulnerabilities in vendor supplied OT hardware and software could persist without BC Hydro's knowledge. The residual risk rating is assessed as MODERATE.

✳ RECOMMENDATIONS

For additional information refer to Recommendations section

Note: Definitions of the Value, Complexity and Priority ratings is contained within the Recommendations section of this report.

ID	Recommendation title	Environment	Value	Complexity	Priority
REC-REG-02	Implement ICS specialized detection	MRS OT	HIGH	MEDIUM	HIGH
REC-NONREG-02	Implement configuration monitoring	Non-MRS OT	HIGH	HIGH	HIGH
REC-NONREG-03	Implement patch deployment cadence	Non-MRS OT	HIGH	MEDIUM	HIGH
REC-NONREG-04	Implement the planned vulnerability scanning and penetration testing program	Non-MRS OT	HIGH	MEDIUM	HIGH
REC-GEN-07	Expand third-party monitoring	ALL	MEDIUM	MEDIUM	MEDIUM
REC-GEN-08	Expand threat hunting	All	HIGH	HIGH	MEDIUM

T.04 INSIDER FACILITATES DATA LEAKAGE

	Relative Risk Assessment			
Environment	Inherent Likelihood	Inherent Impact	Inherent Risk	Current Residual Risk
Corporate IT	MODERATE	HIGH	HIGH	MODERATE
MRS OT	MODERATE	HIGH	HIGH	MODERATE
Non-MRS OT	MODERATE	MODERATE	MODERATE	LOW

✳ SUMMARY OBSERVATION

What does this mean for BC Hydro?

The threat of data leakage from insiders with access to sensitive or confidential information continues to be high for the utilities sector. BC Hydro has existing strengths which reduce the potential for data leaks associated with insider access, including identity and access management processes and technical controls, EDR protection on corporate devices, USB blocking, awareness and training, and the green laptop OT initiative.

There are several opportunities for improvement across Corporate IT, MRS OT, and Non-MRS OT which should be considered to further reduce the insider data leak risks, including strengthening internal and external monitoring and detection capabilities, bolstering network protection using a NAC solution or implementation of zero trust, UEBA monitoring, DLP technologies, and furthering TLS inspection capabilities.

✳ GENERAL DESCRIPTION

What is this threat scenario?

The data that organizations hold is vital for operations, but also introduces a target for threat actors. Different threat actors may target sensitive data for different reasons: Cyber criminals may target customer data as a method of extorting an organization; or disgruntled employees may attempt to post sensitive data broadly online in an attempt to damage the reputation of an organization; or Hacktivists may target organizations in order to cause media scrutiny which could cause significant reputational damage.

Insiders have valid access to affect BC Hydro's information systems, sensitive data, and operational processes. The risk associated with specific individuals is related to their levels of access and to the types of information they have access to (e.g., customer data repositories or data regarding ICS control systems).

Existing known threat actors, such as the ransomware gang LockBit, are changing their tactics, techniques, and procedures to include the recruitment of persons inside companies, who can be motivated to expose or provide internal network information.

Environment Specific Scenarios	
IT	*A threat actor uses their insider access to access, exfiltrate, and publish a large customer data set.*
MRS OT	*An insider sees that a malicious group is offering a large monetary payout for providing access to ICS networks. The insider threat actor provides valid credentials to a malicious threat actor.*
Non-MRS OT	*A threat actor has obtained sensitive information about a current employee at BC Hydro. The threat actor blackmails the employee to destroy SCADA equipment at a substation.*

✳ KEY VECTORS

How could this threat scenario materialize?

Credential Theft	Phishing	Human Error
Valid access	Misconfigurations	Malicious Insider

✳ EXPECTED CAPABILITIES

What is required to protect against this threat scenario?

Asset Management	Awareness & Training	Info. Protection Processes and Procedures
Security Continuous Monitoring	Communications	

T.04 INSIDER FACILITATES DATA LEAKAGE

✳ **CAPABILITY ASSESSMENT** *How effectively does BC Hydro execute against this threat scenario?*

Corporate IT

Identified Capabilities

- Role based access control provides least privilege access control for users
- Identity and access management processes are automated through CA IDM
- Change control processes prevent unauthorized changes to the environment
- FireEye EDR provides alerts to BC Hydro via dedicated console, while Mandiant MDR provides further 24x7 alerting to high risk incidents
- Mandiant MDR provides biweekly threat hunting
- Splunk SIEM environment provides monitoring of the environment, and has data exfiltration use cases defined
- External data shares (SFTP) are monitored
- Local administration rights are restricted
- Cyber security training and awareness program educates users on identifying potential data breaches and reporting cyber incidents
- Regular phishing simulations are performed for all BC Hydro employees, and a phishing reporting capability has been deployed
- Physical controls are designed for least privilege
- Cisco Umbrella is deployed for DNS filtering and monitoring of common data upload / exfiltration services, which generates alerts on suspected incidents
- Removable media, such as USB sticks, is blocked which could prevent an insider from copying data onto removable media.

Observations for Immediate Action

- None.

Observations to Improve Control Environment

- No dedicated real time threat intelligence or Dark Web monitoring, e.g. credential leaks, initial access brokers
- Cisco Umbrella logs are not yet ingested into Splunk; certain database systems and applications do not provide log feeds into SIEM solution
- NetFlow analysis is not in place to detect abnormal data transfers
- TLS inspection is not performed on the perimeter
- PAM solution is not fully implemented (although CyberArk solution is being rolled out)
- No data asset inventory is in place (inventory is focused on physical and software assets)
- Data flow mappings do not exist
- Internal corporate network segmentation is not robust, (e.g. critical servers, workstation-to-workstation, and hypervisor are in the same network segment)
- Log data for backup infrastructure is not ingested for monitoring of inappropriate access
- No NAC solution in place.

Additional Observations for Consideration

- Data leak prevention capabilities are not established
- UEBA is not applied as part of detection processes (FireEye EDR provides some capability to scoped endpoints)
- Recovery planning is not designed to contain and mitigate insider threat events, and different types of insider threats (sabotage, fraud, IP theft).

Residual Risk Summary

Prevention of insider threat events requires more than common data protection and access controls. Mature data protection capabilities such as DLP and UEBA technologies which could prevent or detect insiders from exfiltrating large amounts of data from the environment, are not present. As a result, BC Hydro's assessed residual risk rating is MODERATE.

T.04 INSIDER FACILITATES DATA LEAKAGE

MRS OT

Identified Capabilities

- Asset registers to maintain an inventory of critical systems, providing a clear inventory of critical systems and the data contained within
- Green laptops to enable monitoring, and limitations to internet connections (i.e. to prevent exfiltration of data and emailing/posting to a cloud storage provider)
- File transfer is limited to Green Laptops with green removable media, or File transfer Service
- Network segmentation prevents the traversal of data across IT and OT networks
- Corporate networks do not have direct connections to OT environment
- Training assigned by role security clearances
- Serial firewalls prevent administrative commands to serial connected devices
- Intrusion Detection Systems (IDS) are in place at network boundaries
- Change control processes which prevent the unauthorized modification of systems.

Observations for Immediate Action

- None.

Observations to Improve Control Environment

- Monitoring and detection visibility, use cases do not contain user focused anomaly detection
- Lack of 24x7 monitoring by security team individuals, a control room engineer would be the only individual present during night shifts and may not be trained to contain a cyber incident (the individual would enact the CSIRP and call an on-call staff).

Additional Observations for Consideration

- Recovery planning is not designed to contain and mitigate insider threat events, and different types of insider threats (sabotage, fraud, IP theft)
- Absence of data leakage detection mechanisms.

Residual Risk Summary

The MRS OT environment has controls in place which limit the likelihood of an insider threat exfiltrating sensitive data or making unauthorized changes to a system. However, there are some gaps in detective controls which would enable nonrepudiation and timely detection of events. The residual risk rating is assessed as MODERATE.

NON-MRS OTs

Identified Capabilities

- Training assigned by role security clearances
- Serial firewalls prevent administrative commands to serial connected devices
- Change control processes which prevent the unauthorized modification of systems.

Observations for Immediate Action

- None.

Observations to Improve Control Environment

- Lack of asset visibility which would provide a clear inventory of critical systems and the data contained within
- Field engineers often share a single set of credentials for access to site systems
- Monitoring and detection visibility, use cases do not contain user focused anomaly detection
- The use of shared account creates a risk of non-repudiation on access to data (for some shared accounts)
- Lack of 24x7 monitoring by security team individuals; some environments closely related to MRS systems may have a control room engineer present during night shifts.

Additional Observations for Consideration

- Recovery planning is not designed to contain and mitigate insider threat events, and different types of insider threats (sabotage, fraud, IP theft)
- Absence of data leakage detection mechanisms.

Residual Risk Summary

The non-MRS OT environment does not have technical controls in place which would deter or prevent an insider threat from acting maliciously within the environment, including common access control mechanisms. However, there are a limited number of individuals with access to the non-MRS OT environment, reducing the threat likelihood. There are ongoing initiatives which will align non-MRS environmental controls with those found in the MRS environment over the course of 3 – 5 years. The residual risk rating is assessed as LOW.

T.04 INSIDER FACILITATES DATA LEAKAGE

✳ RECOMMENDATIONS

For additional information refer to Recommendations section

Note: Definitions of the Value, Complexity and Priority ratings is contained within the Recommendations section of this report.

Reference No.	Recommendation title	Environment	Value	Complexity	Priority
REC-GEN-03	Continue asset management formalization	All	HIGH	HIGH	HIGH
REC-CORP-01	Expand logs to SIEM	Corp IT	HIGH	HIGH	HIGH
REC-CORP-06	Expand network security toward zero trust	Corp IT	HIGH	HIGH	HIGH
REC-REG-01	Expand logs to SIEM	MRS OT	HIGH	HIGH	HIGH
REC-NONREG-01	Implement asset management planning	Non-MRS OT	HIGH	MEDIUM	HIGH
REC-GEN-06	Expand and consolidate PAM	ALL	HIGH	HIGH	MEDIUM
REC-REG-04	Expand detection abilities	MRS OT	HIGH	MEDIUM	MEDIUM
REC-CORP-10	Expand threat intelligence	Corp IT	HIGH	LOW	MEDIUM
REC-CORP-12	Complete addition of CSIRP playbooks	Corp IT	HIGH	MEDIUM	MEDIUM
REC-NONREG-05	Implement consolidated PAM	Non-MRS OT	HIGH	HIGH	MEDIUM
REC-NONREG-06	Adopt consolidated SIEM	Non-MRS OT	HIGH	HIGH	MEDIUM
REC-GEN-10	Develop dataflow mappings	All	HIGH	HIGH	LOW
REC-CORP-14	Continue to enhance user anomaly detection	Corp IT	HIGH	MEDIUM	LOW
REC-CORP-15	Implement data leak prevention controls	Corp IT	MEDIUM	HIGH	LOW

T.05 BUSINESS EMAIL COMPROMISE

	Relative Risk Assessment			
Environment	Inherent Likelihood	Inherent Impact	Inherent Risk	Current Residual Risk
Corporate IT	HIGH	MODERATE	MODERATE	LOW
Non-MRS OT	LOW	LOW	LOW	LOW
MRS OT	LOW	LOW	LOW	LOW

✳ SUMMARY OBSERVATION

What does this mean for BC Hydro?

Email threats apply primarily to Corporate IT, as this environment houses the email infrastructure. MRS OT and Non-MRS-OT do not run email infrastructure, and devices within these environments do not access email services. MRS OT and Non-MRS OT are segregated from the Corporate IT environment, limiting the impact of email threats that may materialize in Corporate IT.

BC Hydro has implemented several capabilities to address email threats, including organization-wide cyber security awareness, an integrated email security platform, DNS and URL filtering, and multi-factor authentication for remote access to services. While capabilities in place reduce the likelihood and impact of email threats, in particular phishing and credential theft threats, BC Hydro should continue to strengthen capabilities to respond to email threats within their response plans. BC Hydro should also consider the potential likelihood and impact of MRS-OT and Non-MRS OT information that could be disclosed through a Corporate IT email threat event (e.g. leakage of information).

Note – Business processes to prevent or detect downstream effects of Business Email Compromise (BEC) such as wire fraud, payroll changes etc. have not been assessed

✳ GENERAL DESCRIPTION

What is this threat scenario?

Social engineering continues to be the top attack pattern leading to cyber security breaches today[18]. Unsurprisingly, phishing makes up the vast majority of social engineering attacks, followed closely by BEC. Social engineering attacks often lead to theft of credentials which can be used in later attacks (e.g. to access remote access or cloud systems), and to distribution of malware.

The most common types of malware distributed through phishing and spam emails are command and control (C2), backdoors, and trojans. Malware distributed by phishing and spam is often the first stage of a larger attack (e.g. ransomware), whereby the initial compromise and malware sits for a period of time before being activated or upgraded to a second stage, often interactive, malware.

Business email compromise (BEC) refers to an email-based cyber-attack which is intended to gain access to critical business information or extract money through email-based fraud. In a BEC attack, cyber criminals send email that appears to be coming from a trusted person's (e.g. the CEO, CFO, manager, trusted colleague) email address (using a compromised employee or third party's email account, or simply a fake account) and attempts to extract sensitive business or financial information, or process a payment-related request (e.g. wire transfer, payroll change). According to the FBI's 2020 Internet Crime Report, the FBI received over 19,000 business email compromise complaints in 2020, with adjusted losses of over $1.8 billion.

Environment Specific Scenarios	
IT	*A BC Hydro employee receives a mass campaign phishing email, clicks the malicious link, and enters their BC Hydro credentials. The cyber-criminal uses the stolen credentials to access the email account of the BC Hydro employee.*
MRS OT	*A BC Hydro employee receives a phishing email containing a malicious document. The employee opens the malicious document which executes malware on their corporate computer. The cyber-criminal pivots from the corporate network to the OT network.*
Non-MRS OT	*A BC Hydro employee receives a phishing email containing a malicious document. The employee opens the malicious document which executes malware on their corporate computer. The cyber-criminal pivots from the corporate network to the OT network.*

✳ KEY VECTORS

Examples of how this threat scenario could materialize

Spear phishing	Phishing / Spam	Pre-texting
Cloud storage phishing	Mobile phishing	Supply chain compromise

✳ EXPECTED CAPABILITIES

What is required to protect against this threat scenario?

Governance	Info. Protection Processes & Procedures	Supply Chain Risk Management
Awareness and Training	Security Continuous Monitoring	

[18] Verizon, 2021. 2021 Data Breach Investigations Report.

T.05 BUSINESS EMAIL COMPROMISE

✳ CAPABILITY ASSESSMENT

How effectively does BC Hydro execute against this threat scenario?

Corporate IT

Identified Capabilities

- Integrated malware capabilities, including DNS security, email protection, malware sandboxing, and threat intelligence (provided by Cisco IronPort, AMP, and ThreatGrid)
- BC Hydro blocks all personal email services, such as Gmail, Hotmail, etc.
- A cyber security training and awareness program is implemented across BC Hydro covering cyber security policies and common threats
- Regular phishing simulations are performed for all BC Hydro employees, and a phishing reporting capability has been deployed
- Multi-factor authentication is deployed for Office 365 and remote access VPN
- Cisco Umbrella is deployed for DNS filtering and monitoring.

Observations for Immediate Action

- None.

Observations to Improve Control Environment

- Lack of 24/7 dedicated security monitoring and response capability for email related threat events
- Lack of network segmentation on corporate network could allow for lateral movement and / privileged escalation
- Limited of automation and orchestration for malicious email containment and remediation.

Additional Observations for Consideration

- None.

Residual Risk Summary

A number of common cyber security capabilities have been implemented to reduce the likelihood and impact of email-based threats such as phishing and business email compromise. There are however some opportunities for improvement which would help to further limit the potential impact of an email-based threat in the IT environment, enhancing detection and response capabilities. The assessed residual risk rating for Corporate IT is ***LOW.***

MRS OT

Identified Capabilities

- *All controls in place to mitigate phishing on corporate email apply to devices that may be used to access MRS OT*
- Corporate computers are – by policy - not used to physically connect to the OT network; hardened green laptops are used
- NERC CIP training is required to share or view confidential information
- MRS OT network is segregated from the corporate network
- Access is via VDI through the INTERMEDIATE zone and requires MFA.

Observations for Immediate Action

- None.

Observations to Improve Control Environment

- N/A

Additional Observations for Consideration

- None.

Residual Risk Summary

As most email-based threats are expected to originate in Corporate IT (and be subject to the capabilities described above), the likelihood of an email-based threat having a material impact on MRS OT is considered to be low. The assessed residual risk rating for MRS OT is ***LOW.***

T.05 BUSINESS EMAIL COMPROMISE

NON-MRS OT

Identified Capabilities

- *All controls in place to mitigate phishing on corporate email apply.*
- Corporate computers are – by policy - not used to physically connect to the OT network; hardened green laptops are used
- The non-MRS OT network is segregated from the corporate network (with the exception of certain supporting systems described in the scope section).
- Access to some non-MRS OT externally routable networks, must be done through a secure jump host (i.e. NERC INTERMEDIATE) which uses non-corporate dedicated authentication mechanisms.

Observations for Immediate Action

- None.

Observations to Improve Control Environment

- No broad use of jump hosts to access externally routable connected sites

Additional Observations for Consideration

- None.

Residual Risk Summary

*As most email-based threats are expected to originate in Corporate IT (and be subject to the capabilities described above), the likelihood of an email-based threat having a material impact on NON-MRS OT is considered to be low. The assessed residual risk rating for NON-MRS OT is **LOW.***

✳ RECOMMENDATIONS

For additional information refer to Recommendations section

Note: Definitions of the Value, Complexity and Priority ratings is contained within the Recommendations section of this report.

Reference No.	Recommendation title	Environment	Value	Complexity	Priority
REC-CORP-01	Expand logs to SIEM	Corp IT	HIGH	HIGH	HIGH
REC-GEN-04	Expand SOC resourcing	All	HIGH	HIGH	HIGH
REC-CORP-06	Expand network security towards zero trust	Corp IT	HIGH	HIGH	HIGH
REC-GEN-05	Consolidate SIEM	All	HIGH	HIGH	MEDIUM

T.06 EXTERNAL NETWORK SERVICE COMPROMISE

	Relative Risk Assessment			
Environment	Inherent Likelihood	Inherent Impact	Inherent Risk	Current Residual Risk
Corporate IT	HIGH	HIGH	HIGH	MODERATE
MRS OT	MODERATE	HIGH	HIGH	LOW
Non-MRS OT	HIGH	LOW	MODERATE	MODERATE

✳ SUMMARY OBSERVATION

What does this mean for BC Hydro?

BC Hydro has implemented several capabilities that address threats arising from increased network exposure, including perimeter controls (firewalls, intrusion prevention, web application firewalls, etc.), internal network segmentation between IT and OT networks, patching and vulnerability management, and strong authentication for services accessible from the internet (i.e. multi-factor authentication).

There are several opportunities for improvement across Corporate IT, MRS OT, and Non-MRS OT which should be considered to further reduce the risks associated with network exposure, including strengthening internal and external monitoring and detection capabilities, strengthening asset identification, monitoring, and vulnerability identification in OT networks, and increasing penetration testing and red teaming coverage.

✳ GENERAL DESCRIPTION

What is this threat scenario?

External network service compromises arise from the growing number of devices connected to a network at any given time. The growing number of connected devices makes managing and securing those exposed points challenging. Attacks on exposed servers were the third most common attack type in 2020, with attackers exploiting stolen credentials and known vulnerabilities to gain access[19]. According to the FBI[20], major vulnerabilities in products such as Citrix NetScaler, Pulse Secure Connect VPN, Fortinet VPN, Apache, Microsoft Windows Server, and Microsoft Exchange have been amongst the most exploited by cyber-criminals in the past year, often resulting in unauthorized access, the ability to execute unauthorized code, and disclosure of sensitive information such as credentials.

The global pandemic has led to a rapid increase in remote work, significantly increasing the attack surface. Before COVID-19, data, endpoints, and applications were largely contained and controlled within defined network boundaries, protected by perimeter controls like firewalls. The COVID-19 "work from home" shift has driven these important assets away from controlled spaces and into homes and public locations, increasing the reliance on remote working technologies like VPN, cloud, and remote desktop. With phishing and malware running rampant, work devices being used for personal activity (and vice versa), and work systems and data being accessed from unprotected networks, the attack surface has undoubtedly increased.

Lastly, OT/ICS/SCADA systems were not predominantly designed with access to the internet in mind, so in many cases lack the required cyber security capabilities. Recent advances mean that many of these systems can be monitored and controlled remotely, and the increasing use of industrial internet of things (IIoT) devices and cloud services in industrial systems has increased the attack surface. Threat actors are conducting continuous scanning activity to locate and exploit poorly configured, networked devices, which could lead to unauthorized access to control systems and the broader technology environment.

Environment-Specific Scenarios	
IT	*Through continuous scanning, a threat actor identifies a vulnerable server connected to the internet, exploits the known vulnerability, pivots from the DMZ to the internal network, and executes persistent malware on an internal BC Hydro server.*
MRS OT	*A threat actor identifies vulnerable industrial internet of things (IIoT) devices that are accessible from the internet, exploits the known vulnerability, and executes malware on the devices, adding them to an IIoT botnet.*
Non-MRS OT	*A threat actor identifies a network exposed device which is used to connect to corporate networks to support equipment condition monitoring, exploits a known vulnerability, and executes malware on the devices.*

✳ KEY VECTORS

How could this threat scenario materialize?

Automated scanning	Vulnerable software	Credential theft
Human error	Exposed services	Brute force

✳ EXPECTED CAPABILITIES

What is required to protect against this threat scenario?

Access Control	Maintenance	Info. Protection Processes & Procedures
	Security Continuous Monitoring	

[19] IBM Security, 2021. X-Force Threat Intelligence Index.

[20] hxxps://us-cert.cisa.gov/ncas/alerts/aa21-209a

T.06 EXTERNAL NETWORK SERVICE COMPROMISE

✳ **CAPABILITY ASSESSMENT** *How effectively does BC Hydro execute against this threat scenario?*

Corporate IT

Identified Capabilities

- Ongoing third-party passive scanning using BitSight platform to provides insights into third party external cyber risk posture
- Shodan subscription provides monitoring of exposed services and BCH address space
- Vulnerability management program provides ongoing scanning of environment, individual projects undergo security reviews prior to release
- IPAM is in place providing visibility into IP space
- Perimeter security controls, ForcePoint WebSense for outbound proxy and filtering for blocked websites
- External authentication of BC Hydro users requires multi-factor authentication
- Intrusion Prevention System (IPS) on perimeter and between PowerEx and PowerTech
- TELUS provides DDoS attack protection services
- Authentication into the network is via BC Hydro device certificate and registry key, and VPN with MFA
- ForcePoint WebSense for outbound proxy and URL filtering prevents access and provides reporting on known command and control or data upload location
- MyHydro application is protected by F5 Web Application Firewall (WAF)
- Patching on windows systems is executed effectively
- Threat intelligence reports provided through Mandiant relationship, as well as through CCCS, e-ISAC, vendors, etc.
- Mandiant conducts twice weekly active threat hunting as part of EDR services.

Observations for Immediate Action

- None.

Observations to Improve Control Environment

- Existence of legacy systems that have reached end-of-life and are unable to be patched
- Patching processes for certain systems do not follow a regular frequency
- No dedicated real time threat intelligence or Dark Web monitoring, e.g. credential leaks, initial access brokers
- Network is not segmented, allowing internal workstations and servers to connect freely
- No penetration testing (penetration testing strategy is developed and to be implemented FY22) to identify vulnerabilities in systems and processes
- No network anomaly detection capabilities
- Instances of Cisco NetFlow are in place, but logs are not analyzed.

Additional Observations for Consideration

- No TLS inspection is performed.

Summary

While BC Hydro applies perimeter prevention controls, the size of BC Hydro's networked device ecosystem is expansive and requires further procedural and detective controls to be applied. BC Hydro should implement mature processes such as penetration testing, Dark Web monitoring, and network anomaly detection, some of which is identified on upcoming cyber security roadmaps. The residual risk rating is assessed as MODERATE.

T.06 EXTERNAL NETWORK SERVICE COMPROMISE

MRS OT

Identified Capabilities

- Intrusion Detection Systems (IDS) are in place at network boundaries
- Dial up connections are protected through pin codes
- Cisco firewall log data is recorded, with a data collector on the generation network and a data conserver on the corporate network
- Active vulnerability assessments are performed monthly
- Patching is assessed monthly and deployed as required
- Configuration monitoring is done through agents, and tracked in SigmaFlow
- Environment segmentation from other networks is achieved through firewalls
- Connections into the OT environment are restricted (including the use of a virtual desktop environment for access from outside the OT network)

Observations for Immediate Action

- None.

Observations to Improve Control Environment

- No restriction of (or list of approved) dialup connections
- No penetration testing (penetration testing strategy is developed and to be implemented FY22) to identify vulnerabilities in systems and processes
- Dialup connections are not logged.

Additional Observations for Consideration

- None.

Summary

BC Hydro is required to regularly monitor configuration of MRS OT systems, including exposed networking configuration, and document and log required changes. MRS OT systems are well positioned to identify and mitigate against vulnerabilities or improperly exposed interfaces. The residual risk rating is LOW.

NON-MRS OT

Identified Capabilities

- Dialup connections are protected through pin codes
- Serial firewalls block network admin commands
- McAfee ePolicy Orchestrator (ePO) is in place, to enable consistent security posture management of endpoints.

Observations for Immediate Action

- None.

Observations to Improve Control Environment

- Dialup connections are not logged
- Inadequate firewall governance processes, rulesets do not have change management nor are subject to ruleset reviews
- IPSEC VPN connections provide direct access to the network without the use of a jump host
- Asset and firmware management capabilities are not broadly performed (there is an initiative underway to formalize this)
- No restriction of dialup connections
- Dial up connections have duplicated pin codes across sites
- No vulnerability scanning or penetration testing (strategy is developed and to be implemented FY22) to identify vulnerabilities
- Patching is done ad hoc and infrequently.

Additional Observations for Consideration

- None.

Summary

Non-MRS processes do not apply expected controls to network exposure threats. However, the non-MRS attack surface limits the exposure to this threat. Without proper controls in place the likelihood of this threat is increased, and while the attack surface may be small, threat actors can impact exposed OT networks. The residual risk rating is assessed as MODERATE.

T.06 EXTERNAL NETWORK SERVICE COMPROMISE

✳ RECOMMENDATIONS

For additional information refer to Recommendations section

Note: Definitions of the Value, Complexity and Priority ratings is contained within the Recommendations section of this report.

Reference No.	Recommendation title	Environment	Value	Complexity	Priority
REC-CORP-01	Expand logs to SIEM	Corp IT	HIGH	HIGH	HIGH
REC-CORP-04	Continue patching program expansion	Corp IT	HIGH	MEDIUM	HIGH
REC-CORP-06	Expand network security toward zero trust	Corp IT	HIGH	HIGH	HIGH
REC-CORP-07	Continue TLS inspection	Corp IT	MEDIUM	HIGH	HIGH
REC-CORP-09	Execute penetration testing strategy	Corp IT	HIGH	HIGH	MEDIUM
REC-CORP-10	Expand threat intelligence	Corp IT	HIGH	LOW	MEDIUM
REC-REG-05	Restrict authorized connections	MRS OT	LOW	MEDIUM	MEDIUM
REC-NONREG-07	Expand use of jump hosts	Non-MRS OT	MEDIUM	MEDIUM	MEDIUM
REC-NONREG-08	Implement process for reviewing firewalls	Non-MRS OT	LOW	LOW	LOW

RECOMMENDATIONS

The recommendations below take into consideration the relative impact the recommended control improvements would have on the threat scenario and related risk, as well as the complexity related to achieving this risk reduction. In addition, a guideline for relative priority has been provided. Priority does not directly link to reduction of highest residual risk, but rather assigns a relative priority based upon technical and resource feasibility, order of implementation and upon risk reduction value of the recommendation to the organization. These priorities will require further analysis by BC Hydro, which is anticipated to be completed as part of the Directive 9 deliverable. The following series of legends provides a description of how each recommendation has been assessed. In addition, each recommendation is assigned an indication as to whether BC Hydro is: currently in the process of actioning the recommended activity with an in-flight initiative, currently planning for the implementation of the recommendation, or currently considering how and when to implement the recommendation.

Value Legend

Value Ranking	Description
HIGH	Initiatives which provide substantial risk likelihood or impact reduction.
MEDIUM	Initiatives which provide additional risk likelihood or impact reduction, typically augmentation or additional to controls already in place.
LOW	Initiatives which provide marginal risk likelihood or impact reduction, typically addition of mature controls.

Complexity Legend

Complexity Ranking	Description
HIGH	Initiatives which will be considerably challenging to implement due to resourcing, duration, technical expertise, and/or cultural adaptation requirements.
MEDIUM	Initiatives which could undergo challenges during implementation due to resourcing, duration, technical expertise, and/or cultural adaptation requirements.
LOW	Initiatives which should not be challenging due to resourcing, duration, technical expertise, and/or cultural adaptation requirements.

Priority Legend

Priority Ranking	Description
HIGH	Recommendation which addresses a higher risk item, or which is a foundational recommendation required to be in place due to dependencies with follow-on recommendations. These recommendations should receive higher relative prioritization when conducting follow up consideration and planning as part of Directive 9.
MEDIUM	Recommendation which addresses a less risky item and/or is dependent on a foundational implementation or certain item to be in place. Initiatives which should receive medium relative prioritization when conducting follow up consideration and planning as part of Directive 9.
LOW	Recommendation which addresses an even lower risk item and can be addressed after completion of HIGH and MEDIUM recommendations or has critical dependency requirements with HIGH and/or MEDIUM recommendations. Initiatives which should receive lowest relative prioritization when conducting follow up consideration and planning as part of Directive 9.

Management's Indicated Status

Priority Ranking	Description
In-flight	BC Hydro management's assertion that the recommended initiative is currently being actioned.
Planned	BC Hydro management's assertion that the recommended initiative has not yet commenced but is identified on a cyber security roadmap and will continue to be actioned, but the timing and sequencing may be adjusted in consideration of the Report.
Under consideration	BC Hydro management's assertion that the recommended initiative will require further planning by BC Hydro to determine how and when to implement.

Enterprise wide

Recommendation ID	Recommendation description	Applicable Threat Scenario	Value	Complexity	Priority	Management's Indicated Status
REC-GEN-01	**Implement governance model**: Review, augment, and implement a formal governance structure with assigned, approved, and widely understood accountabilities and authorities that incorporates and harmonizes capability delivery across IT, OT, regulated, and unregulated environments.	All	HIGH	MEDIUM	HIGH	Planned
REC-GEN-02	**Expand internal cyber reporting**: Augment existing executive cyber risk reporting process to provide granular insights into ongoing cyber risk posture and active cyber risk treatment initiatives.	All	HIGH	LOW	HIGH	Planned
REC-GEN-03	**Continue asset management formalization:** Continue implementing asset management solutions (i.e. ServiceNow) and work towards harmonization of process and toolset across environments (where not restricted due to NERC CIP confidentiality requirements - MRS OT asset management may be better served by a dedicated OT asset database complying with NERC CIP requirements).	T.04	HIGH	HIGH	HIGH	Planned
REC-GEN-04	**Expand SOC resourcing**: Expand SOC resources to accommodate 24x7x365 monitoring and response model, or consider augmentation with outsourcing (*related to recommendation item REC-GEN-02).*	T.01, T.05	HIGH	HIGH	HIGH	Under Consideration
REC-GEN-05	**Consolidate SIEM**: Consider consolidation of SIEM infrastructure, resourcing, and operations to a single enterprise program.	T.01, T.05	HIGH	HIGH	MEDIUM	Planned
REC-GEN-06	**Expand and consolidate PAM**: Consider consolidation of PAM program across BC Hydro environments (i.e. corporate IT and OT) with vaulting solution segmentation in critical environments (MRS OT).	T.01, T.02, T.04	HIGH	HIGH	MEDIUM	Under Consideration
REC-GEN-07	**Expand third-party monitoring**: Implement ongoing third-party reporting of cyber security programs and posture in alignment with existing third-party cyber security requirements.	T.03	MEDIUM	MEDIUM	MEDIUM	In Flight
REC-GEN-08	**Expand threat hunting**: Augment and expand existing threat hunting capability to deliver broader enterprise capability using threat-driven approaches to search for exposure to threat-relevant TTPs and indicators of compromise (IOCs).	T.02, T.03	HIGH	HIGH	MEDIUM	Under Consideration
REC-GEN-09	**Implement network anomaly analysis**: Ensure expansion of Netflow log collection from network devices from all environments, and implement NetFlow analysis capability, to perform in-depth monitoring and understanding of network traffic data.	T.02	MEDIUM	LOW	MEDIUM	Under Consideration
REC-GEN-10	**Develop dataflow mappings**: Develop data flow mappings and identify control points / gaps, prioritizing critical information assets. Consider implementation of automated dataflow mapping tools to facilitate initial exercise and sustainability of dataflow mappings.	T.04	HIGH	HIGH	LOW	Under Consideration

Corporate IT

Recommendation ID	Recommendation description	Applicable Threat Scenario	Value	Complexity	Priority	Management's Indicated Status
REC-CORP-01	**Expand logs to SIEM**: Continue to expand log feeds integrated into Splunk SIEM environment.	T.04, T.05, T.06	HIGH	HIGH	HIGH	In Flight
REC-CORP-02	**Continue securing backups**: Complete the project to implement technical controls to secure backups and backup systems, including segmentation and encryption.	T.01	HIGH	HIGH	HIGH	In Flight
REC-CORP-03	**Continue vulnerability management expansion**: Continue to expand scope and rigor of vulnerability management program; continue Tenable implementation.	T.01	HIGH	MEDIUM	HIGH	In Flight
REC-CORP-04	**Continue patching program expansion**: Update existing patching program to include all corporate servers, workstations, and systems, extending beyond O/S and Office patching to include all applications, databases, middleware, etc. This will include staged upgrading or retirement of legacy end-of-life technologies.	T.06	HIGH	MEDIUM	HIGH	In Flight
REC-CORP-05	**Continue AD hardening**: Continue AD hardening initiatives identified in Mandiant Ransomware Assessment.	T.01	HIGH	MEDIUM	HIGH	In Flight
REC-CORP-06	**Expand network security towards zero trust**: Continue software defined network architecture initiative to implement more robust corporate network segmentation; consider designs which would position the organization for future implementation of zero trust architectures .	T.01, T.02, T.04, T.05, T.06	HIGH	HIGH	HIGH	In Flight
REC-CORP-07	**Continue TLS inspection rollout**: Continue to implement capability to perform TLS inspection, to enable the decryption and inspection of encrypted network traffic.	T.04, T.06	MEDIUM	HIGH	HIGH	In Flight
REC-CORP-08	**Complete CyberArk implementation**: Complete PAM improvements project, including formalization of PAM processes, and implementation of CyberArk solution (*related to recommendation REC-GEN-06).*	T.02	HIGH	HIGH	MEDIUM	Planned
REC-CORP-09	**Execute penetration testing strategy**: Implement penetration testing program per defined strategy.	T.02, T.06	HIGH	HIGH	MEDIUM	Planned
REC-CORP-10	**Expand threat intelligence**: Expand threat intelligence services to include Dark Web monitoring; searching for Dark Web matches of BC Hydro credential leaks, initial access brokers.	T.04, T.06	HIGH	LOW	MEDIUM	Under Consideration
REC-CORP-11	**Implement enterprise red teaming**: Implement enterprise red/purple teaming program, to emulate threat actors approaches to multistep, cross-environment attack execution.	T.01	HIGH	LOW	MEDIUM	Planned
REC-CORP-12	**Complete addition of CSIRP playbooks**: Complete build out of detailed cyber incident response playbooks and implementation of related technical capabilities to quarantine systems.	T.01, T.04	HIGH	MEDIUM	MEDIUM	In Flight
REC-CORP-13	**Implement deceptive detection tactics**: Implementation of deceptive threat detection techniques and honey pots such as decoy device, files, systems, accounts, etc.	T.02	HIGH	LOW	LOW	Under Consideration
REC-CORP-14	**Continue to enhance user anomaly detection**: Complete implementation of Splunk Enterprise Security and enable UEBA and advanced analytics capability.	T.04	HIGH	MEDIUM	LOW	Planned

Recommendation ID	Recommendation description	Applicable Threat Scenario	Value	Complexity	Priority	Management's Indicated Status
REC-CORP-15	**Implement data leak prevention controls**: Implement DLP capabilities and controls, which can detect and prevent unauthorized exfiltration or destruction of sensitive data.	T.02, T.04	MEDIUM	HIGH	LOW	Planned

MRS OT

Recommendation ID	Recommendation description	Applicable Threat Scenario	Value	Complexity	Priority	Management's Indicated Status
REC-REG-01	**Expand logs to SIEM**: Expand ingestion of log information from MRS OT systems and network devices (i.e. NetFlow logs) in alignment with BC Hydro's log management standard, where technically feasible.	T.04	HIGH	HIGH	HIGH	Planned
REC-REG-02	**Implement ICS specialized detection**: Implement dedicated ICS threat identification platform (e.g. Dragos), to provide robust threat detection, visualization, and response capabilities.	T.02, T.03	HIGH	MEDIUM	HIGH	Under Consideration
REC-REG-03	**Implement consolidated PAM**: Consider integration with consolidated PAM program, and implementation of dedicated OT environment PAM solution instance (*related to recommendation REC-GEN-06).*	T.01	HIGH	HIGH	MEDIUM	Under Consideration
REC-REG-04	**Expand detection abilities**: Expansion of use cases within MRS environment beyond compliance required use case set (*related to recommendation REC-GEN-05).*	T.04	HIGH	MEDIUM	MEDIUM	Under Consideration
REC-REG-05	**Restrict authorized connections**: Implement restriction of remote access (dialup) connections to specified numbers.	T.06	LOW	MEDIUM	MEDIUM	Under Consideration
REC-REG-06	**Expand network security towards zero trust**: Consider network architecture security initiatives (related to those in flight in corporate environment) which would position the organization for future implementation of zero trust architectures.	T.01	MEDIUM	HIGH	LOW	Under Consideration

Non-MRS OT

Recommendation ID	Recommendation description	Applicable Threat Scenario	Value	Complexity	Priority	Management's Indicated Status
REC-NONREG-01	**Implement asset management planning:** Asset management capabilities (i.e. through a ServiceNow instance) are being planned for non-MRS OT systems to align with MRS processes.	T.04	HIGH	MEDIUM	HIGH	Under Consideration
REC-NONREG-02	**Implement configuration monitoring**: Document and define hardened configuration standards for non-MRS systems, and implement processes and tools for ongoing configuration monitoring to detect unauthorized changes to systems.	T.01, T.03	HIGH	HIGH	HIGH	Under Consideration
REC-NONREG-03	**Implement patch deployment cadence**: Implement formal patch release cycles including test and deployment windows based on patch and asset criticality in alignment with BC Hydro's risk appetite.	T.02, T.03	HIGH	MEDIUM	HIGH	Under Consideration

REC-NONREG-04	**Implement the planned vulnerability scanning and penetration testing program**: Implement process for ongoing vulnerability scanning and penetration testing to identify and remediate system vulnerabilities.	T.01, T.03	HIGH	MEDIUM	HIGH	Planned
REC-NONREG-05	**Implement consolidated PAM**: Consider integration with consolidated PAM program, alignment to BC Hydro's access management/control policies and standards, and implementation of dedicated non-MRS OT environment PAM solution instance (*related to recommendation REC-GEN-06).*	T.01, T.02, T.04	HIGH	HIGH	MEDIUM	Under Consideration
REC-NONREG-06	**Adopt consolidated SIEM**: Consider adoption of enterprise SIEM program and expand resources to accommodate integrate log feeds to a SIEM environment where technically feasible and monitoring/response resources (*related to recommendation item REC-GEN-05).*	T.01, T.02, T.04	HIGH	HIGH	MEDIUM	Under Consideration
REC-NONREG-07	**Expand use of jump hosts**: Expand the use jump hosts for connections to provide access control layers to remote connected systems.	T.01, T.06	MEDIUM	MEDIUM	MEDIUM	Under Consideration
REC-NONREG-08	**Implement process for reviewing firewalls**: Conduct regular firewall ruleset reviews to review, identify, and remediate changes or drifts from hardened firewall security configurations (could leverage corporate processes).	T.06	LOW	LOW	LOW	Under Consideration
REC-NONREG-09	**Implement ICS specialized detection**: Implement dedicated ICS threat identification platform (e.g. Dragos) where feasible to provide robust threat detection, visualization, and response capabilities.	T.02	MEDIUM	MEDIUM	LOW	Under Consideration

APPENDIX A: LIST OF DOCUMENTS REVIEWED

Document Title	File Name
3rd Party Cybersecurity Requirements Attestation	3rd party Cybersecurity Requirements Attestation.xlsx
Acceptable Use Policy	2A.020 Acceptable Use Policy.pdf
Access Control Policy	7A.206 Access Control Policy.pdf
Application Information Access Control Standard	7D.220 Application Information Access Control Standa.pdf
Approved Products for Hardware, Software	3D.001 Approved Products For Hardware, Software.pdf
Asset Management Policy	7A.202 Asset Management Policy.pdf
Asset Strategy and Plan Template	6G.100 Asset Strategy and Plan Template.doc
BAU Hardware Acquisition Standard	3D.012 BAU Hardware Acquisition Standard.pdf
BC Hydro Archives Standard	6D.203 BC Hydro Archives Standard.pdf
BC Hydro CIP Mitigation Actions Tracker	BCH Mitigation Actions Aug_24_2021_{13.08}.xlsx
BC Hydro Cloud Census June 2021	Copy of BCH Cloud Census_Jun2021.xlsx
BC Hydro Corporate Cyber Security Risk Register	BCH Corp CS Risk Register (xRM)_Jul 2021.xlsx
BC Hydro Cyber Threat Actor Profiles July 2021	Cyber Threat Actor Profiles_Jul2021.docx
BC Hydro Cyber Threat Profile	BC Hydro Cyber Threat Profile_Jul2021.docx
BC Hydro Cybersecurity Incident Response Plan	BCH cybersecurity-incident-response-plan.pdf
BC Hydro Downtown Network Diagram	downtown.pdf
BC Hydro Enterprise Risk Resource Guide	BC Hydro Enterprise Risk Resource Guide.pdf
BC Hydro Five Year Enterprise Strategy	BC-Hydro-five-year-strategy.pdf
BC Hydro High-Level WAN Network Diagram	BCH High Level WAN.v1.2.pdf
BC Hydro IT Application List	BCH IT Application List.xlsx
BC Hydro IT BIA 2017 and ongoing ITSCIA Tracker	BCH IT BIA 2017 and ongoing ITSCIA - CONSOLIDATED RESULTS.xlsx
BC Hydro IT Infrastructure List	BCH IT Infrastructure List.xlsx
BC Hydro OT Cybersecurity Risk Assessment by Siemens	BC Hydro OT Cybersecurity Risk Assessment by Siemens (final version).pdf
BC Hydro Policies and Standards User Guide	BCH Policies and Standards User Guide.pdf
BC Hydro Privacy Impact Assessment Template	BCH_PIA_Template.docx
BC Hydro Privacy Policy	BCH Privacy Policy (from intranet site).docx
BC Hydro Risk Management Process Summary	BCH risk-management-process-in-a-page.pdf
BC Hydro Technology Division Strategy and Five-Year Plan 2020	Technology Strategy and 5-Year Plan - Sept 2020 - FINAL.pdf
BC Hydro Technology Organization Chart	BCH Technology Organization Chart.pdf
BC Hydro's Industrial Control Systems (ICS) Cybersecurity Risk Mitigation Plan (OAG Response)	ICS Cybersecurity Remediation Plan 2021.pdf
BC Hydro's Remediation Response to OAG Audit 2019	OAG CS Action Plan and Progress Assessment BC Hydro Feb 2021.pdf
Business Requirements for Access Control Standard	7D.215 Business Requirements For Access Control Standard.pdf
C2M2 Report - Sept 2019	C2M2 REPORT-09_25_2019.docx
C3 PLCY CORP CYBER SECURITY POLICY	C3 PLCY CORP Cyber Security Policy.pdf

Document Title	File Name
Change Management SIAM Process Diagram	SIAM_BCH Change Management Level 2 and Level 3 Process - 3 February 2020.vsd
Communications Operations Management Policy	7A.205 Communications Operations Management Policy.pdf
Compliance with Security Policies, Standards	7D.231 Compliance With Security Policies, Standards.pdf
Continuity Plan - Generation System Operations	Continuity Plan - Generation System Operations.pdf
Continuity Plan - Technology (IT)	Continuity Plan - Technology (IT).pdf
Continuity Plan - Transmission and Distribution System Operations	Continuity Plan - Transmission and Distribution System Operations.pdf
Controlling the Threat of Malicious Codes	3B.030 Controlling the Threat of Malicious Codes.pdf
Corp Record Guidelines	6D.120 Corp Record Guidelines.docx
Correct Processing in Application Systems	7D.223 Correct Processing In Application Systems.pdf
Cryptographic Standard	7D.106 Cryptographic Standard.pdf
Cryptography and Key Management Policy	7A.211 Cryptography And Key Management Policy.pdf
Cyber Penetration Testing Strategy 2021	Cyber Pen Testing Strategy - 2021 Refresh.pptx
Cyber Security Risk Matrix	CS Risk matrix.xlsx
Cyber Security Strategy 2020	Cybersecurity Strategy 2020 (CFO endorsed).pptx
Cyber Security Three Year Plan 2020	Cybersecurity 3-Year Plan 2020 - FINAL - Oct 2020 - ET Version.pptx
Cyber Threat Level Weekly Report - April 4 2021	20210401- Cyber Threat Level Weekly Report - April 4 2021.docx
Cyber Threat Level Weekly Report - March 21 2021	20210319- Cyber Threat Level Weekly Report - March 21 2021.docx
Cybersecurity and Compliance Resource Plan	Cybersecurity Resource Plan - September 2020 - FINAL.pdf
Cybersecurity Configuration Standard	7D.238 Cybersecurity Configuration Standard.pdf
Data Backup and Recovery Guidelines	1D.040 Data Backup and Recovery Guidelines.pdf
Data Network Protocol Standards	2D.002 Data Network Protocol Standards.pdf
Detection and Response to Cybersecurity Threats on BC Hydro's Industrial Control Systems 2019 (Public Release of OAG Audit)	OABGC_Cybersecurity-ICS-BC-Hydro_RPT.pdf
Disaster Recovery Network Diagram Calgary Datacentre	Disaster Recovery 12_02_28.pdf
Disclosure Storage and Access	7A.102 Disclosure Storage and Access.pdf
Edmonds Network Diagram (1/2)	Edm Pods.pdf
Edmonds Network Diagram (2/2)	Edm Tower.pdf
E-Mail Practice, Virus Protection	6B.015 E-Mail Practice, Virus Protection.pdf
Employment Security Standard	7D.205 Employment Security Standard.pdf
Exchange of Information Standard	7D.213 Exchange Of Information Standard.pdf
External Party Security Standard	7D.202 External Party Security Standard.pdf
Fraser Valley Operations - SIO - Non-NERC Network Diagram	BCH FraservalleyOps-SIO_non NERC.vsd
Guidelines for Preventing Accidental	6B.042 Guidelines for Preventing Accidental.pdf
Hardware Refresh Standard	3D.013 Hardware Refresh Standard.pdf
Home Wireless LAN Security Installation	2G.100 Home Wireless LAN Security Installation.pdf
Home Wireless LAN Setup Guidelines	2D.020 Home Wireless LAN Setup Guidelines.pdf
Human Resources Security Policy	7A.203 Human Resources Security Policy.pdf

Document Title	File Name
Information Security Classification Policy	7A.200 Information Security Classification Policy.pdf
Information Security Compliance Policy	7A.210 Information Security Compliance Policy.pdf
Information Security Incident Management Policy	7A.208 Information Security Incident Managment Policy.pdf
Information Security Policy	7A.100 Information Security Policy.pdf
Information System Design Security Review	4B.032 Information System Design Security Review.pdf
Internal Audit Cyber Security Remediation Tracker	Internal Audit Cybersecurity.docx
Internal Organization Security Standard	7D.201 Internal Organization Security Standard.pdf
IS Acquisition Development and Maintenance Policy	7A.207 IS Acquisition Development And Maintenance Policy.pdf
IS Audit Considerations Standard	7D.232 IS Audit Considerations Standard.pdf
IS Governance Process Definition	7B.100 IS Governance Process Definitio.pdf
IT Inventory Update and Reporting	6B.050 IT Inventory Update and Reporting.pdf
IT Security Design Checklist	7G.100 IT Security Design Checklist.docx
IT Security Design Checklist Procedure	5B.060 IT Security Design Checklist Procedure.pdf
IT Service Continuity Management Plan Playbook	DR - ITSCM Playbook.pdf
IT Services Delivery Management Policy	6A.005 IT Services Delivery Management Policy.pdf
Java SE (JRE and JDK)	5D.102 Java SE (JRE And JDK).pdf
Lower Mainland Network Diagrams	lower mainland.pdf
Lower Mainland WiMax Network Diagrams	Lower Mainland WiMax.pdf
Manage IT Asset Portfolio Process	6B.115 Manage IT Asset Portfolio Process.pdf
Mandiant Ransomware Assessment 2021 - Strategic Report	M_BCHydro_RansomwareDefenseAssessment_StrategicReport_Draft_3.19.2021.docx
Mandiant Ransomware Assessment 2021 - Technical Report	M_BCHydro_RansomwareDefenseAssessment_TechnicalReport_Draft_3.19.2021.docx
Mobile Device Use Standard	7D.221 Mobile Device Use Standard.pdf
Nanaimo Network Diagrams	Nanaimo.pdf
Network Access Control Standard	7D.218 Network Access Control Standard.pdf
Network Host and Telecom Asset Naming	2D.210 Network Host And Telecom Asset Naming.pdf
Northern Interior Network Diagrams (1/2)	Northern Interior A-M.pdf
Northern Interior Network Diagrams (2/2)	Northern Interior N-Z.pdf
Northern Interior WiMax Network Diagrams	Northern Interior WiMax.pdf
OAG Audit Remediation Actions Tracker	BCH External OAG Audit 2019.xlsx
Office of the Auditor General ICS Cybersecurity Report 2019	ICS Cybersecurity Management Report.pdf
Operating System Access Control	7D.219 Operating System Access Control.pdf
Operational Procedures Responsibilities Stand	7D.207 Operational Procedures Responsibilities Stand.pdf
Organization of Information Security Policy	7A.201 Organization Of Information Security Policy.pdf
Packaged Application Customization	5D.100 Packaged Application Customization.pdf
Pre-Employment Security Standard	7D.204 Pre-Employment Security Standard.pdf
Prince George Network Diagrams	Prince George.pdf
Printer, Plotter, and MFD Standard	3D.020 Printer, Plotter, and MFD Standard.pdf
Privacy Impact Assessment Policy	6A.100 Privacy Impact Assessment Policy.pdf
Project Management Guidelines	6D.105 Project Management Guidelines.pdf

Document Title	File Name
Protection Against Malicious and Mobile Code	7D.210 Protection Against Malicious And Mobile Code.pdf
Records Management Policy	6A.120 Records Management Policy.pdf
Responsibility for Assets Standard	7D.203 Responsibility For Assets Standard.pdf
Security in Development Support Processes	7D.225 Security In Development Support Processes.pdf
Security Logging Standard	7D.102 Security Logging Standard.pdf
Security of System Files Standard	7D.224 Security Of System Files Standard.pdf
Security Requirements IS Standard	7D.222 Security Requirements IS Standard.pdf
Selecting, Developing, Or Changing	3A.011 Selecting, Developing, Or Changing.pdf
Server Product Standard	3D.010 Server Product Standard.pdf
Siemens Non-NERC ICS/OT Asset Register	OT ICS assets_2019 assessment.xls
Siemens Non-NERC ICS/OT Cyber Risk Assessment 2019	non NERC OT Cyber Risk Assessments Siemens.docx
Siemens Non-NERC ICS/OT Cyber Threat and Risk Matrix	OT Cybersecurity Threat Scenarios and Risk Matrix - Final Version – 2019102301.xlsm
Software Security Patching Standards	3D.004 Software Security Patching Standards.pdf
Southern Interior Network Diagram	southern interior.pdf
Southern Interior WiMax Network Diagram	Southern Interior WiMax.pdf
Surrey Network Diagram	Surrey.pdf
Technical Vulnerability Management Standard	7D.226 Technical Vulnerability Management Standard.pdf
Tetra Network Diagrams	Tetra.pdf
Third Party Data Access Request Process	6B.108 Third Party Data Access Request Process.pdf
Third Party Delivery Management Standard	7D.208 Third Party Delivery Management Standard.pdf
Unmanaged LAN Switch Standard	2D.230 Unmanaged LAN Switch Standard.pdf
User Access Management Standard	7D.216 User Access Management Standard.docx.pdf
User Responsibilities Standard	7D.217 User Responsibilities Standard.pdf
Vancouver Island Network Diagrams	Vancouver Island.pdf
Vancouver Island WiMax Network Diagrams	Vancouver Island WiMax.pdf
Vernon Network Diagrams	Vernon.pdf
Virtualize First Policy	3A.101 Virtualize First Policy.pdf
Vital Records	6D.202 Vital Records.pdf
VPN Security Requirements	6g.113 VPN Security Requirements.pdf
WAN Acceleration Standard	2D.460 WAN Acceleration Standard.pdf
WECC Compliance Audit July 7, 2021	2021 BCHA Non-Public Final Report_WECC.pdf
WiMax IP Address Map	WIMAX - MR IP Map R17 draft.pdf
Wireless LAN Standard	2D.200 Wireless LAN Standard.pdf

APPENDIX B: LIST OF STAKEHOLDERS INTERVIEWED

BC Hydro Stakeholder	Role
Adam French	Manager, Telecommunications Delivery & Operations
Alan McLeod	IT Cybersecurity Advisor, Splunk SIEM
Djordje Atanackovic	Engineering Division Manager, Real Time Systems
Edwin Christopher	Senior Engineer, Real Time Operations
Emanuele De Giorgi	Project Manager – Project Management Office (PMO)
Enisa Kojic	Engineering Team Lead - OT
Helen Whittaker	Director, Planning & Performance
Jason Farmer	IT Advisor, Network Operations
John Lee	Engineering Team Lead, Real Time Systems
Jose Clapauch	Project Engineer Specialist
Juergen Ostrinski	Senior Manager, Cyber Security Planning & Operations
Kip Morison	Chief Information Officer
Kyle Luciak	IT Architect Specialist, Enterprise Architecture (Infrastructure)
Manoj Saha	Information Protection Lead
Mark Christianson	Senior Manager, Governance Risk and Compliance
Moe Kia	IT Architect Specialist, Enterprise Architecture (Cybersecurity)
Peter Eijsberg	IT Project Manager, Telecom & P&C Department
Rob Antonishen	Director, Cyber Security & Compliance
Rob McLellan	IT Project Manager - Customer Service Delivery
Ryan Planinshek	Manager, Business Partner Services
Tom Griffith	Manager, Network Operations
William Leung	IT Enterprise Solution Lead - SAP Security
Yingzi Jan Zhang	IT Compliance & Risk Assessment Lead

Stakeholder names are listed in alphabetical order