ADDIS ABABA UNIVERSITY

ADDIS ABABA INSTITUTE OF TECHNOLOGY (AAiT)

SCHOOL OF INFORMATION TECHNOLOGY AND ENGINEERING

CYBERSECURITY INCIDENT MANAGEMENT FRAMEWORK FOR SMART GRID SYSTEMS IN ETHIOPIA

BY

GETINET ADMASSU

June 2024

ADDIS ABABA, ETHIOPIA

ADDIS ABABA UNIVERSITY

ADDIS ABABA INSTITUTE OF TECHNOLOGY (AAiT)

SCHOOL OF INFORMATION TECHNOLOGY AND ENGINEERING

A PROPOSAL SUBMITTED TO THE SCHOOL OF GRADUATE STUDIES OF ADDIS ABABA UNIVERSITY IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE CYBER SECURITY WITH A SPECIALIZATION IN CYBERSECURITY GOVERNANCE AND MANAGEMENT.

By: GETINET ADMASSU

ADVISOR: HENOCK MULUGETA (Ph.D.)

ADDIS ABABA UNIVERSITY

ADDIS ABABA INSTITUTE OF TECHNOLOGY (AAiT)

SCHOOL OF INFORMATION TECHNOLOGY AND ENGINEERING

CYBERSECURITY INCIDENT MANAGEMENT FRAMEWORK FOR SMART GRID SYSTEMS IN ETHIOPIA

By: GETINET ADMASSU

Name and Signature of Members of the School Graduating Committee (SGC)

HENOCK MULUGETA (Ph.D.)	_____	_____
Advisor	**Signature**	**Date**
ELEFELIOUS GETACHEW (PH.D.)	_____	_____
Examiner	**Signature**	**Date**
ABEBE DIRO (PH.D.)	_____	_____
Examiner	**Signature**	**Date**

Declaration

This thesis has not been accepted for any degree previously and is not presently submitted for any degree to any other university. I hereby declare that this thesis is the result of my research, except where otherwise indicated.

I conducted the research with the guidance and support of my research advisor. I acknowledge all the other sources by explicit citations, and a list of references is included.

Signature: _____

Getinet Admassu

Acknowledgment

Let me start by thanking Almighty God for the strength and blessings that have been my mainstay in life.

I would also like to take this opportunity to express my profound gratitude to my advisor, Dr. Henock Mulugeta, who was tireless in providing guidance and assistance throughout the process. You were kind and accommodating. Any time I called on you or went to your office, you willingly gave your hand to assist me. Thank you!

I want to express my deep gratitude to my family and friends, who supported me morally and inspired me. Their contribution was indispensable to my finishing my studies.

Abstract

Merging OT and IT into smart grid systems brought along new advantages. Smart grids will be able to use this amalgamation to manage energy generation and transmission with minimal loss of energy, a factor that results in high efficiency. Besides that, integrating IT and OT into the smart grid presents real-time infrastructure management monitoring. On the other hand, this digital change subjected smart grids to many cybersecurity threats. This will be achieved by developing and implementing stable cybersecurity incident management systems to secure key infrastructures. Based on evidence from existing literature and expert judgments, this paper enumerates the principal challenges power utilities face in managing cybersecurity incidents. Then, it outlines a comprehensive cybersecurity incident management framework. This framework will, hence, enable power utilities to take on an active role and deal with relevant powers regarding cybersecurity incidents. Also, the model ensures that cybersecurity, concerning all strategic, engineering, procurement, construction, and operational aspects and involving all parties and resources concerned, is put together systematically. The underlying design science qualitative approach facilitated the development of this framework. It organizes sophisticated threat detection techniques and counter-threat strategies and correlates with Risk Management, Threat Analysis, Security Controls, Operational Models, and Management. They also involve real-time network traffic and system log monitoring, anomaly detection algorithms, intrusion detection, and prevention systems. Power utilities will significantly improve the ability to effectively detect and respond to cybersecurity-related events. The following threat scenarios, including organized DDoS and ransomware attacks as a taxonomy against the various components of the proposed framework, show how these smart grid technologies mentioned above can be used to develop effective solutions in response to cyber security incidents. It is indeed a systematic framework; it gives good advice. The recommendations will target particular challenge areas within the electric power industry and underpin its cybersecurity posture, with a view that our critical energy infrastructure will be reliable and capable of being counted upon in grace. This research encourages sustainable development and social welfare by resilience in cybersecurity for smart grid systems.

Keywords: Cybersecurity, Incident Management framework, Smart Grid, Operational technologies (OT), Information Technology (IT), Threat Scenarios.

Table of Contents

List of Tables

List of Figures

List of Acronyms	
COBIT	Control Objectives for Information Technologies
DSO	Distribution system operator
ANISA	European Union Agency for Cybersecurity
IEC	International Electro-Technical Commission
INSA	Information Network Security Agency
IoT	Internet of thing
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
SCADA	Supervisory Control and Data Acquisition
OT	Operational Technology
IT	Information Technology

Chapter One

1. Introduction

1.1. Background Information

Modern society heavily relies on electricity supply; technological devices depend on electricity to run machinery, which is fundamental in the mechanism for the performance and propelling of an economy. Electricity can be produced by a power station from areas with further transportation via high-voltage lines from the power provider into a distribution system shared among homes, businesses, and industries. To achieve the goals of the smart grid, today's power industry needs to prepare for tomorrow, laden with new information technology (IT) and operational technology (OT) as pillar devices or controllers called industrial Internet of Things (IIoT). Now, remote controls and online communication are integrating with power grids like they never have before. The product of this integration is a smart grid. This advanced power network uses digital communications technology to monitor, control, and optimize generation and distribution. Smart grid technologies provide many benefits, such as excellent reliability and efficiency and increased incorporation of renewable energies, but their rise outpaces lower costs. On the other hand, these developments also mean a much larger number behind potential attackers and, therefore, an increased likelihood of computer attacks. Cyber-attacks are growing in intensity and frequency; smart grids have become the latest target [2]. As these cyberattacks become more sophisticated, a short interruption in service can create havoc throughout tens of thousands of public utilities and businesses and undermine the operations and reputations of critical infrastructure organizations.

The disruption will also have profound and unexpected consequences in many other sectors, including telecommunications and healthcare, with far-reaching adverse effects across political and economic systems. It may even threaten national security [3]. For example, it is estimated that prolonged power outages can severely impact a country's gross domestic product [4], and cyberattacks are becoming more common in the power sector [6]. The 2015 smart grid cyberattack [7] in Ukraine triggered concerns about the cybersecurity of the power systems that make up the electricity grid. The attack targeted a regional electricity supplier and caused a power outage for several hours, affecting about 225,000 customers. Cyberattacks and power outages have demonstrated that external, unauthorized entities can infiltrate and control power grids through Internet-connected systems [8]. Stadtwerke Bruck, an Austrian utility company,

experienced a security incident in its IT systems on March 4. The affected services were quickly restored, and the company was fully operational by March 11. The business data was reconstructed from a data backup, and an IT forensic investigation was conducted to determine the nature and progression of the security incident. There was no indication that any data had been removed from the company's systems at the time of notification. An initial preventive report was submitted to the relevant authorities for transparency.] The Electricity Transmission System Operator of the Republic of North Macedonia (MEPSO) was hit by a cyberattack. Still, it did not target the company's critical energy infrastructure, which remained secure and fully operational. MEPSO reported the incident to the relevant authorities and worked with cybersecurity experts to mitigate the effects of the attack and normalize its operations. The company's website was restored on March 11, and no ransom demand was made to unlock the hacked information systems. The Cactus ransomware attack targeted Schneider Electric, a French multinational energy company, on January 17. The attack was limited to the company's Sustainability Business division and resulted in corporate data theft. It disrupted part of Schneider Electric's Resource Advisor cloud platform. The company worked with cybersecurity firms to investigate the incident and restore operations within two days. Schneider Electric informed affected customers and reported that access to business platforms was restored on January 31.

Technology advances and the demand for energy efficiency have pushed Ethiopia's smart grid systems to be adopted in recent years. There have been no reported attacks yet on Ethiopia's smart grids; nonetheless, it's critical for this country to prioritize and strengthen its cybersecurity because the threat landscape is constantly changing globally, technology leaves potential weaknesses, and the consequences of a successful attack could be very serious. Learning from foreign experience and adopting a proactive attitude, power utilities in Ethiopia will be able to protect their critical energy infrastructure and regularly provide our citizens with a stable, uninterrupted electricity supply. One possible proactive measure to defend smart grids against attacks puts forward a comprehensive incident management framework that is proactive rather than reactive (despite never having been attacked before). It will have predefined strategies, principles, and steps for efficiently handling and limiting cybersecurity incidents. It should assign responsibility to relevant parties.

A practical incident management framework can keep the heads of power grid operations managers above water when there are abounding cyber threats, reduce downtime, and maintain the reliability and resilience of the power grid system. Such a framework is multifaceted. Firstly, a thorough risk assessment has to be done to study concrete vulnerabilities and threats to intelligent grid infrastructure in Ethiopia. In this paper, we have discussed the technical and human nature of the Smart Grid and what factors determine its vulnerability. By understanding the peculiar risks and challenges that the Ethiopian power grid faces, leaders and operators can adapt the incident management framework to meet those dangers. Meanwhile, comprehensive training and publicity should be carried out among all staff members to operate and maintain the Smart Grid. These include the technical staff, management people at the executive levels, and at least end-users of every aspect of technology. These approaches are set to assist the response rate on cyber-fraud incidents that, through such avenues, ensure this response meets up well in training, enlists public interest, and moves alongside the scientific strides taken.

Besides, the incident management framework should establish precise communication techniques and channels within the power grid operator's organization and with external stakeholders like government agencies, law enforcement agencies, and the wider public. Good communication is a question of confidence, coordinating the response, and ensuring accurate information is rapidly passed on to the public. Therefore, a cyber incident management framework must incorporate systematic evaluation, testing, and continuous improvement. This will keep it awake and effective in front of ever-changing cyber threats and changes in capabilities. Hence, the better the framework, the better the position of power companies in Ethiopia to move ahead with the times and protect against cyber-attacks on the vital power infrastructure. In light of this, with a mature and in-depth incident handling mechanism chain, the power utilities from Ethiopia can take actual moves forward in protecting their smart grid system, ensuring power supply reliability even after all-natural disasters have occurred. Therefore, the active and timely interventions by utilities in Ethiopia within the framework of committed investment in cybersecurity measures have to come forward with engagements with regional and global partners to ensure utility companies take proactive approaches toward finding their way around treacherous waters in a security landscape that is increasingly challenging given its evolving character, toward providing safe, secure, and sustainable energy.

1.2. Motivation of the Study

This research paper is motivated by cybersecurity incident management in smart grid systems. Over the years, more attention has been drawn to cyber threats against such large infrastructure systems, especially toward smart grids. There is a high tendency for most utilities to shift towards smart grids; from that aspect alone, huge and changing alterations in fit-out, market regulations, and new integrations of sources have been achieved or will be undertaken in the coming times. This accounts for a resultant smart grid market size of US$36.9 billion in 2021 and is likely to inflate to US$55.9 billion by 2026, thereby bearing out the rapid adoption of these advanced technologies worldwide. Besides, smart grid technology offers a number of benefits, including more efficient energy use, reliability, convenience, and integration of variable renewable generation sources like solar and wind. Smart grids can manage the flow of electricity according to demand with advanced sensors, communication networks, and automated control systems; they can detect and respond to any break in the electric power system much faster than previous systems could, and they enable seamless integration of distributed sources. These are reasons why power utilities have lately been embracing smart grid systems in upgrading infrastructure and coping with changing energy needs. However, while introducing information and communication technologies in smart grid systems, new cyber security risks and vulnerabilities appear because malicious actors might get unauthorized access to smart grid control systems, disturb normal operations, and cause significant economic consequences due to wide blackouts.

This is an ever-increasing problem for power utilities, particularly in developing areas such as Africa, where reliable electricity delivery is crucial to economic development and corporate and domestic well-being. Power utilities in Ethiopia are implementing smart grid solutions that will enable better monitoring and controlling of the National Grid. Whereas such efforts tend to create more robustness and efficiency in the general power system, these efforts have also exposed the utilities to possible cyber-attacks. Critical smart grid facilities such as the national load dispatch center, sub-stations, or power plants could sustain local power outages with corresponding economic losses if successfully attacked. It would directly affect businesses, hospitals, schools, and homes in the affected area for days or weeks. The financial impact of such an attack could be crippling since reliable electricity is a cornerstone of economic growth and living standards everywhere. Therefore, this research focuses on developing a comprehensive cybersecurity incident management framework tailored to meet the particular

needs and challenges of the smart power grid. The proposed framework will go a long way in hardening the defenses of power companies and grid operators against cyber incidents, targeting intelligent power grids' vulnerabilities and risks to save customers money. It will also ensure that electricity keeps flowing reliably without being shot down.

1.3. Statement of the Problem

The large-scale application of the Internet of Things (IoT) technology has promoted revolutionary changes in the power industry and is conducive to building smart, distributed, and integrated power systems. The technological transformation has addressed many issues, especially those revolving around enhancing energy efficiency, grid resilience, and incorporating renewable energy sources. Yet, this transformation has also brought new vulnerabilities that can damage the whole power ecosystem. Due to the interdependency and digitalization of modern power grids, cyber threats can potentially have a more significant impact as emerging protocols and workflows introduce new vulnerabilities that malicious actors can exploit. Experts have shown that terrorism on a national scale through cyber-attacks will cause a massive failure to our grids, resulting in long-term power outages that affect lifeline services like health care, food supply, and public safety [2]. Such a scenario can become life-threatening and is directly linked to the safety and health of citizens, with cascading consequences on critical infrastructure and the functioning of society. The 2015 attack on the Ukrainian power grid [7], which resulted in outages impacting hundreds of thousands of customers, was a serious wake-up call for the power sector. This incident highlighted the living, breathing consequences of cyber threats and the urgent need for a comprehensive cybersecurity incident management framework to safeguard these critical systems. The growing adoption of smart grid and digitalization in Ethiopia has raised concerns about the potential exploits of cybercriminals, which could affect millions of people if any vulnerability is exploited. Smart grid systems are increasingly deployed, enabling seamless incorporation of advanced communication, control, and automation technologies to improve energy efficiency and grid reliability and better integrate renewable energy sources. However, these intricate systems also pose new attack surfaces that malicious actors can exploit. The growing integration of IoT devices and distributed energy resources into the power grid has also widened the attack surface, making it even more challenging to secure the entire system. Cybercriminals might see an opportunity to breach the grid by exploiting weaknesses in connected devices, control systems, or communication protocols, which could lead to massive

disruptions, physical destruction, and even loss of life. The emerging cybersecurity threats in the power sector must be addressed to secure such critical services.

1.4. Research Questions

The following research questions guide the development of the cybersecurity incident management framework for smart grid systems:

RQ 1: What are the specific cybersecurity threats and vulnerabilities unique to smart grid systems in the Ethiopian context, and how can these be effectively addressed in an incident management framework?

RQ 2: How can a cybersecurity incident management framework be designed to integrate with existing smart grid infrastructure and operations in Ethiopia, ensuring minimal disruption and effective response during and after an incident?

RQ 3. What are the key stakeholders involved in smart grid cybersecurity incident management in Ethiopia, and how can their roles and responsibilities be defined to ensure effective collaboration and communication during an incident?

RQ 4. How can the effectiveness of a cybersecurity incident management framework for smart grid systems in Ethiopia be evaluated, and what metrics can be used to measure its success in mitigating risks and ensuring the power grid's resilience?

1.5. Objective of the Study

A. General objective

To develop and evaluate a comprehensive cybersecurity incident management framework tailored to the specific needs and challenges of smart grid systems in Ethiopia. The aim is to enhance the power grid's resilience and ensure uninterrupted energy delivery in the face of cyber threats.

B. Specific objectives

The specific objectives of this study are:

- Provide risk assessment guidelines to determine and prioritize cybersecurity threats and vulnerabilities that could affect Ethiopian smart grid systems, with special consideration given to issues such as legacy infrastructure, integration of renewable energy sources, and human error potential.
- Template the incident management framework adaptable to Ethiopia's smart grid frameworks and operational structures. It should address minimizing downtime and streamlining the incident response process.
- Identify key stakeholders for smart grid cybersecurity in Ethiopia (e.g., government agencies, power utilities, technology providers, and cybersecurity experts) and define their respective roles, responsibilities, and communication pathways in the proposed incident management framework.
- Implement KPIs and metrics for assessing and evaluating the incident management framework's effectiveness, such as incident detection time, response time, recovery time, and impact on power grid operations.

1.6. Contribution of the Study

This research contributes to cybersecurity by developing a comprehensive incident management framework tailored to smart grid systems.

Theoretical Contributions:

- **Framework for Incident Management of Cybersecurity on Smart Grids:** The proposed framework for managing cybersecurity incidents, especially on smart grids, will consider developing countries and encompass the technical, operational, and regulatory aspects of incident management while considering the opportunities and challenges specific to developing countries.
- Contextualized Threat Model: This research will develop a contextualized threat model characterizing the risks associated with Ethiopian smart grid systems. Driven by the specific vulnerabilities faced by that country, from legacy infrastructure to integration of renewables and human error, it will be a valuable model for other developing countries with similar circumstances.
- Critical Infrastructure Stakeholder Collaboration Model: This study will also develop a model for effective collaboration among various stakeholders in responding to smart grid cybersecurity incidents. This model will also guide other critical infrastructure sectors beyond Ethiopia—even worldwide—on the roles, responsibilities, and communication channels of government agencies, power utilities, technology providers, and cybersecurity experts.

Practical Contributions:

- **Framework for incident management:** This research will deliver the most substantial tangible outcome: a generic but detailed framework for incident management on the Ethiopian smart grid systems. The framework will act as a handy, concrete reference point that power utilities, government agencies, and other relevant stakeholders could use for adequate preparation against and response to cyber incidents with minimal impact on critical infrastructure.

- **Evidence-Based Policy Recommendations:** The result will be a report with evidence-based policy recommendations for the Ethiopian government and other regulatory organizations to aid them in further formulating national strategies on cybersecurity and related regulations. These strategies shall be in tune with the peculiar Ethiopian context of a wise grid and a secure and resilient energy infrastructure.

This research advances the knowledge base around cybersecurity within the bright grid environment by presenting a holistic, encompassing framework that addresses technical and organizational issues in the domain. This new methodology will help build a more secure and robust cybersecurity framework for a smart grid ecosystem.

1.7. Scope/delimitation

Considering the study's objective, the research will focus on tailoring the cybersecurity incident management framework for smart grid systems for power utilities. This research does not include business continuity and disaster recovery planning.

Chapter Two

2. Literature review and Related work

2.1 Literature review

This chapter describes common concepts and terminology used in both incident management processes and explains various standards and guidelines for incident management.

Information Security Incident Terms will need to know the definition of Information Security Events Protocols & Computer Security Incidents: It is essential to make a difference between an Information Security incident and a computer security event. Based on the ISO 270002 [24] standard, it can be defined as follows:

- "Security event": An identified system, service, or network condition that indicates a potential violation of an information security policy, a security policy control failure, or a known or unknown state of the system that is based on the security concern.
- "Security incident": A single or a combination of unwanted or harmful events that may compromise business operations and information security.

In contrast to this, the NIST Special Publication (SP) 800-61: Computer Security Incident Handling Guide [19] goes on to define as follows:

- "Event": An observable occurrence in any network or system.
- "Security incident": Any identifiable unlawful act or threat, human or computer, against computer security policies, acceptable use policies, or security practices

What is Cybersecurity Incident Management? This general term encompasses the response to incidents and the entire lifecycle from planning, training, and awareness through detection, response, and post-incident learning.

Best practices and possible roles to fulfill for effective and quick incident handling are laid out in various guidelines and standards. Keep in mind that incident response takes a lot of planning and resources. A few key things in incident management are guidelines to

communicate and prioritize incidents and working with an assessment process to learn from incidents. [19]

Power utilities should have incident management policies, plans, and procedures (hereinafter collectively referred to as "incident management plan") as a part of their incident management capabilities, which need to be aligned with the organization's unique needs. Also, there's a methodology for reporting vulnerabilities that haven't been exploited yet. [10]

Information systems security incidents are a risk to an organization, so incident management is not just an IT-related question. Thus, organizations must have a planned and dedicated approach to building capabilities related to incident management to safeguard information. Incident management aims to prevent, contain, and resolve incidents and perform post-learning. According to ENISA [11], incident management "is an important tool of overall governance and to have it, in whatever form or shape, is necessary."

In recent years, cyberattacks have become far more complex, more prominent in scale, and more common—consequently, incident management techniques have transformed into critical measures for efficient cyber defense [14]. As a result, heightened privacy and security concerns create additional obstacles for organizations managing cybersecurity risks. A poorly designed incident response plan, or no plan, comes at significant risk, impacting areas such as revenue, legal implications, damage to the brand, and loss of customer trust. All of these can endanger the survival of an organization following a massive cyber-attack [15].

Equifax's 2017 data breach affected 147 million customers; better incident management could have made that incident less impactful. Poor internal controls and poor plans for incident management compounded the breach. Equifax's delay in notifying affected customers also led to considerable anger, lawsuits, and settlements. Ultimately, the company spent $18.5 billion on legal fees and compensation [16], eventually settling for $425 million for those affected by the breach 17.

Most cybersecurity incident management frameworks are risk-based or security controls-based to enhance organizational security. Yet, these frameworks fail to achieve an integrated flow through the whole industry value chain, especially in the energy industry, where the protection of assets is a key factor in electricity generation, transmission & distribution. This environment desperately craves an integrated framework that combines risk management, threat profiling, security controls, operational models, and governance. Such a framework is a means to

empower companies with proactive cyber incident management capabilities that span across the entire energy value chain from power utilities lifecycle phases (engineering, procurement, and construction (EPC))-to operation and retail. The cybersecurity frameworks typically focus on fortifying enterprise IT or Operational Technology (OT) infrastructure.

While they may assimilate pieces of the industry value chain and client business activity, this is not always their goal. The end game for organizations is to prevent different kinds of threats and mitigate threats to the value chain across strategic and operational levels. This cannot be understated significantly in smart grids, where access to energy is a key prerequisite for socio-economic development. Energy providers: As the energy transition accelerates, they are adopting digital technologies to drive reliability improvements across generation, transmission, distribution, and retail operations. This digital transformation involves the utilization of technologies such as supervisory control and data acquisition (SCADA) energy management systems (EMS) systems, as well as dispatching management solutions (DMS) to transform energy workflows. In addition, smart meters and Advanced Metering Infrastructure (AMI) software optimize customer energy consumption, and new electronic payment methods, such as mobile payments, are being implemented.

In addition, cybersecurity standards and guidelines are different around the world, which may include national standards like the National Institute of Standards and Technology (NIST) in the US, international standards such as ISA/IEC 62443, as well as national and international/global standards like ISO/IEC 27001 and 27002. ENISA Publications in Europe, publications by the European Union Agency for Network and Information Security (ENISA), have also been instrumental in establishing cybersecurity practices in the energy sector. As such, the intersection of cyber and digitalization in the energy space highlights the need for a comprehensive framework that balances the industry's value chain with proper safeguards against evolving threat vectors.

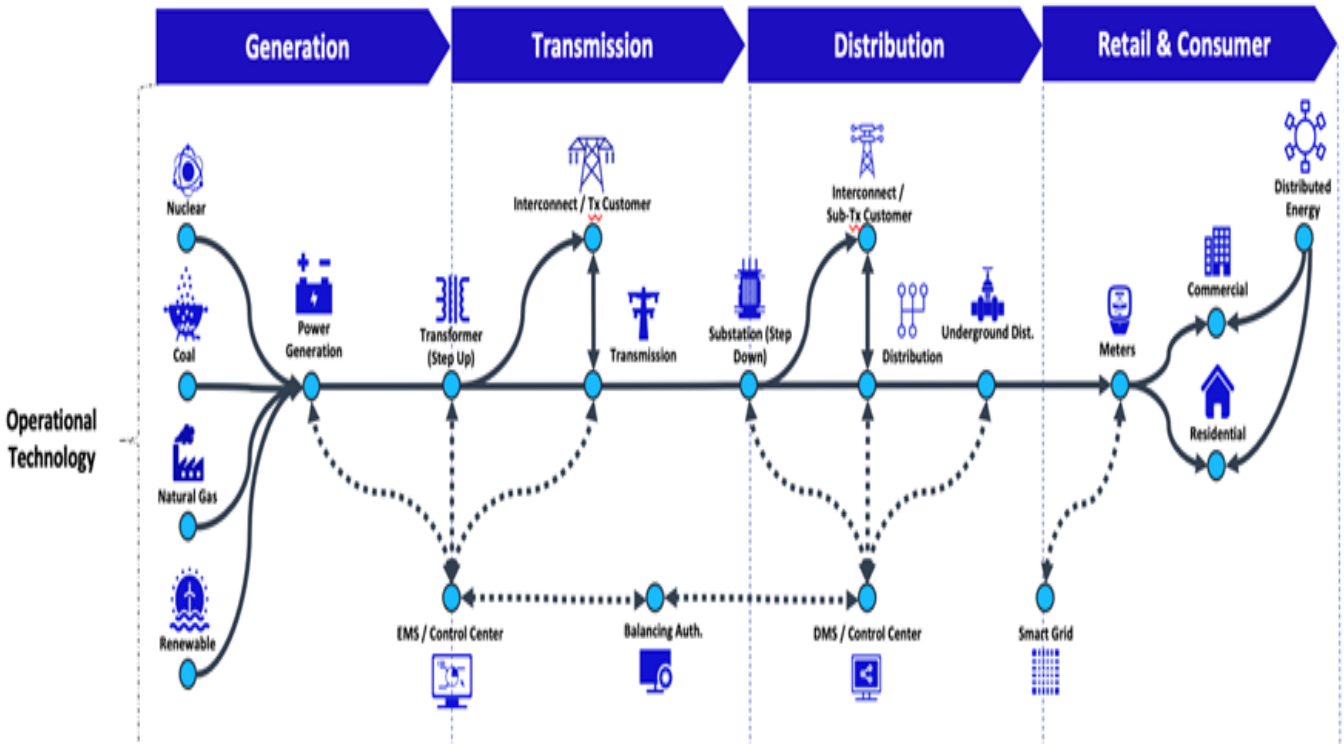


Figure 1: smart grid industry value chain.

Recently, with their providing advanced openings, digitalization has become great, lifting the evolution of countries. Significant investments are focused on creating the conditions for an affordable, secure, reliable, and cost-competitive environment for citizens and businesses in the region. However, setting up intelligent components necessary to join the overall Power Grid for high reliability and operational effectiveness paradoxically enhances the risks of disruption and inefficiency due to their vulnerability to cyber-attacks.

The entire value chain of smart grids is now facing multiple threats. The recent attacks demonstrate inherent power grid weaknesses, from the notorious Stuxnet computer worm in 2010 in industrial systems as a weapon to follow-up events like the Ukrainian Grid Attack dominated in 2016, the Russian crisis, New Delhi—India—Power Grid Attack—in 2021, and the European cyberattack offline 5800 wind turbine in Germany. Likewise, the 2023 breach of the AMI platform in Ghana accentuates the urgent call for robust cybersecurity protocols.

Cyber incidents are now a grim reality, the new normal. Critical infrastructures of the states hosted by power utilities are poised with the real risk of catastrophic disruption. Therefore, they must utilize all resources and efforts to protect and build a cyber-resilient infrastructure that commonly provides crucial services so that the safety of the people, the economy, the social structure, and the environment do not suffer consequences. Cyber resilience, supported by a practical cyber incident management framework, is the key to withstanding disruptions for power utilities. This integrated framework should reflect risk management, threat profiling, security controls, operating models, and governance, specifically customized for the energy value chain. The framework allows companies to take on such cybersecurity measures and better plan in advance to prepare for any cyber incidents. Furthermore, the framework should improve how cybersecurity is approached well beyond vertical technology implementation. It needs to shift to a federated, pragmatic approach that can activate all enterprise stakeholders and responsively compromise all resources across operational segment domains (strategic layer, operational layer). Although several cybersecurity frameworks take risk-based or security controls-based approaches, most of their practice emphasizes securing enterprise assets such as data, infrastructure, networks, and systems. Yet, these frameworks are frequently not seamlessly integrated into the overall industry value chain, leaving interrelated assets with points of failure. Therefore, it is necessary to have an integrated cybersecurity incident management framework in the smart grid industry, which integrates the technical, organizational, and strategic aspects and provides a roundabout way to leverage cybersecurity in the industry. The figure above depicts the cybersecurity incident management framework for smart grid systems.

2.2 Standards and Guidelines

Per NIST SP 800-61, incidents shall be prioritized, and handling, including the subsequent recovery of systems affected by incidents, shall consider any potential impact on service operation and data integrity. The aim is to reduce impact while maintaining the flow of critical services. It covers the entire cycle of incident handling, from preparation to recovery, for traditional IT systems, without a specific focus on energy systems. The SANS Incident Handler's Handbook provides a response and recovery, with key stages of identification, containment, remediation, recovery, and lessons learned. It's a handsome adventure and also focuses on elements of mitigation, preparation & incident management with its significance.

For example, Control Objective DSS02 of the ISACA-published COBIT® 2019 IT Governance Framework details managed service requests and incidents. According to this guidance, the top priority for an incident response within the context of incident management is providing Information and technology services. It includes mitigating, preparing, responding, and recovering with a possible guide for organizations when dealing with problems, such as identifying potential incidents, performing triage, successfully containing the incidents, and recovering after the containment. ISO/IEC 27035 discusses basic concepts of tools, techniques, and approaches that need to be taken in case of a cyber incident. Part 1: Information Security Incident Management — Introduces the principles of information security incident management, which integrates the phases of event detection, reporting, assessment, and response, as well as the lessons learned for application in response and recovery. Part 2 covers planning and preparing for cyber incident response and recovery.

Based on the IEC 62443 series allows processes to be established for setting up secure industrial control systems (ICS). Part 2-1 recommends setting up an ICS security program covering incident response and recovery preparedness. The rest of Part 4-2 also covers the technical security requirements for the ICS components, with guidelines for implementing rapid responses for security breaches agreed upon by notifying the responsible personnel and providing details of the security breach. Innovative grid information systems should be able to maintain or resume operations if standard functionality is interrupted. This encompasses a suite of high-level requirements for incident response aligned to the governance, risk, and compliance levels. This framework aims to improve cybersecurity risk management for critical infrastructure by providing a structured organization of standards, policies, and practices for

multiple cybersecurity risk management methods. Response and recovery are two of the five core federal functions.

NERC CIP-008-06 – Cyber Security Incident Reporting and Response Planning – sets standards for reporting incidents and creating incident response plans for North American electrical systems. By establishing incident response standards, these guidelines limit the potential for cybersecurity incidents to impact the continued reliable operation of large electrical systems and U.S. electricity infrastructure cybersecurity guidelines updated To fulfill these missions, the policies described in the INSA Critical Mass Cybersecurity Requirements framework are: a national information security policy, a national cybersecurity strategy, and a cybersecurity governor structure at the national level. It gives you a high-level overview of the incident management process. NIST SP800-82 outlines the steps for securing industrial control systems, offering an overview of the system architecture and vulnerabilities and both general and specific solutions to mitigate risk. This document describes response and recovery policies in industrial control systems, including incident detection, indigestion, response actions, and recovery actions

2.2.1 Summary of Standards/Guidelines

NIST SP 800-61 highlights the significance of collaborating and exchanging information with internal and external parties. The document outlines a broad structure for responding to incidents. It suggests ways to establish an incident response team with appropriate capabilities, policies, plans, and communication procedures to coordinate and share information with external parties. Additionally, the document guides creating procedures and offers hypothetical scenarios to apply the framework principles. However, NIST SP 800-61 does not cover energy automation or SCADA systems.

NIST's Guidelines [21] outline a series of overarching requirements for incident response in a smart grid information system. However, these requirements focus solely on governance, risk, and compliance and do not specify any relationship between information technology and operational technology systems. In Part 3 of the Guidelines [22], NIST highlights the need for further research on incident response in the cross-domain of IT and power systems. They note a lack of research and experience in incident response for operating environments where IT and control systems are closely integrated. The current recommendations only include high-level requirements for governance, risk, and compliance [15].

The NIST cybersecurity framework is structured by five ongoing and concurrent functions that provide a high-level strategic view of the lifecycle of an organization's management of cybersecurity risk. These functions, Identify, Protect, Detect, Respond, and Recover, offer a comprehensive lifecycle of cybersecurity risk management. Still, they primarily focus on risk control and prevention, not real-time response or recovery, when an organization is in the throes of a cyber-incident. The NIST Guide for Cybersecurity Event Recovery [32], on the other hand, provides an exhaustive disaster recovery strategy for a cyber-incident, including the proactive preparation and testing of recovery scenarios to be a part of a significant incident.

The ISO/IEC 27035 standard generally deals with enterprise systems and does not consider specific energy automation or industrial control systems considerations. Compared to other frameworks, ISO/IEC 27035 provides more detailed guidelines for incident classification while putting less emphasis on information exchange and focusing more on the organization itself. The SANS Institute handbook is relatively brief and lacks practical guidelines, except for detailing which activities should be conducted during each phase. On the other hand, the COBIT® model does not provide a lifecycle but instead describes management processes necessary for incident response and the mechanisms to assess the maturity of those processes.

Table 1 : Summary of standard/guidelines

Standard number/name	Benefits	Limitation
NIST (SP 800–61)	It describes the ability to use information gained during incident handling to better prepare for handling future incidents and to provide stronger protection for systems and data	✓ Did not address energy automation systems or SCADA systems in general. ✓ Lack of defining roles and responsibilities ✓ Lack of Asset management ✓ Lack of risk management.
IEC 62443	Establishing an ICS security program, including planning for incident response and recovery.	✓ Includes no post-incident analysis, risk management documentation, critical asset assessment, and continuous threat analysis for vulnerability remediation.
ISO/IEC 27019	Provides guidance to fulfill the objectives set out in ISO/IEC 27001 and 27002 for ICS within the energy utility industry	✓ Includes no post-incident analysis for root cause, incident detection mechanisms, and personnel training for response teams and awareness.
ISO/IEC 27035	Provides best practices and guidelines for conducting a strategic incident management plan and preparing for incident response.	✓ covers enterprise systems in general and does not include considerations specific to energy automation or industrial control systems. ✓ lack of information on post-incident analysis. ✓ Lack of defining roles and responsibilities ✓ Lack of Asset management
NISTIR 7628	It describes the ability to develop effective cybersecurity strategies tailored to their combinations of bright grid-related characteristics, risks, and vulnerabilities.	✓ describes high-level requirements for incident response for a smart grid. However, all requirements are at the governance, risk, and compliance levels.

NIST framework for improving critical infrastructure	The Framework's prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of critical infrastructure	✓ The framework consists of five continuous and concurrent functions. These include Identify Protect, Detect, Respond, and Recover functions. These features do not help an operator respond to or recover from a cyber incident that is happening in real-time; instead, they are designed to control risk before a cyber occurrence.
NERC (CIP-008-06)	To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by	✓ Lacks details on continuous threat analysis for addressing vulnerabilities and reducing attack vectors, and omits risk management documentation guidance.
	specifying incident response requirements.	caused by an incident and eradicating incidents.
NIST SP 800–82	Guide organizations on how to secure their industrial control systems against cyber threats.	✓ Has no information on staff training, such as response team training or awareness training? ✓ reporting occurrences to the proper persons (internal or external). ✓ lessons learned from previous incidents to enhance present defensive capabilities.

2.3. Related works

As far as I know, literature reviews that primarily address the practices and frameworks of cybersecurity incident management in power utilities are scarce. Moreover, the scope of these reviews is usually narrow. Line et al. For instance, [35] studied, among other things, the distribution system operators (DSOs) in the Norwegian electric power industry and the main DSOs (both small and large). According to the study, risk perception and preparedness levels are particularly low within smaller DSOs. The researchers said DSOs should establish written procedures, conduct exercises to validate readiness, and increase detection capabilities

surrounding the response to new and emerging threats posed by cybersecurity incidents for control systems.

However, it lacked generation and transmission system operators and did not offer an integrated framework to manage cybersecurity incidents. In contrast, the study of Tondel et al. further departed from the Meyrick method (in that its focus was distribution system operators) [36]. Included in several recommendations following an extensive literature review of industry incident management practices. Although ISO/IEC 27035 is not tailored to power utilities, the study did use relevant practices and compiled those in terms of the incident management phases given in the standard.

Similarly, Jaatun et al. They addressed specific aspects as part of a broader investigation [37] focused on information security incident response management within power distribution service operators (DSOs). Using semi-structured interviews, the researchers highlighted the importance of communication and collaboration in managing and responding to information security incidents. However, this study only focused on DSOs, and generation and transmission system operators were excluded from the interview process. Barnes et al. [38] also emphasized the requirement for explicit human capital to handle cybersecurity breaches efficiently.

Tondel et al. L.D. Zhi et al. However, for information security in the power industry, they state that a broader view of incident management is required to prepare the field against future challenges, specifically the implementation of Smart Grids [39]. The study showed, however, that information technology (IT) and information and cyber security (ICS) disciplines prepare for information security incidents differently. However, the work left some areas of incident management practices untouched.

Line and co-authors [40] explored the relevance of industrial [Page 10] safety management techniques for managing information security incidents. However, their study focused on planning, compliance, situational responses, training, and incident learning. Another line of work along this direction [41] suggested future jigs of study to make enterprises stronger against information security incidents and how the power industry complies with the resilience engineering principles. However, their work did not investigate generation and transmission system operators, and the ISO/IEC 27035 standard was not customized for the electric utilities industry.

Table 2: Summary of Related Works

Author and Citation	Contribution	Limitation
Line, M.B., Tøndel [33]	Survey and discuss current practices regarding information security incident management in small and large distribution system operators (DSOs) in the Norwegian electric power industry. Several recommendations are provided based on the findings.	✓ The survey did not center on the cybersecurity incident management framework and did not involve generation, transmission, and system operators.
I. Tøndel, M. Line and M. Jaatun [34]	Surveyed literature that focuses on current practice and experiences with incident management, covering various organizations. based on the incident management phases of ISO/IEC 27035.	✓ Incident management phases of ISO/IEC 27035 were not tailored for electric utilities.
M. Jaatun, M. Bartnes, I. Tøndel [35]	A survey and discussion on knowledge and communication between Information and Communication Technology (ICT) and industrial control system staff should improve the incident handling process.	✓ Did not focus on the cybersecurity incident management framework. The survey did not include generation and Transmission, and system operators.
M.Bartnesa, N. Moeb, P. Heegaarda [36]	Comprehensive surveys of the need for well-established human capital to respond to unwanted incidents.	✓ The emphasis was on training, and a customized cybersecurity incident management framework was not proposed.
M. Line, I. Tøndel and M. Jaatun [37]	Reviewed the potential of using current practice regarding planning and preparation activities for incident management and identified similarities and differences between the two traditions of conventional IT systems and industrial control systems.	✓ This survey did not include incident management activities other than training and did not cover generation, transmission, and system operators.
M. B., Line E. Albrechtsen [38]	To assess whether industrial safety management strategies are appropriate for handling information security incidents.	✓ They only focused on planning, compliance, situational response, training, and incident learning.

M. B. Line [39]	This study examines how closely the power sector adheres to the resilience engineering principles and makes recommendations for future actions that may be performed to increase resiliency to information security incidents.	✓ Incident management phases of ISO/IEC 27035 were not tailored for electric utilities, and the survey did not include generation and Transmission system operators.

2.4 Research Gaps

To address the gaps in the existing literature, the review summarized in Table 2 highlights the contributions and limitations of previous studies. Consequently, the current study seeks to develop a customized cybersecurity incident management framework for power utilities that address these shortcomings.

Chapter Three

3. Research Design Methodology

A design science and qualitative discussion research methodology has been used to develop a comprehensive cybersecurity incident management framework for smart grid systems.

3.1 Problem Identification

Problem Identification: The first step in the design science research methodology is problem identification. This problem is identified by lacking a holistic power utility cybersecurity incident management framework. Abstract Cyber-attacks on power utilities can potentially cause dire consequences on the power grid, from power outages to equipment destruction and even physical damage. These attacks may be done with the knowledge that an organization works under the element of surprise, without a proper framework on how to counter such attacks within incident management to ensure recovery and sustainability of the grid. Therefore, the Cybersecurity Incident Management System framework is highly regarded for helping the power utility effectively identify, detect, act upon, and recover from cybersecurity incidents.

3.2 Objectives of the Solution

The research objectives are to develop a tailored cybersecurity incident management framework for power utilities to analyze their affectivity, reduce the impacts of cyberattacks on power grid systems, and improve the general cybersecurity posture. The study would identify the problems and needs of power utilities in this domain and establish more adaptable and implementable frameworks for power utility organizations.

3.3 Design and Development

The design and development phase of the cybersecurity incident management framework for power utilities is critical in ensuring that the final framework is effective in addressing the identified problem and the framework will be designed to address the specific needs and requirements of power utilities and will be based on industry standards and best practices. This will involve reviewing existing frameworks or best practices and adapting them to the specific needs of the power utility.

3.4 Evaluation

The effectiveness of a cybersecurity incident management framework specifically designed for smart grid systems was validated by presenting threat scenarios involving Distributed Denial of Service (DDoS) and ransomware attacks to determine how well the framework addresses these prevalent cyber threats by mapping the DDoS and ransomware scenarios to various components of the cybersecurity incident management framework, including visibility, detection, analysis, containment, eradication, and other components the framework and evaluate the strengths and weaknesses of the framework in combating these threats.

3.5 Communication

The proposed cybersecurity incident management framework will be communicated and disseminated to relevant stakeholders for power utilities, and it will strengthen cybersecurity resilience in smart grid systems, supporting sustainable development and social well-being.

Chapter Four

4. Problem identification, objective and Design of the framework

4.1 Problem identification

Cyberspace has witnessed growing complicity and frequency of cyber-attacks targeting smart grid systems. Instead, one example is the attack on Ukraine's power grid in 2015-2016, which resulted in large-scale power outages and demonstrated the deep-scale impact of cyber-attacks on smart grid infrastructures. Curaçao's utility company Aqualectra suffered a cybersecurity incident and disconnected from the Internet to secure its internal systems and customer services. This followed the Dec. 6, 2023, claim of responsibility by the Akira ransomware group, saying they had accessed the company's operational files, business documents, payment information, and other sensitive data. A cyber intrusion occurred within AVU, a German energy provider that supplies electricity to Hattingen and Sprockhovel, 2023. As a safety measure, AVU's systems were quickly severed from the internet and went offline to ensure no potential injury occurred. As a result, the company's online customer service platform was temporarily disabled. On May 18, 2024, SCADA systems were targeted by the Ransom Hub ransomware group, encrypting and exfiltrating 400 GB of data, potentially stopping production and disrupting waste and energy management [43]. For example, the Solar Winds supply chain breach 2020 highlighted the risk that critical infrastructure providers, including those supporting smart grid systems, may be targeted by cybercriminals seeking to compromise software supply chains.

The challenges they face in managing cybersecurity incidents have been elaborated during discussions with a focus group of Ethiopian power utilities comprising a cybersecurity team, power grid engineers, managers, and operators from generation, transmission, and distribution sectors:

- Legacy Systems: Many power grid systems without current security features use old technology. Retrofitting these legacy systems with robust cybersecurity without introducing new disruptions to operations is a considerable challenge.
- Old Security Protocols: Systems existed before hackers and were not integrated with the necessary security elements. Hence, they are vulnerable to all cyberattacks, such as malware infections and data breaches.

- Limited Patching and Updates: Once manufacturers stop providing patches and updates, outdated systems become susceptible to vulnerabilities. These systems usually stay the same for long periods, making them relatively easy targets over time.
- Supply Chain Vulnerabilities: An international supply chain supplies power grid components. These components provide avenues through which threat actors can exploit them during manufacture, transport, or even installation, resulting in higher possibilities of cybersecurity breaches.
- Insider Threats: Disgruntled workers or contractors who gain vital access to energy plant systems present serious dangers. Such insider attacks, whether malicious or inadvertent, can shut down the power grid's operations.
- Password Sniffing, Guessing, and Cracking: Sniffing, which includes guessing and cracking of password hash dumps, is no different as a negligent per-box security policy, old software, and lack of encryption on power grid networks make sniffing a golden opportunity for password hash dump crackers.
- Malware: Building on the earlier threat class, malware is a significant and dangerous risk to the smart grid setting. If left uncontained, malware can wreak havoc and thrive in unprotected network infrastructure in the power grid.
- Social engineering: Power grid operators are particularly vulnerable to social engineering attacks, as cybersecurity defenses often take a backseat to networks designed for operational efficiency and cost-effectiveness.
- Cybersecurity incident management framework not applicable to the power utilities industry – The lack of a cybersecurity incident management framework for the power utilities industry makes cybersecurity risks even higher. Power utilities find it challenging to investigate and respond to threats without a defined strategy for cybersecurity incident management. This gap exposes critical energy infrastructure to potential cyberattacks, putting operational continuity and public safety at risk.
- Absence of 24/7 Security Monitoring—The shortage of continuous security monitoring in power utilities makes cybersecurity incident management harder. Q: What if there is no real-time surveillance? A: The delay will result in detection and response, leading to ineffective threat detection. This enhances the opportunity for effective cyber-attacks to threaten the reliability and integrity of critical energy infrastructure systems.
- Insufficient automation and tools—The Power utility industry lacks sufficient tools to handle cybersecurity incidents efficiently. Manual processes increase the time it takes

to detect and respond to threats, leaving systems vulnerable to exploitation. Advanced automation and algorithms play a fundamental role in the timely detection and response to cyber threats, ensuring the resilience of energy infrastructure.

- Shortage of specialist cybersecurity manpower—The scarcity of cybersecurity analysts within power utilities undermines the effectiveness of their management of cybersecurity incidents. Undeniably, this talent shortage undermines threat detection and response, increasing the likelihood of cyber-attacks. By attracting and retaining qualified professionals, incident management capabilities can be developed to protect critical energy infrastructure against a growing tide of emerging threats.

4.2. Objective of the Framework

The cybersecurity incident management framework for smart grid systems aims to:

- Define a process for identifying and responding to cybersecurity incidents.
- Enable smart grid operators and cyber security teams to rapidly identify and respond to such incidents, thereby preventing incidents from impacting critical infrastructure and ensuring the ongoing availability of vital public services.
- Promote holistic, autonomous cybersecurity event management protocols to counter threats, providing utilities with a full-spectrum approach, appropriate competencies, and operating models to handle smart grid risk and residual risk autonomously independent of the security standards of these security professionals.
- Include a small core set of capabilities, an operating model, and people to cover the entire smart grid value chain.
- Respond to cybersecurity incident management along the smart grid value chain, such as identifying risks to critical assets such as generation, transmission, distribution, marketing, AMI, and retail.

4.3. Design requirements

Currently, there are no such comprehensive guidelines to deal with the issue, and this formidable framework for managing cybersecurity incidents in smart grid systems will serve as an ultimate guide for smart grid operators and cybersecurity personnel to enhance their capabilities and ensure the mitigation of security incidents. This is important because it is based on the modern architecture of the power grid, with all its interconnectivity, presenting an immense attack surface for many types of cyberattacks. This framework was developed based on a comprehensive literature review, focused group discussions, and observations of the power grid ecosystem. The research group focused on analyzing multiple factors that affect power grid infrastructure cybersecurity incident management, both technology-related, organizations-related, and human factors. We captured these influential factors and included them as a key input to the initial definition of the framework's architecture. It is anticipated that this framework will serve as a means by which the detection, analysis, containment, and response to cybercrime incidents will be fast-tracked, streamlining the process for both smart grid operators and security personnel.

Recognizing that the smart grid world is evolving, the proposed framework is flexible enough to keep up with the flow of change in the electricity industry while adapting as new technologies and challenges emerge. The framework uses advanced technologies, data analytics, and cybersecurity incident management best practices to improve the overall resilience and security of smart grid systems and electricity supply for energy end-users. With increasing concerns over the cyber vulnerability of power grid infrastructure, this framework for cybersecurity incident management was developed as a fundamental step to allow those real-world initiatives to succeed. With the growing dependence on smart grid technologies, there is an increasing demand for effective cybersecurity incident management strategies. The framework can provide an essential tool in the continued efforts to protect the energy infrastructure's critical components and strengthen the power grid's reliability and resilience.

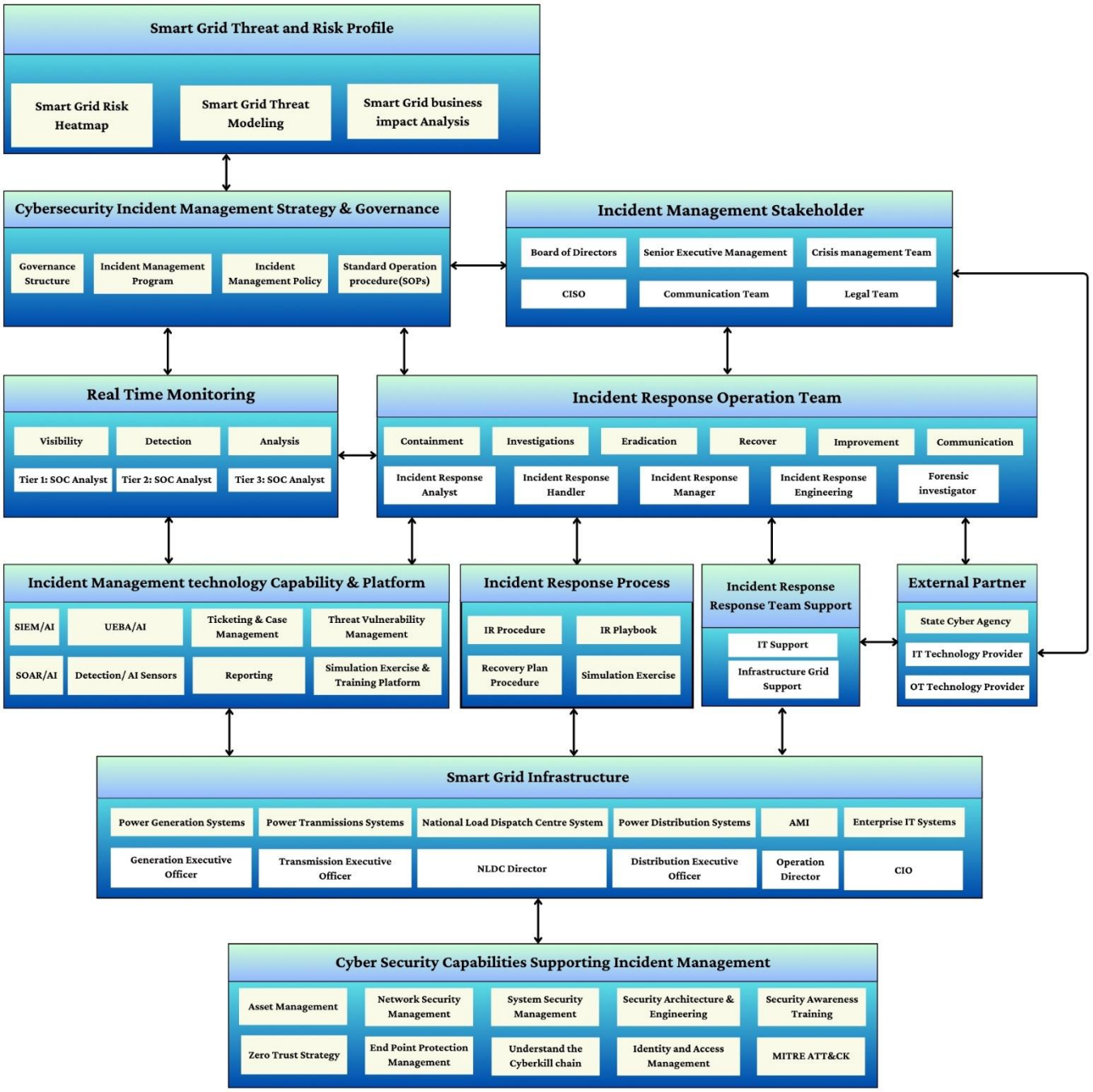


Figure 2:Proposed Framework for Smart Grid System

4.4. The framework components

4.4.1. Smart Grid Threat and Risk Profile

Worry about an aging power infrastructure due to the risk that outdated technologies, legacy transmission, and distribution systems may not have been updated, with decades of experience in cyberwarfare helping to create more up-to-date cybersecurity measures. These older systems are increasingly susceptible to cyber threats due to unsupported software, outdated standards, and fundamental security vulnerabilities. Nonetheless, modernization initiatives are still in continuous progress, digitizing the smart grid of the imminent generation, transmission, and distribution and implementing smart meters in Ethiopia's generation, substations, and distributions. As operational technology (OT) and information technology (IT) systems become more integrated, supply chain threats arise because vulnerabilities in the smart grid's third-party software or hardware components can potentially be exploited to compromise the entire infrastructure. It also creates a security vulnerability through insecure IoT devices, which are usually entry points to monitoring and control by smart meters and sensors. Smart grid systems constitute various stakeholders and personnel with different levels of cybersecurity awareness. Thus, insider threats can be considered intentional or unintentional, and the scale of impacts goes from data theft to sabotage or unauthorized systems access. The threats imposed by cyberattacks may be severe, disrupting vital services and leading to economic and social damage. It is very important to protect these key infrastructure units for economic versatility in a country and for the quality of life of its citizens. These growing digital perils call for proactive measures in the form of robust cybersecurity strategies, a practical cybersecurity incident management framework, and collective efforts among these stakeholders so that the risks are minimal and Ethiopia's essential power grid infrastructures are saved from imminent eventualities. Inadequately trained and uninformed personnel may accidentally create various threats to the smart grid, which would otherwise detect and respond to a cyber-attack. Budget restrictions can lead to neglect of key cybersecurity components, including legacy defenses, underdeveloped monitoring systems, and slow response to new threats. The smart grids are interconnected and vulnerable to cascading effects: a cyber-attack on one system can affect many critical services and infrastructure, and the remote or even rural areas smart grid infrastructures may not well serve the purposes of physical security and monitoring, which leaves potential vulnerabilities for cyber hackers taking advantage of their weaknesses.

Conducting a thorough risk assessment tailored to Ethiopian power utilities requires a structured methodology that addresses specific vulnerabilities, assesses relevant threats, and prioritizes risks based on their potential impact on energy delivery and operational continuity. The process involves the following detailed steps:

a) Vulnerability Identification

Perform engineer's physical inspections of smart grid infrastructure such as power generation plants, substations, transmission lines, distribution grids, and control rooms. Assess for vulnerabilities, including open access points, weak perimeter security, and critical equipment weaknesses. Develop an exhaustive listing of all hardware and software used for smart grid operations. Scrutinize configuration details and look for outdated firmware, default passwords, or unpatched systems. Automated tools and manual testing are used to find system vulnerabilities and periodic vulnerability scans are used to identify network, application, and industrial control systems' (ICS) weaknesses. Assess third-party vendors' and suppliers' components and services offered to the smart grid. Evaluate the supply chain risk from software dependencies and hardware integrations.

b) Threat Assessment

Monitor threat information related to the energy sector, including advisories from cybersecurity authorities, sector associations, and global entities. Monitor and report emerging threats against smart grid infrastructures like ransomware and DDOS. Assess internal risks that employees, contractors, and third-party service providers who can access key systems may pose. Analyzing historical data of incidents and breaches, identify recurring trends indicating that an employee may threaten the organization. Based on the identified vulnerabilities as well as any known adversary TTPs, develop threat scenarios. Containing threats targeting the Ethiopian smart grid, such as ransomware and DDOS targeting energy operations, now estimates the probability for each threat scenario based on historical data, threat intelligence, and expert assessment. Evaluate the impact on energy flow, availability of operations, potential financial losses, and public safety.

c) Risk Prioritization

Further evaluate the potential impact of each risk identified on key activities, including power generation, transmission, and distribution disruption. Consider customers' impact on, as well as repercussions affecting, the image of power utilities. Assess the likelihood of the occurrence of every risk case with regards to intelligence threats, assessment of vulnerabilities, and also based on operations' considerations. Employ a qualitative or quantitative method to assign likelihood ratings. Create a risk matrix integrating impact and likelihood scores to rank the risks. Assign numerical or qualitative risk levels (e.g., low, medium, high) to each identified risk scenario.

d) Risk Treatment Recommendations

A risk mitigation strategy recommendation is based on the priority risk assessment result. Invest in cybersecurity controls, risk transfer mechanisms, and incident response capabilities. For Ethiopian power utilities, the analytical process includes examining vulnerabilities, threats, and risks. The implementation of threat-modeling protocols will be one of the steps to counter attacks on the smart grid in Ethiopia; this includes a systematic To-Be Planning perspective of the utilities to identify a vulnerability from a power generation/transmission/distribution point of view accompanied by threat-assessment methodologies unique to the Ethiopian smart grid establishment with attendant risk management processes that help prioritize attacks relative to the challenges these utilities are facing so they focus first on the most threatening total cyber-attack events. This procedure enriches risk assessment according to the threat references, detection, and data conclusion.

In Ethiopia, smart grid components face cybersecurity threats that can significantly impact energy delivery, operational continuity, and grid reliability. Cyberattacks are a crucial concern for the smart grid components of Ethiopia. Following are specific examples of threats to smart grid components, their implications, and common approaches employed by attackers:

- Such attacks include malware and ransomware that can delay the operation of the smart grid by either bringing down critical systems like SCADA (Supervisory Control and Data Acquisition) systems or delaying their ability to operate. Attackers can exfiltrate sensitive data related to grid operations, customer information, or financial data, causing privacy violations and regulatory penalties. The financial implications of ransomware go beyond ransom payments and recovery costs. Phishing emails that

contain links or malicious attachments are often effective ways for attackers to infect systems with malware and gain initial entry into smart grid networks. Take advantage of known shortcomings in software and systems used within the smart grid components, like SCADA, EMS, and OTN systems. When on the network, they leverage lateral movement techniques to spread malware and ransomware to mission-critical systems to maximize impact. Privileged access for such insiders can be exploited to access sensitive systems or data, thus bypassing security controls like authentication or authorization.

- Deliberate deeds of insiders can interrupt organizations, change information or hurt the physical facilities of the smart grid framework. They do so for their profit or also for the benefit of outsiders. Insiders misuse their valid access to cripple systems or steal data. Insiders steal sensitive information without setting off security alarms using authorized access. One concern involves potential insiders with physical access to the smart grid components and could manipulate devices or systems for disruption or damage.

- Distributed Denial of Service Attack (DDoS) — DDoS attacks flood Smart grid networks with massive data traffic, resulting in service outages, which prevent legitimate users from accessing services. Due to the frequency of networks congested by DDoS attacks, delayed responses occurred in energy generation, transmission and distribution, and load balancing. If downtime and service interruptions occur, financial losses and penalties can happen due to SLA (Service Level Agreement) violations. As IoT devices with weak security or default credentials are compromised, attackers use botnets to launch significant DDoS attacks on smart grid infrastructure. Utilize amplification methods to supercharge DDoS traffic, inundating network bandwidth and impairing services. Overwhelming smart grid applications/services deplete server resources and disrupt services.

- Attackers infiltrate the supply chain, introducing malicious hardware or software into smart grid components, jeopardizing integrity. Firmware or software can make unauthorized changes in supply chain attacks that corrupt data and change operational

parameters. Supply chain attacks can be complicated to detect and mitigate, allowing attackers to operate for long periods of time while undermining trust in smart grid infrastructure. Attackers replace genuine parts with fake ones that contain malicious malware or vulnerabilities. Compromised software updates or patches propagated via the supply chain to introduce malicious code into smart grid systems target third parties.

Threat actors targeting smart grids in Ethiopia to exploit vulnerabilities can take several forms of tactics, techniques, and procedures to achieve malicious objectives; understanding these TTPs is essential to effective defense development and incident response strategies. Some common TTPs conducted against the power grid include:

Table 3 : Threat tactics techniques procedure

Threat	Tactics	Techniques	Procedures
Phishing and Social Engineering	Social Engineering: Threat actors craft convincing phishing emails or messages specifically designed for employees of power utilities or suppliers within the smart grid ecosystem. These messages deceive recipients into revealing sensitive information or clicking on malicious links. **Impersonation:** Attackers pose as legitimate entities, such as government agencies or trusted suppliers, to gain trust and solicit sensitive information or access credentials from their targets	Email Spoofing: Use spoofed email addresses that appear legitimate to trick power utility employees into disclosing credentials or downloading malicious attachments. **Credential** Harvesting: Create fake login pages or forms to capture usernames and passwords from unsuspecting victims.	Targeted Campaigns: Conduct spear-phishing campaigns against specific individuals within power utilities or suppliers involved in smart grid operations. **Pretexting:** Fabricate scenarios to manipulate victims into providing access to critical systems or divulging sensitive information in the power utilities.

Distributed Denial of Service (DDoS) Attacks	Botnet Recruitment: Recruit IoT devices or compromised systems to form a botnet capable of launching DDoS attacks. Traffic Amplification: Exploit vulnerable services or protocols to amplify the volume of traffic directed at smart grid infrastructure.	Use UDP-based protocols with spoofed source IP addresses to overwhelm network bandwidth. Application Layer Attacks: Target specific applications or services within smart grid networks to exhaust server resources.	Attack Coordination: Coordinate simultaneous DDoS attacks against multiple points in the smart grid infrastructure to maximize disruption. Impact Measurement: Monitor the impact of DDoS attacks to adjust tactics and maintain sustained disruption over time.
Insider Threats	Legitimate Access Abuse: Insiders misuse their authorized access to smart grid systems for malicious purposes. Sabotage: Intentionally disrupt operations or manipulate data within the smart grid infrastructure.	Data Theft: Steal sensitive information related to smart grid operations, customer data, or financial records. Physical Manipulation: Physically tamper with smart grid components to cause damage or disruption.	Covert Actions: Conceal malicious activities within legitimate operational tasks to evade detection. Data Exfiltration: Extract stolen data from smart grid systems using covert communication channels or removable media.

The ISO 27005 standard provides a structured framework for risk management, focusing on identifying, assessing, and treating risks to information security.

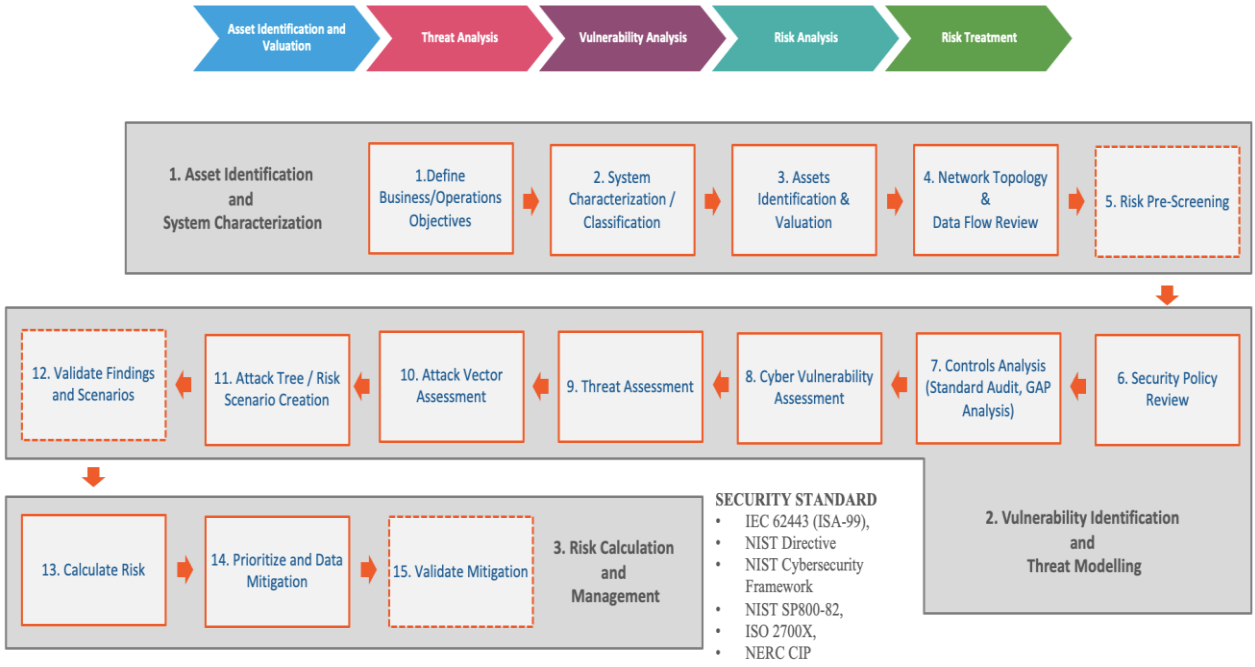


Figure 3: Risk Management process 27005

Applying this framework to smart grid infrastructure in Ethiopia involves several steps tailored to local context factors. Here's a detailed step-by-step explanation:

- Risk **Identification:** Identify all critical assets within the smart grid infrastructure, including generation, substations, transmission, distribution systems and networks, national load dispatch systems, and Advanced Metering Infrastructure (AMI). Including administrative systems, different databases, ERP systems, and communication networks. Assess risks posed by external actors such as cybercriminals, state-sponsored entities, hacktivists, and organized crime targeting power grid infrastructure. Consider risks from insiders, including employees, contractors, and third-party vendors with access to critical systems. Conduct vulnerability assessments to identify weaknesses in IT and OT systems, software applications, network infrastructure, and physical security controls. Consider vulnerabilities specific to the smart grid environment, such as outdated firmware, unpatched systems, lack of network segmentation, and insufficient access controls. Evaluate risks associated with

non-compliance with local regulatory requirements and international standards. Ensure alignment with regulatory frameworks applicable to the energy sector in Ethiopia.

- Risk Assessment: Determine the likelihood of occurrence for each identified risk using historical data, threat intelligence, and expert judgment. Assess the implications for each risk scenario on energy delivery, operating continuity, financial loss, and regulatory compliance. Quantify and prioritize risks using a risk matrix or scoring system based on likelihood and potential impact. Reviewing identified risks, assigning numerical values (e.g., 1-5 on a likelihood and impact scale) for each criterion to get a risk score for all your identified risks. For example, you may classify whether a risk is high/medium/low based on a risk score. Focus on the high-risk cases, which may seriously threaten smart grid infrastructure and information security.
- **Risk Treatment**: Network and IT cybersecurity controls like identity and access management, network access control, firewalls, intrusion detection systems (IDS), endpoint detection and response solutions, and PKI can safeguard both IT and OT systems. 04 Define the policies, procedures, and guidelines for secure configuration management, access control, incident response, and disaster recovery. Physical security control improvements at important infrastructure locations Explore Insurance and Contractual Strategies: Consider insurance options and contractual agreements to transfer financial risks associated with cybersecurity incidents to third parties. Include cybersecurity responsibilities and liabilities in contracts with vendors and suppliers. Describe risks that are accepted according to the way they are likelihood, impact, and power utilities risk tolerance level. Keep track of accepted risks and review periodically to look for changes in risk factors or mitigation actions.

Approach and Metrics

The framework leverages different approaches, best practices, and metrics.

- Risk heat map per energy segment /CMMI
- Financial Impact / Operational Impact / Customer Impact
- Threat profile per segment coverage
- Business Impact analysis
- RTO/ RPO/MTD

These metrics are used collectively to assess the overall effectiveness of the incident management framework in smart grid cybersecurity. By setting benchmarks and tracking these metrics over time, power utilities can identify trends, recurring issues, and areas for enhancement in incident response capabilities.

4.4.2. Cybersecurity incident management strategy and governance

Governance structure

A structured, supervised approach to responding to cybersecurity incidents is essential to manage the process. Either way, frameworks are established that define Roles, responsibilities, and protocols necessary to mitigate cyber threats. This implies that power corporations must construct a concentrated crew with different organic backgrounds in authority grid projects, IT, and cyber security. This team must be able to react, assess, and respond to cyber events in a coordinated manner to preserve the continuity of critical services. Cyber-security threats from various smart grid infrastructures can impact power supply and operations. Therefore, power companies must establish governance strategies that operationally manage cyber-related risks.

New security frameworks take a long time to adopt, and many utilities are even slower in upgrading their protection stack as they are not yet used to the security landscape. The changes might make employees resistant to new policies, procedures, and systems. Resource shortages in finances and personnel can also limit full-fledged security rollouts. Only communication and cooperation of different departments can help overcome these difficulties. Workshops and training for staff to understand the importance of cybersecurity should be conducted by power firms.

Cybersecurity becomes maintainable when utility providers work collaboratively with change-makers of the various departments, ensuring they take the steps required to achieve a solid framework. A careful assessment of risks and when to bolt down on cybersecurity is critical. Therefore, cybersecurity incidents cannot be managed in a vacuum; collaboration between almost all inter-departments, including cybersecurity, IT, operations, legal, and management, will be needed. Regular meetings and collaborative tools are needed to support effective communication and coordination. Protocols for interdepartmental cooperation on cybersecurity incident response should be clear. Identify who is responsible for decision-making within each role so that responses can be fast and efficient, and establish escalation processes for important decisions that require higher approval. Establishing communication protocols for regular updates and information sharing among stakeholders is also crucial. Cultural barriers inhibit cybersecurity awareness and incident reporting. Training that factors in the local cultural context can instill cybersecurity awareness. This can help make the training more relatable and

practical, for instance, by using local examples and case studies. Designing rewards to promote reporting of cybersecurity incidents by employees who participate in training programs can reward proactive behavior and instill responsible ownership for cybersecurity bottlenecks, processes, and initiatives. Cycle Awareness Campaigns, Newsletters, and Workshops Keeping cyber security in mind.

Approach and Metrics

Security governance aligned to strategic and operation actors that are involved in the risk impact:

- The baseline process is defined, as well as the implementation maturity and coverage.
- Role and responsibility definition based on people and assets involved in risk scenario Level of maturity
- The governance model integrates leadership, which is the risk owners.
- Scope of responsibility / Organization scope completion.

I. Incident Management Program

Setting achievable goals is critical for power utility companies pouring resources into their cyber incident response program. Establishing these goals early will inform staffing requirements, budgeting, and the choice of third-party solutions that best meet the use cases for the power utilities. The power utilities board and senior management should evaluate their current level of operational readiness, establish objectives, and, based on these factors, consider where to allocate funds for the incident management program. A key challenge of the smart grid's cybersecurity incident management strategy is its need to explore multiple cybersecurity risks for its components—generation, transmission, distribution, metering, and information systems. These risks are why power utilities need to be prepared for various scenarios. The main goal of this strategy is to assess and establish objectives for risk mitigation through the effective management of cyber incidents, thus minimizing their impact.

Approach and Metrics

Clearly define the objectives of the cybersecurity incident management program, such as reducing the impact of cybersecurity incidents, protecting critical assets, ensuring compliance with regulations, and maintaining business continuity:

- Program definition and engagement / Program progression/ Level of maturity.
- Attacker Heat maps in smart grid: Attacker heat maps represent a prioritized list of attack techniques that are most relevant in the smart grid
- Defensive Heat map: A defensive heat map represents a prioritized list of the mitigating value that implemented security controls have for attack techniques in the smart grid.
- Visibility Heat map: This heat map provides insight into visibility in a smart grid with an existing tool).
- Detection Capabilities heat map.
- Monitoring heat map.
- Process heat map.

II. Incident Management Policy

Such steps will require that many power companies have a cybersecurity incident management strategy in place as they work to safeguard the reliability and integrity of critical energy infrastructure. The plan protected systems that generate, transmit, operate, and distribute electricity from potential attacks. This is accomplished through a clearly defined incident management framework that establishes roles for all participants. Very important to report the power utilities to plan how to manage cybersecurity incidents with a high-level objective, scope, and guidelines. Businesses are also responsible for ensuring compliance with relevant laws and regulatory requirements. This includes a full analysis of all legal and regulatory compliance requirements, which may involve enlisting the help of attorneys to bring things in line with national and international standards to create and implement associated policies and processes. These policies should be updated regularly to remain compliant with ever-evolving

regulations. These policies must be communicated clearly to everyone managing cybersecurity incidents.

Approach and Metrics

Define the scope of the incident management policy, including the types of incidents to be addressed, the assets and systems covered, and the stakeholders involved.

- Policy coverage,
- Policy application

III. Standard operating procedure

A cybersecurity incident management plan for smart grid systems systematically manages cyber risks to the power grid's critical infrastructure. And as grid systems become increasingly digitized, those risks are at risk of becoming much worse. The plan addresses the need for practical guidance to mitigate incidents affecting smart grid systems' overall resilience and reliability. This plan bolsters the protection of the grid from cyber threats. This plan ensures effective incident management to minimize disruptions to essential energy services by establishing roles, escalation steps, and communication protocols. Utilize incident response playbooks to help dictate steps during cybersecurity incidents. Dynamic cybersecurity threats raise continuous improvement challenges, making it hard to know whether the framework remains effective. Keep the incident management framework fit by periodically reviewing and auditing it. Consider using audit findings to identify gaps and areas of improvement. Identify terms of reference: Critical to this is establishing clear roles, responsibilities, and workflows for the processes you introduce. Use that input to the work and continue to develop the framework. Create processes for routinely refreshing the framework as new threats and technologies emerge and lessons from previous events are understood. In this ever-changing world, staying updated on the latest news and trends helps keep your knowledge and understanding relevant and useful. Keeping up with the latest developments enables the security team to be well-informed, stay ahead of the competition, and respond to the changing environment.

Approach and Metrics

Develop a comprehensive strategy that outlines the necessary measures to be taken during a security breach. This should include clearly defined responsibilities, communication protocols, and a well-defined escalation process. Establish a uniform operating model across all aspects of procurement, design, and operation within the organization to ensure that best practices are consistently followed and resources are mobilized efficiently.

- Maturity in the standardization plan,
- scope of coverage,
- Procedure completion,
- Level of Procedure application,

4.4.3 Incident management stakeholder

The chief information security officer (CISO) is empowered to make decisions quickly during a security crisis. However, the chief executive officer (CEO) still has the final say on escalated issues. Conflicts must be resolved according to established protocols, and the CEO has ultimate decision-making authority. The incident response team performs an initial evaluation to assess the incident's severity and impact. They develop an action plan from this assessment, which the CISO then evaluates and approves. Any significant decisions are brought to the CEO for the final call. The incident response team then executes the approved action plan, and a post-incident review is held to learn lessons and improve future incident responses. You must invoice factors as part of your decision-making process: impact on operations, data integrity, customer trust, human and financial resources needed to respond (if needed), legal and regulatory compliance, and cost impact to internal and external stakeholders.

Table 4: Incident Management Stakeholder roles and Responsibilities

Incident management stakeholder	Roles and Responsibilities
Board of Directors	Strategic Decisions: Set cybersecurity strategy and risk tolerance. Resource Allocation: Approve budgets for cybersecurity initiatives. Oversight: Monitor overall cybersecurity posture and compliance.
CEO and Top-Level Management:	**Strategy Implementation**: Ensure integration of cybersecurity strategy into the business structure. **Incident Management**: Oversee incident management and response efforts. **Policy Approval**: Approve and enforce cybersecurity policies and procedures
Chief Information Security Officer (CISO)	**Risk Management**: Conduct risk assessments and develop protection plans. **Compliance**: Ensure adherence to regulatory requirements. **Incident Response Leadership**: Lead the Cybersecurity Incident Response Team (CIRT).
Cybersecurity Incident Response Team (CIRT):	Incident Detection and Analysis: Identify and assess the severity of cybersecurity incidents. Response Coordination: Implement response strategies and facilitate communication. Recovery: Expedite recovery efforts to minimize impact.
Legal Team:	Legal Compliance: Evaluate legal obligations and ensure compliance. Risk Mitigation: Guide disclosures and collaborate with law enforcement. Incident Response Support: Provide legal advice during incident response.
Communication Team:	Internal Communication: Share information with internal stakeholders. External Communication: Manage communication with external parties to maintain transparency and minimize reputational damage. Customer Assurance: Communicate the organization's commitment to resolving issues and maintaining customer trust

It is crucial to have continuously open and secure internal communication channels. This systematic communication of updates has allowed us to keep everyone as aware of the situation as possible.Guidelines followed by updated reports make such coordinated effort possible. For external outreach, model responses dictate interactions with the media. Impacted customers are promptly, and reporting to regulatory bodies is completed. Centralized platforms allow all stakeholders to share real-time information and coordinate with external organizations and

partners. The Incident Response Framework has a tiered structure. The Incident Response Team handles lower-level issues and keeps the CISO informed. CISO involvement will escalate concerns from medium to low and be replaced with those that warrant direct CISO involvement, escalating to potential CEO engagement. The CEO, Board, and possibly outside authorities must have been engaged for incidents with high severity. Once the Initial Response Team mitigates the situation to the greatest of its ability, it could escalate the situation to the CISO if the incident exceeds its capabilities. If an incident has legal, regulatory, or broader implications, external agencies are also involved, but the CEO is involved in high-impact incidents. Run exercises to simulate an incident response to bolster preparedness. Staff are kept updated on new multi-platform threats and mitigation tactics through workshops and seminars, while online courses allow ongoing education in case of resource issues; these can be tackled through prioritization of Cybersecurity funding for budget considerations, grants from specialist and international institutions, and leveraging with technology providers for innovative use cases.

Building cybersecurity competency requires an all-of-the-above approach. This includes investing in employee skill development through training, hiring skilled cybersecurity professionals, and working with external agencies to tap into specialized expertise. Security Training at different levels of an organization should be tailored. The Board should understand security threats, and management approaches at a high level, senior executives should incorporate security into business functions and incident response frameworks, CIRT team members should be continuously trained on detection, analysis, and response, and general staff should be equipped with basic security awareness and best practices.

Table 5: Stakeholders Metrics

Stakeholders	Metrics
Board of Directors	**Budget Allocation:** Percentage of budget allocated to cybersecurity. Reduction in identified risks over time
CEO and Senior Management	**Strategy Implementation:** Success in integrating cybersecurity into business operations**.** **Incident Response Time:** Time taken to respond to and resolve incidents. Adherence to regulatory requirements and internal policies.
CISO	**Incident Detection Rate:** Number of incidents detected versus actual incidents. **Compliance:** Adherence to regulatory requirements and internal policies.
CIRT	**Response Time:** Time taken to detect, analyze, and respond to incidents.
Legal Team	Number of incidents: managed in compliance with legal requirements Effectiveness in mitigating legal risks.
Communication Team:	Timeliness: Speed of internal and external communications during an incident. Stakeholder Feedback: Feedback from stakeholders on communication effectiveness.

.

4.4.4. Real-Time Monitoring

IT environments should use centralized log management and event correlation systems (SIEM) to monitor tools and techniques to differentiate IT and OT environments. In OT environments, ICS monitoring tools are specialized to provide real-time visibility into the operation. Implement intrusion detection solutions to monitor network traffic for suspicious activities and potential threats. EDR (End Point Detection and Response) tracks and responds to activity on the most vital endpoints. Data anomaly detection has progressed over the past few years to establish baselines that define normal behavior based on observational data. So, all of the intelligent algorithms used to detect anomalies in the smart grid should be improved by minimizing the false positives by tuning the abnormal factors, ranges, and rules. I would use machine learning methods, and then we can create models that adapt as new threats emerge and get more accurate over time when detecting anomalies.

Using forensic analysis tools to reconstruct events and ascertain root causes is part of the incident analysis process. Data from logs, network traffic, and system behaviors are used to identify indicators of compromise (IoCs) and attack patterns. Advanced analytics and threat intelligence are key to proactively looking for network threats. Form a cross-functional team of IT, OT, and security practitioners to benefit from their diverse perspectives while investigating incidents. It is vital to understand the role of a SOC analyst. Tier 1 analysts perform initial triage, verify alerts, and take basic-level incident response actions. The Tier 2 analysts perform a deeper investigation of the events, identify the root causes, and determine the severity and impact of the incident. Tier 3 analysts drive advanced incident response, coordinate with external parties, and apply strategic guidance to containment and recovery. Distinct escalation policies must also be defined depending on incident severity and complexity. Through such processes, communication and cooperation between SOC tiers must be ensured to facilitate knowledge sharing. Performance metrics also cover the time lapsed when a security breach is detected since the sooner such detection is accomplished, the smaller the potential damages. Effectively monitoring and lowering false alarms maximizes a security operations center's efficiency by minimizing irrelevant alarms. Assessing how quickly incident response activities were undertaken to limit downtime and minimize operational impact is critical. To detect threats comprehensively, organizations must evaluate the extent and depth of monitoring coverage across IT and operational technology environments—leverage reputable threat intelligence from external parties to augment monitoring and detection abilities. Using indicators of compromise to help identify and block known bad actors is a great

approach. Combining tactical (specific technical threat information) and strategic (broad threat landscape) intelligence to enhance contextual awareness and response efficacy.

Real-time monitoring components consist of the following subcomponents:

I. Visibility

Visibility Grounding in the cybersecurity incident management framework for smart grid systems, visibility refers to the full awareness of actions, threats, and vulnerabilities in the network. It is critical for fast detection, analysis, and response to incidents. Such visibility could be maintained through centralized log management, SIEM systems, and advanced monitoring tools for device behavior, system logs, and network traffic analysis. This vigilance is continuous so experts can identify suspicious behavior, investigate problems, and respond quickly. Reducing cyber and operational risks requires identifying and monitoring all connected OT and IoT devices and scaling OT asset inventory management across the power grid infrastructure.

II. Detection

The detection phase of cyber security attacks in smart grid systems is vital for managing such threats as it identifies abnormalities or security problems in the network. These systems are designed to promptly identify hazardous actions, illicit activity, or abnormal behavior for early intervention and response. Anomaly detection, advanced behavior analytics, and more are used to examine device activities, system logs, and network traffic to enable users to detect a possible threat and react on time. Effective detection reduces how long attackers are in the network and the overall impact of a security issue. For prevention, analytics have to be integrated with early warning systems and technologies that help us detect them in time and respond quickly to prevent more significant damage.

III. Analysis

The analytical phase is vital in the smart grid system-based containment mechanism for cyber security incidents. Critical assets, vulnerabilities, network design, and more must be meticulously analyzed. Phase: Analysis In this phase, the power utilities study potential threats and examine the impact of attacks on the operation of the smart grids. They map the threats to pin vulnerabilities through prolonged vulnerability assessments and help build containment protocols through network segmentation. Advanced monitoring tools will be able to detect anomalies that enable swift action.

IV. Tier 1: SOC analyst

A Tier 1 SOC analyst promptly addresses security alerts in smart grid systems. They track the system in real-time and event logs and take action according to business processes to resolve or escalate issues. These analysts are crucial in promptly identifying and classifying possible security threats to the smart grid system. They process initial analysis, elevate the gravity of occurrences, and take action to improve information distance for cyberattacks on the smart grid.

V. Tier 2: SOC analyst

Tier 2 Security Operations Centre (SOC) Analyst is an intermediary-level resource in the hierarchy of cybersecurity incident management for smart grid systems that conducts in-depth investigations and responses toward more sophisticated security threats. They work closely with Tier 1 analysts to further investigate escalated incidents, sucks as correlate data from multiple sources, and offer a holistic view of threats. Their experience includes combating advanced threats and limiting the consequences of security breaches while helping to boost detection improvements and strengthen smart grid cyber defense overall.

VI. Tier 3: SOC analyst

A Tier 3 SOC analyst can be seen as the top tier of cybersecurity incident management for smart grid systems, specializing in research and complex analysis. These analysts had to investigate the situation, figure out the threat, and devise a novel way to mitigate it. They conduct in-depth forensic analysis, work with other SOC tiers, and help gather threat intelligence. Tier 3 analysts are critical for understanding changing threat environments, building and improving detection and response capabilities, and maintaining resilience in smart grid cybersecurity. Their expertise is essential to tackling complex and enduring threats to critical infrastructure.

Approach and Metrics

Ensure that the perimeter is fully supervised and that the asset inventory, detection capabilities, response, and recovery are processed with the right maturity level.

- MTTD/ Detection rate
- False positive Rate
- Alert Triage time
- Percentage of Visibility

4.4.5. Incident Response Operation Team

The team assigned to respond to smart grid security incidents is a group of professionals trained in these attacks. The analyst reviews security alerts and incidents with a solid understanding of smart grid architecture and protocols. The incident response team kicks in action with containment and initial mitigation steps. The manager leads the organization in coordinating the response effort, allocating resources, and making critical decisions. The engineer provides technical knowledge and in-depth expertise in operational technology (OT) systems, network configuration, and smart grid network infrastructure. The cybersecurity investigator performs thorough forensic analysis, determines the root causes, and advises on remedial actions. To respond to these security incidents effectively, the team must understand OT systems, SCADA protocols, and grid operations. They also require cyber security principles, incident response frameworks, and threat intelligence analysis expertise. Because the approach includes many different team members and stakeholders, effective collaboration and strong communication skills are essential to keeping everyone coordinated.

Incidents are assessed by severity, based on surges in impact on grid operations, availability of service, and impact on customers—the risk assessment process factors into potential consequences and the possibility of further escalation. Resourcing decisions are based on the importance of the incident, aiming to reduce service outages and business impacts. Moreover, for addressing implementation challenges, real-time assessment of incidents must be in place so that they can be prioritized dynamically while keeping in mind emerging threats, system vulnerabilities, and evolving technology. As the smart grid infrastructure expands and cybersecurity threats evolve, the prioritization framework must be scalable.

Physical barriers and access controls are in place to protect critical systems and prevent unauthorized access. In the meantime, redundant backup systems allow essential services to

remain enabled while the incident is remediated. Automated systems react swiftly and effectively to contain impacted elements, utilizing human interaction only when automation fails to provide a viable remedy. Forensic analysis can take several days, and logs, network data, and system settings must be collected and analyzed to create a timeline of events. They identify the initial attack vector and, with that, the vulnerabilities exploited, then they come up and execute remedial measures, whether that be patching the system, updating the configuration, or changing the network architecture. In-depth post-incident reviews highlight failings in response protocols and ways to ameliorate them. This will create feedback loops for updated incident response plans and training programs. Data is critical for developing incident response tactics based on emerging threats and changes in the cybersecurity landscape. Internal communications are handled on encrypted platforms for team discussions, and this is used to facilitate updates. Communication protocols for incident updates, decision-making, and escalation processes are clearly defined, and protocols are established for engaging with regulators, law enforcement, customers, and the media during incidents to maintain transparency and manage reputational risk.

Organizing cross-team training efforts with IT, operations, and security to collaborate on joint training exercises. For instance, a centralized information-sharing hub could enable internal departments and external partners to exchange threat intelligence, incident data, and best practices. Therefore, senior executives can regularly align on cybersecurity and incident response capabilities through executive alignment meetings, enabling search-and-rescue teams and leadership teams to find and rescue others in strategic alignment. Power utilities can look at average detection times to evaluate the team's skills, which illustrates the efficiency of the triage process. The average response time tracking assesses the ability to contain and remediate incidents promptly. Analyzing how accurate they are in identifying actual security events is critical. Regular simulation and training assessments can improve response times and incident management capabilities. Proper coverage of these factors allows smart grid operators to strengthen incident management solutions, improve cybersecurity resilience, and ensure the continuity of their services in the face of the evolving cyber threat landscape applicable to smart grids.

4.4.5.1 Incident Response Operation Team Subcomponents

I. Containment

Containment is one of the significant elements in the cybersecurity incident management framework of smart grid systems. At a very immediate moment from identification, it is most important to act swiftly to stop incidents and minimize the impact on more assets. These are done by isolating affected systems and networks, preventing further unauthorized access, data loss, and interruption of critical processes. This can range from the isolation of compromised devices and network quarantine of segments to restricting access privileges and establishing temporary security measures. It may also involve setting firewall rules for power utilities, updating access controls, or creating network splits to reduce an incident's reach and minimize further damage. Containment strategies deal with how security events can be contained, or better said, mitigate the impact of security events, namely, operational downtime and further compromise of essential infrastructure elements. A well-implemented containment will allow an organization to investigate, erase, and recover from a cyberattack without giving up the integrity and availability of smart grids.

II. Investigation

Smart grid systems are crucial to cybersecurity incident management, and investigations are critical. It means gathering and analyzing data to understand the extent and impacts of security incidents. Such analysts would use forensic tools like system logs and network traffic to identify what happened before the attack. The aim is to understand the root cause of the breaches, learn how threat actors can exploit vulnerabilities, and assess the effects on critical infrastructure. Investigators also use forensic tools to maintain evidence and create timelines. They work with internal teams, external partners, and regulatory authorities to collect further information and guarantee compliance with legal obligations. The information learned from investigations assists in eradicating and recovering from incidents and building stronger armor to withstand future attacks better. Investigations are integral to security incidents, contributing to resilience and protecting critical infrastructure in smart grid systems.

III. Eradication

Settling smart grid systems and eliminating the misconfigurations, faults, and vulnerabilities that cause a security incident. It identifies any weak links the attacker might have impacted to exploit the system, software, or processes. Future rectification to eliminate not being automated in the smart grid systems will involve removing bugs from the software, upgrading the system configurations, and installing more security features. This is a more advanced stage than containment, focused on improving the smart grid infrastructure to keep it secure. It also encompasses the analysis of attacker techniques, security assessments, and best practices that are helpful in the reduction of risks and the enhancement of threat defense. Power utilities may also update and adopt their incident-response practices, train staff in cyber awareness, and strive to enhance their threat detection and response capabilities. Finally, cleaning protects smart grid systems against diseases by essential vulnerabilities and new threats while minimizing the potential for future attacks and protecting essential infrastructure elements.

IV. Recovery

In the event of a security breach within a smart grid system, recovery would be restoring affected systems, services, and data back to their natural state. This process should include using pre-determined recovery procedures, backups where necessary, and minimal downtime to try and work out the dependability of critical infrastructure components. Recovery attempts for smart grid systems can also entail retrieving lost data from backups, rebuilding compromised systems, and reconfiguring network access controls to make things work as they should. The power utilities should also do incident evaluations to understand the experience and improve incident responses in the future. Communication among stakeholders, like customers and regulators, and even internal teams for recovery reinstates confidence in the security and reliability of the smart grid systems. Power utilities should also pursue other measures toward resilience, including redundancy, refining procedures for incident response, and frequent staff training on cybersecurity. Admittedly, recovery aims to confine the effects of cybersecurity incidents related to smart grid operations to restore normal operations and ensure that the reliability and continuity of key infrastructure services will not be interrupted.

V. Improvement

In this respect, ensuring continuous improvement and optimization of power utility operations regarding cybersecurity incidents in smart grid systems is imperative. This is done through the critical analysis of past incidents to diagnose points of failure in the incident response life cycle and plug those holes. Other possible improvements may include fine-tuning incident detection, reviewing response procedures, and applying lessons learned from investigations to improve general cybersecurity posture further. It aims to address the emerging nature of threats with improvements in the efficiency of detection, response, and recovery of power utility from such security incidents. Regular training and awareness programs, upgrading technologies and tools used for pen-testing, and collaborating & learning from industry peers are constantly explored as part of the process for improvement. This allows the smart grid system to evolve to counter constantly evolving cybersecurity threats.

VI. Communication

Communication is very important in smart grid systems' cybersecurity incident management. Transparency with internal and external stakeholders is critical during and after a security incident, and information must be disseminated in real time. It is the basis for trust and coordination. Communication in the context of smart grids means informing relevant stakeholders efficiently where the respective and senior management, IT, security, power grid system engineers, and operators, among others, are educated on the incident. External communication may include notifying regulatory bodies, government agencies, customers, and the public, depending on the severity of the breach. In addition, transparent communication is critical to managing expectations, mitigating reputational damage, and creating a collaborative atmosphere with outside actors. People become interested in stories and stories as communication strategies, such as regular updates on incident response and remediation efforts. It is also essential to guide customers and partners in protective measures. Drills and simulations help refine communication protocols to ensure a coordinated response to cybersecurity incidents in smart grid systems, reducing the potential impact and helping achieve a swift recovery.

VII. Incident Response Analyst

A cybersecurity smart grid system incident response analyst is key in handling and tackling incidents. These experts zero in on spotting, tackling, and fixing security problems within smart grid systems. In this job, you'll do in-depth analyses and team up with other security pros to create and roll out effective incident response plans. Incident response analysts are vital to finding the root causes of incidents, lessening their impact, and setting up steps to stop future issues. They ensure a swift and well-coordinated answer to cyber threats, guarding critical infrastructure from harmful attacks and boosting the overall safety of smart grid systems.

VIII. Incident Response Handler

An Incident Response Handler in the cybersecurity field for smart grid systems is an expert who steps in to manage and coordinate the game plan when a security issue arises. Their primary focus is handling the situation, reducing the fallout from incidents, and leading the recovery efforts. These folks work closely with different groups, like SOC analysts, power grid engineers, operators, and IT specialists, to ensure that the response to cyber threats is quick and effective. By tackling security incidents swiftly, they help keep smart grid systems running smoothly, minimize disruptions to essential operations, and put measures in place to prevent similar issues down the line—ensuring the integrity of the infrastructure stays intact.

IX. Incident Response Manager

An Incident Response Manager has a significant role in driving the development, coordination, and execution of incident response strategy as part of the smart grid systems' cybersecurity incident management framework. Leadership encompasses determining response priority, incident response team management, and maintaining consistency with the organization's overall goal. Incident response managers play a crucial role in improving the overall cybersecurity resilience of smart grids by leading effective response programs, developing cooperation among staff members, and improving incident response programs continuously through lessons learned from security incidents.

X. Incident Response engineering

In the context of smart grid system cybersecurity incident management, an incident response engineer is a technical professional charged with designing, implementing, and maintaining incident response capability. The job includes creating and enhancing response procedures and installing and configuring incident response software. Incident Response Engineers have an important role in enhancing smart grid systems' readiness and response capability to respond rapidly to cyber threats, minimize the effects of incidents, and ensure the reliability and availability of critical infrastructure components.

XI. Forensic investigator

Forensic specialists have a central function within the smart grid cybersecurity incident handling field. They identify the origin and effect of cyberattacks. Their principal roles are to gather and examine digital forensic proof for the purposes of reconstructing the chronology of events that led to an incident. In addition, they identify the methods used in the attack and, where possible, assign blame to the associated threat actors. Forensic examiners and incident response groups help organizations understand the breach and make effective recovery and mitigation plans. They fully document what they discover, which is necessary for legal action, regulatory compliance, and strengthening cybersecurity. As smart grid technology advances, so do cyber threats. Forensic examiners reinforce ongoing work to enhance incident response capabilities and improve the resilience of critical energy infrastructure. Their skills and knowledge are essential in protecting the security, accessibility, and confidentiality of smart grid systems.

Approach and Metrics

Operation team handling incident process, covering all assets supervised and understanding the process to carry out using clear procedure and collaborating with all technical team per domain/

- MTTD/MTTR/Closure Time
- / Incident Level / Response team performance / %Incident Contained/
- Root cause Analysis completion rate/ Adherence to Incident Response Plan/
- IR quality documentation /
- Training effectiveness / compliance rating

4.4.6. Incident management Technology capability & Platform

Overcoming integration barriers with legacy systems addresses the issues of integrating with older existing OT systems, ensuring compatibility and the least disruption to grid operations. Define the data ingestion approaches and processing capabilities to handle the vast volumes of real-time data from a range of smart grid devices. Leveraging emerging technologies research using AI and ML algorithms for advanced anomaly detection in smart grid traffic and device behavior, enhancing early warning threat detection capabilities. Use predictive analytics models to forecast potential cyber threats from previous history and current-day network trends. Third-party security solutions must be integrated with smart grid infrastructure, and regulatory requirements must be met. Scalability is important in designing an infrastructure that can adapt and scale to accommodate the evolving needs of the smart grid and the increasing volume of security data while maintaining performance. Conduct a comprehensive cost-benefit analysis to validate investment in security technologies like SIEM, SOAR, and others based on operational and reputational risk. Calculate the return on investment based on improved incident response, reduced downtime, and enhanced compliance. Create customized training programs incorporating SIEM, SOAR, and UEBA for your security team and prioritize cross-functional collaboration to bridge skills gaps and strengthen incident response capacity. Incident Response Operation Team components include the following subcomponents:

I. SIEM/AI

Integrating AI into SIEM platforms will make it easier to respond to incidents in smart grid environments more timely and effectively. AI-powered SIEM systems monitor the elements of smart grid systems and record and analyze events to detect vulnerabilities causing security breaches. The AI-powered SIEM solution is key to managing cybersecurity incidents associated with the smart grid. But this platform is not just smart; it combines the two disciplines that constitute most SIEM platforms: Security Information Management, or SIM, and Security Event Management, SEM. If one wants to understand what an AI SIEM does, then the best way, in my opinion, is to understand the duties that SIM and SEM perform across the smart grid infrastructure. It's all about real-time analytics of security alerts and log data

from the smart grid perspective. Let's dive into this: The installed base for SIEM is pretty thin regarding smart grid infrastructure. More reason to work smart and efficiently invest in upgradeable SIEM, not like a crummy refrigerator, but acting like a fine-tuned cybersecurity Rube Goldberg machine.

II. SOAR/AI

With Security Orchestration, Automation, and Response, teams can collaborate harmoniously with security tools and systems. AI powers this automation and replaces human effort for mundane tasks to ensure timely and accurate threat mitigation. Response: It involves taking correct and precise action over incidents from a single platform. Integration of AI with SOAR enhances cybersecurity incident management in smart grid systems. AI-driven SOAR enhances cybersecurity operations by embedding advanced orchestration, automation, and informed decision-making in incident response. In the context of smart grid systems, AI-enhanced SOAR assures unparalleled efficiency with the automation of routine tasks, consistent and adaptive responses, integration of diverse security technologies, and scalability to cope with complex infrastructures. It enhances cybersecurity incidents' detection, analysis, and response toward a more resilient and secure infrastructure.

III. UEBA/AI

AI integrated with a UEBA system enhances cybersecurity in the smart grid to a great level. It is used for threat detection, especially insider threats. The inclusion of AI will extend its capability of analyzing user and entity behaviors to a large extent to recognize possible security risks accurately in real-time. AI-driven UEBA uses advanced machine learning algorithms to determine baseline behavior for users and entities. It is always on guard for deviations, such as unauthorized access, abnormal data transfer, or any other suspicious activity. This will allow quicker and more accurate detection of cyber threats in an inter-connectedly complex environment such as smart grid systems. AI can enable the UEBA solution to analyze the vast volume more efficiently and detect subtle patterns or anomalies that had remained undiscovered earlier, thus enhancing the system's general in smart grid security or quick response incidents. Basically, times like this demand getting updated on such recent changes coming into AI-integrated UEBA, which is very important for its application in various settings.

IV. Detection / AI Sensors

AI-powered sensors for smart grid cybersecurity are game-changing. Equally important, these are effective means for closely monitoring activities within the network about system records and device behavior through artificial intelligence to quickly detect anomalies, such as unauthorized attempts at accessing the network, malware, or unusual behavior patterns. These sensors can identify threats more precisely than ever by adding AI capabilities. Thus, the response swiftly mitigates risks and controls incidents before things get bigger. Integrated detection sensors using AI are vital in the development of smart grid infrastructure for strengthening its security. AI thus puts utilities in an adequate condition to take proactive defense measures against the threats of the cyber world to ensure reliability and integrity within critical energy networks. These sensors are continuously monitored to maintain operational resilience and minimize the impact of cyber incidents. Specialized tools in this ecosystem involve AI-enhanced network intrusion detection systems and web application firewalls. Traffic monitoring, attack pattern detection, and threat response in real-time contribute significantly to obtaining an appropriate framework with effective cybersecurity against rapidly changing cyber-attacks on smart grids.

V. Ticketing & Case Management

Ticketing & Case Management form part of the cybersecurity incident management of smart grid systems. This module or feature of any incident management system is expected to capture security incidents in structured form and manage them to simplify the process through defined reporting, analysis, and resolution procedures. After an incident, it captures vital information regarding the nature of the incident, systems affected, and response action taken through a ticketing system. Case Management aligns disparate incidents within coherent cases. This helps a cybersecurity team look into incidents from all angles necessary and reach cohesively to solve them more coherently. This assurance of a regulated workflow will provide traceable incident response documentation. Thus, ticketing and case management improve incident response capability and compel teamwork by reinforcing infrastructure security through the management and communication of a task effectively from the beginning right through to its closure.

VI. Reporting

Incident management about cybersecurity forms part of the smart grid systems. It would include creating and disseminating information on security incidents in a structured manner. Record and analyze every incident detail to fully understand what transpired. It aims to report incident information to all relevant stakeholders, including the management, regulatory authorities, and cybersecurity teams. A good report would contain, quite literally, the chronology of the event, the extent of the effect, the resolution of the fault, and lessons learned from it. Timely and precise reporting further helps increase transparency to support decision-making and enhances the cybersecurity strategy related to smart grid systems.

VII. Threat Vulnerability management

Smart grid systems are vulnerable to several cybersecurity risks. Threat vulnerability management is proactive in nature, the process of threat vulnerability identification and assessment, followed by mitigation. In general, threat vulnerability management shall provide continuous assurance checks of the smart grid infrastructure about possible vulnerabilities that cyber threats may use. Such assessment shall include periodic scanning for vulnerabilities, penetration tests, and timely execution of security patches and updates where necessary. A threat vulnerability management approach minimizes exploitation by systematically bringing down the probabilities of vulnerabilities against smart grid systems. It, therefore, remains an important incident management framework that will enable smart grids to take up the cyber threat perspective in a very proactive way. Vulnerability management solutions support identifying and patching vulnerabilities, reducing the attack surface to mitigate the risk of incidents in the future. These tools will help an organization trace back to the root cause of the incident- the underlying vulnerabilities or misconfigurations- after the attack for proper remediation.

VIII. Simulation Exercise & Training Platform

Simulation exercises and training platforms constitute any smart grid system's cybersecurity incident management framework. As such, a dynamic, interactive way of training cybersecurity teams on various aspects of incident scenarios is provided. Thus, the cybersecurity professional must first practice and hone their incident response capabilities against a simulated environment with all variables under control. These simulation exercises are designed to simulate real-life cyber threats and events; thus, teams can develop their skills adequately in the setting of detection, analysis, and effective response toward security incidents. Eventually, the cybersecurity workforce will be equipped to handle multi-faceted and continuously changing challenges related to smart grid systems in protecting against cyber-attacks and improving readiness and resilience in general.

Approach and Metrics

The technology must provide the next generation of Detection and response capabilities covering IT and OT with specificity in the Smart grid. The technology platform must also integrate an efficient sourcing strategy, robust architecture, elasticity, simulation environment, improvement, and innovation to cover priority risk, collaboration, and team training.

- Detection rate/ False positive Rate/ MTTD/MTTR/
- Orchestration Efficiency
- Scalability & performance
- Integration Capabilities
- Training and skill development
- Business impact reduction User experience

4.4.7. Incidence Response Process

Develop an overall incident response guide that would provide step-by-step procedures to detect, analyze, contain, eradicate, and recover from incidents unique to the smart grid environment. It should include decision trees and checklists to help cybersecurity teams make decisions in incident handling. In addition, detailed incident response playbooks need to be developed that define roles and responsibilities, communication plans, and processes for recovery. These should be accompanied by practical examples and case studies that can illustrate appropriate incident-handling methodologies for smart grid systems.

However, these considerations from OT will be very important in maintaining security without compromising continuous operational functionality. Incident response strategies should thus be developed so that the prime concern is minimal disturbance to critical grid operations during any security incident. Recovery plans need to be deployed as quickly as possible to allow restoration without compromising essential security measures to enable smart grid resilience.

Incident response playbooks can include threat intelligence to help proactively respond to incidents. This is likely to develop the capability for early identification of malicious attacker tactics, techniques, and procedures through proactive feeds of threat intelligence that impact decisions related to security incident responses. Preparation or effective training should be modeled after simulating practical, real-world scenarios about cyber-attacks aimed at smart grid systems. In these exercises, the roles of the participants and the evaluation criteria should be spelled out in terms of what will be expected from different stakeholders in incident response, such as SOC analysts and IT/OT personnel. The effectiveness of incident response procedures and playbooks should be clearly explained.

The incident response function within smart grid systems requires performance monitoring and benchmarking. A set of relevant, comprehensive metrics needs to be developed to track year-on-year improvement: for example, detection rate, MTTD, and MTTR. Set benchmarks and performance thresholds to ensure continuous progress. Continuous learning and adaptation using structured feedback mechanisms should be followed to capture lessons learned in each incident and simulation exercise. This will enable periodic incorporation of feedback into the incident response procedures and playbooks through updates and revisions. The continuous improvement cycle, including periodic reviews of incident response strategies, procedures, and

playbooks, will enable adaptation to cyber threats and operation requirements for smart grid systems.

Incidence Response procedure has the following subcomponents:

I. Incidence Response procedure

The Incident Response Procedure An incident response procedure in incident management in the case of cybersecurity within smart grid systems refers to an orderly process formulated for mitigating the impacts of security incidents. The procedure will thus present a step-by-step guide to be adopted by cybersecurity teams upon a security event in the systems. Usually, this consists of preparation, detection and analysis, containment, eradication, recovery, and lessons learned. The Incident Response Procedure provides a uniform, timely response when security incidents occur that aims to mitigate the damage, re-establish operations, and prevent recurrences. This is a well-structured process that will add to the overall resilience of smart grid systems because of the capability to give a quick and organized response to cybersecurity threats and vulnerabilities.

II. Incidence Response Playbook

The Incident Response Playbook presents this core of protection of smart grid systems against cybersecurity breaches. This broad document lays out a plan of predefined actions and processes that cybersecurity teams shall undertake in case of security incidents. The playbook will serve as a strategic guide to act against cyber threats and attacks in the smart grid context. This generally includes helpful information such as assigned roles and responsibilities, communication plans, detection and containment strategies, and recovery processes. Incident response playbooks help ensure the incidents are handled consistently and effectively with structured and organized approaches that minimize any adverse impact on smart grid systems. Further updates and rehearsals of the playbook on a periodic basis will develop increased preparedness and flexibility within cybersecurity teams for handling changes in the smart grid domain's landscape of cyber threats.

III. Recovery Plan Procedure

The procedure of a recovery plan in the domain of smart grid systems is important in protecting these systems from cyber threats. This is a written, systematic approach to restoring normal operations after a security incident that outlines steps and strategies that need to be instituted to minimize unnecessary downtime and return functionality to the affected smart grid infrastructure. These include such acts as restoration of data, reconfiguration of systems, and validation of security controls. In addition, it addresses the importance of communication, coordination, and collaboration with proper stakeholders in the recovery process. A well-implemented effective recovery plan aids the smart grid system to bounce back quickly from disruptions for infrastructure resiliency, providing uninterrupted essential services. The recovery plan is regularly tested for refinement in handling various cybersecurity incidents, further improving its effectiveness.

IV. Simulation Exercise

The simulation exercises in response to cybersecurity incidents in smart grid systems involve creating an environment that closely replicates the incidence of a cybersecurity event within controlled conditions. A key goal is to exercise and develop the cyber security team response capabilities in realistic simulated conditions close to real life. These simulations may include cyber security threats and attack scenarios relevant to smart grid systems, such as ransomware attacks or unauthorized access attempts. The aim is to assess and improve the team's capability to detect, analyze, and respond to incidents effectively. Through simulation exercises, cybersecurity professionals identify strengths, weaknesses, and areas of enhancement in incident response procedures that allow smart grid systems to be resilient against cyber threats.

Approach and Metrics

The technology provides the next generation of Detection & Response capabilities covering IT and OT with specificity in the Smart grid. The technology platform must also integrate efficient sourcing strategy, robust architecture, elasticity and simulation environment, improvement, and innovation to cover priority risk, collaboration, training for the team

- Detection rate/ False positive Rate
- MTTD/MTTR/ Orchestration Efficiency
- Scalability & performance / Integration Capabilities /

- Training and skill development
- Business impact reduction User experience

4.4.8 Incident Response: Response Team support

The team structure and expertise in smart grid environments are crucial in managing incidents. In particular, the composition should contain an IT Support Team that comprises network analysts, cybersecurity experts, incident responders, and system administrators. The members should be proficient in IT and OT systems to manage incidents effectively. It is further supported by an Infrastructure Grid Support Team composed of engineers, technicians, and operational people with expert knowledge of smart grid components, physical infrastructures, and operational procedures. Since collaboration mechanisms will be essential to smooth operations, clear communication paths and protocols between the IT Support Team and the Infrastructure Grid Support Team must be implemented, sharing information associated with any incident and responding jointly in case of a security incident. Exercises on joint training are warranted; tabletop simulation exercises and drills of various natures to show team interaction or coordination must be rehearsed for particular scenarios and their development of action programs needed in various specific incident response cases.

There are also specialized OT requirements in this respect. This includes formulating guidelines and procedures in incident response within OT environments under smart grid systems. Such guidelines must consider those particular challenges of OT systems, including real-time operational impact and IT/OT technology integration. The smart grid is singular in its operation and, as such, requires unique tools and resources. This includes monitoring solutions designed for operation technology, diagnostic solutions for physical infrastructure, and secure protocols for remote access. Incident Response: Responsibilities need to be explicitly assigned. Roles at every triage stage, containment, elimination, and recovery, must be pointed out for every team member. Decision-making power, procedures of escalation, communication with stakeholders, and management should be outlined in detail. Cross-training between IT and Infrastructure Grid Support further advances mutual understanding of the roles and full cooperation in cases of incidents.

Team effectiveness needs to be measured against specific metrics. It's about setting appropriate performance indicators, such as incident resolution ratios, recovery effort outcomes, and periodic reviews to understand team performance and areas for improvement. Success shall be measured by incident response quality: contained, no impact on grid operation, and organizational adherence to incident response. Continuous training is required for the teams to maintain or increase their skill level. Training programs should be ongoing to ensure that awareness of cybersecurity, incident response techniques, and emerging threats in Smart Grid environments is conveyed. Such programs shall include hands-on exercises and skills/knowledge certifications. Emphasizing continued skills development in areas like threat intelligence analysis, forensic investigation, and the fundamentals of OT security are some aspects that will make teams' readiness powerful and capable of adaptation.

Incident Response: Response Team support components include the following subcomponents:

I. IT Support Team

The IT Support Team participates in the core of the cybersecurity incident response process for the smart grid system. Their main objective is to provide technical assistance and know-how for a fast and effective response against cyber-attacks. Within the incident response team, they apply their expertise in IT systems and cybersecurity protocols to monitor, investigate, and mitigate various security incidents in the smart grid infrastructure. Also, they need to play an imperative role in implementing measures for prevention, sharp analysis of incidents, and the realization of corrective actions. Perfect coordination and communication are possible through this IT Support Team, therefore enhancing the capability of incident management processes that help enhance the resilience of the smart grid system against cyber-attacks.

II. Infrastructure Grid Support Team

The support from the Infrastructure Grid Support is essential for the cybersecurity incident response team in charge of smart grid systems. The critical infrastructures should continue to function unhindered by cyber security incidents. Support involves functionality in the smart grid system's important physical and digital parts. The Infrastructure Grid Support team supports the cybersecurity incident response team by promptly addressing disruptions and assisting in timely recovery; it also institutes measures that help protect essential services. Monitoring health and integrity on grid infrastructure follows through with deployment and works with incident responders on effective incident management strategies. It also improves the ability to handle and respond to cybersecurity incidents by strengthening stability and dependability in the smart grid's infrastructure.

Approach and Metrics

This team is integrated in the organization and is the link between

- Awareness completion
- Resource availability
- Mean time to respond (MTTR)
- Mean time to contain (MTTC)
- Number of successful recoveries

4.4.9 External Partner

Utilities should work with international organizations, research institutions, industry groups, other utilities, and state cyber agencies and technology companies. These diverse relationships can bring utility-specific expertise, resources, and expanded threat intelligence sources. Industry forums and collaboration platforms share best practices, threats, and lessons learned from cybersecurity incidents. Such a shared knowledge base may be helpful for general sector resilience regarding cyber threats. The need to create and make reasonable, formal arrangements with third parties outlining roles and responsibilities during incident response is underscored. Collaboration scope, incident handling, data protection, and other terms regarding responsible sharing and data exchange protocols have to be laid down, all within the ambit of relevant laws and regulations. Therefore, sharing threat intelligence, incident reports, and vulnerability assessments must have well-defined protocols. These protocols should describe how data formats, encryption standards, communication channels, and access controls protect

sensitive information. Mechanisms should allow real-time information sharing during incidents to advise quick response and mitigation.

Incident Response: The Response Team support component includes the following subcomponents:

I. Sate Cyber agency

That means it is on this basis that power utilities depend on state cyber agencies to protect against such threats to critical infrastructure. These agencies, in turn, have become indispensable in incident management, threat intelligence sharing, and collaboration in raising utilities' resilience. Therefore, they will impose cybersecurity standards and regulations, thus playing a core role in the prevention and mitigation process. Proactively, state cyber agencies ensure that the general security and dependability of utilities in power are upheld to reinforce the general defense against cyber adversaries in light of rapid changes in the digital world.

II. IT Technology Provider

IT technology is supportive, and the response team to cybersecurity incidents plays a vital role in smart grid systems. The key objective of the provider is to offer advanced technological solutions, tools, and expertise necessary for effective incident management, including cybersecurity software, threat intelligence, and network monitoring capabilities. The technology provider helped identify, analyze, and act upon many threats arising much quicker, thus adding substantial strength to overall smart grid cybersecurity. Conclusively, they need to collaborate closely with the incident response team, sharing the key knowledge they possess in emerging threats and vulnerabilities. IT technology keeps an incident response team ahead of cyber threats by allowing continuous innovation with a strong technological infrastructure, raising the bar for security and continuity in smart grid systems.

III. OT Technology provider

A key factor to this operation in cybersecurity incident response for smart grid systems involves the provider of OT technology. Instead, its objective should be to enable specialist technologies to be created for various OT environments to guarantee security and resilience to critical infrastructures. The OT technology provider provides anomaly detection tools and expertise in operational process protection and is equipped with advanced industrial control systems security solutions. In offering robust cybersecurity solutions for OT, they enhance the incident response team's capability to identify and mitigate cyber threats specific to smart grid systems. This includes close collaboration with the OT technology provider in developing effective incident response strategies to strengthen the smart grid against disruptions for continuity and security in operating essential services against cyber threats.

Approach and Metrics

These external parties have specific responsibilities based on contractual agreements and regulations. The IRP needs to be defined

- Awareness completion
- Resource availability

4.4.10. Infrastructure Monitored

Focus the framework on infrastructural components at higher criticality or that will lead to other infrastructure components of vulnerability in any smart grid incident management. Most critical infrastructure Generation facilities, transmission systems, and the NLDC have highly linked infrastructure components in smart grid environments. Generation facilities generate electricity flow along high-voltage lines in transmission systems that reach local, state-wide, or cross-boundary distribution systems that deliver electricity to their subscribers. The NLDC coordinates these flows, balancing the supply and demand in real time. Advanced Metering Infrastructure requires distribution and consumer feedback data for optimized grid operations. If any of the components are under a cyberattack, for example, disabling the NLDC-the, the whole grid is affected, affecting generation, transmission, and distribution. Monitoring strategies have to consider these interdependencies so that if an attacker succeeds in compromising one of the components, the others cannot be compromised, and the protection is comprehensive.

These form fundamental principles of maintenance in smart grids; real-time monitoring is unavoidable for cybersecurity across varied infrastructure components of cyber-physical entities. To maintain generation systems against cyber-attack methodologies using SCADA supervisory control and data acquisition system enhanced through appropriate anomaly detection capability tools like Nozomi Networks- operate on real-time monitoring of operating data and may catch irregular activity even at instances of regular operation under attack by sophisticated attacks. Transmission networks use PMUs and WAMS to monitor grid stability, while SIEM systems like Splunk or ArcSight analyze data for threats. These may be subject to latency issues and/or the complexity of managing large volumes of data. Distribution systems are monitored using DMS and advanced DA tools, with security solutions like Fortinet's fabric integrating real-time threat detection. These tools, though powerful, may face challenges in scalability and compatibility with legacy systems. The National Load Dispatch Center (NLDC) is safeguarded through AI-driven threat detection platforms like Darktrace and SIEM solutions for real-time monitoring. Yet, they might not fully address zero-day vulnerabilities—tools in AMI, such as IoT Threat Defense by Cisco, monitor and secure data flow. However, the number of devices will always present some challenges in handling, especially regarding securing a legacy system. The capability of every tool to meet limitations needs to be cautiously judged for comprehensive protection and resiliency within the cybersecurity incident management framework.

Infrastructure Monitored components include the following subcomponents:

I. Power Generation systems

Turbines, generators, and even control systems are various technologies generating energy used by power utilities. These assets and systems must be immensely relevant from their point of view. Strong cybersecurity should be in place with high implementation priority, complemented by an appreciation of the vital contributions these assets give. Protecting them shall be crucial in maintaining reliable and lasting power generation infrastructures.

II. Power Transmission systems

Power transmission assets and systems, including high-voltage lines, transformers, and control systems, form the backbone of utilities' energy supply. Strong cybersecurity measures are essential to protecting these assets and ensuring the reliability and resilience of the power grid.

III. National Load Dispatch Centre Systems

NLDC forms the very hub of power utilities and is centrally involved in the associated control functions relating to the assessment of demand and grid stability. In essence, it lays the basis by mentioning how vital NLDC assets and systems are, be it real-time monitoring, mechanisms for control, or data analysis. In all this, reliability and security form the bedrock of infrastructure at NLDC to ensure adequate national power grids. In this age of omnipresent cyber threats, NLDC must have strong cybersecurity measures. This would protect the integrity of energy transmission and make the entire power utility network resilient to provide uninterrupted and secure electricity to the country.

IV. Power Distribution Systems

Electricity distribution to end-users largely relies on substations, transformers, and smart grid technologies. In addition, considering such assets and systems are critical, cybersecurity should be very high on the agenda. This makes securing the distribution infrastructure critical to providing reliable and secure electricity supplies.

V. Advanced Metering Infrastructure (AMI)

In the world of constantly changing power utilities, Advanced Metering Infrastructure represents a whole different ball game. It renews the communication and real-time monitoring between utility providers and consumers. This first point gives an overview of the general AMI system and its assets, including smart meters, communication networks, and data management systems. AMI improves operational efficiency, demand response initiatives, and grid optimization. With increased development and implementation, cybersecurity of the assets of AMI becomes an immediate concern. The introduction shows the need for stringent

cybersecurity measures to protect the integrity of the AMI infrastructure so that the power grid will remain reliable and secure against the emergence of cyber threats.

VI. Enterprise IT

Networks, servers, and software comprise the Enterprise IT infrastructure of a power utility- the digital foundation- integral to all aspects of its administration and business functions. As mentioned above, the statement specifies the cruciality of enterprise IT assets and systems to help smooth the flow of operations, manage data, and provide straightforward communication channels for utilities engaged in producing electrical energy. Moreover, security features become indispensable when networked technologies are used within a utility context. Cybersecurity has become critical in protecting sensitive data and operational continuity. Power utilities can achieve operational efficiency and regulatory compliance by empowering the resilience of Enterprise IT assets with an improved cybersecurity posture in today's dynamic digital landscape.

Approach and Metrics

The Incident response process starts with threats targeting Power Grid assets (Production, Transmission, Distribution, Market, Retail), where decisions must be made to permit limited access.

- Awareness completion per segment /
- Resource availability per segment /
- Business Impact Reduction / RTO / RPO

4.4.11. Cyber security capabilities supporting incident management

Incident management in smart grid environments has to be collectively performed through various team and departmental collaborations. This may include an integrated approach whereby IT, OT, Security, and operations handle incidents under the same umbrella of approach that deals with each incident integrally. Each brings its peculiar standpoints and different expertise into managing incidents. For example, IT contributes especially to cybersecurity considerations, whereas knowledge about the details of operational systems comes from OT groups. Security teams are concerned with the detection and mitigation of threats, while operations teams are concerned with the execution of responses with functional requirements in place. In this case, these teams together can quickly take action to identify an incident and minimize cascading downtime across interconnected systems. It improves a collaborative perspective in communication and response while protecting every aspect of the smart grid, thus comparing much favorably to an incident management approach.

Cyber security capabilities supporting incident management components include the following subcomponents:

I. Asset management

Cybersecurity asset management is of prime importance in the case of incident management because of its organized approach to the identification, organization, and tracking of digital assets belonging to an organization. Basically, it makes the incident response more effective and efficient by providing the exact inventory of hardware, software, and data resources so that anomalies can be identified quickly, incidents can be contained better, and grooved mitigation of damage can be done. Also, asset management assists in prioritization according to the importance of an asset to focus on and act effectively. Additionally, it will ensure configuration management is done as appropriate to disallow unauthorized changes and facilitate easy return of things to their state before the incident. Lastly, asset management helps to underpin the resilience in cybersecurity and integrity of an organization's digital infrastructure.

II. Zero Trust strategy

Pristinely, the actualization of Zero Trust in the smart grid could first be done with network segmentation, which separates and isolates less critical areas than more critical ones by function and sensitivity, such as generation, transmission, and distribution. Secondly, for greater detail, micro-segmentation will be based on zones, the best practices of internal segmentation firewalls, and segmenting with Virtual Local Area Network to segment into smaller environments, which tightens communication paths while reducing the surface space at which an adversary can attack it. Provide continuous authentication by adopting MFA and RBAC to ensure that only authenticated users and devices can access specific resources. Network traffic and user behavior monitoring should also be done continuously with SIEM tools, identifying anomalies to enforce security policies, never assuming trust, and always assuring security.

III. Network Security Management

Perhaps among such leading cybersecurity capabilities for incident management come the areas of Network Security Management. This type of security focus is targeted at shielding the network structure of an organization from unauthorized intrusion, disruption, and other malicious forms of cyber threats. Through incident management, Network Security Management performs real-time monitoring of the network and the flow of traffic. Thus, it helps discover abnormalities or other types of suspicious activity. It means setting up a firewall and systems for intrusion detection and prevention. Still, all those relevant security methods are involved in potentially preventing all incidents or perhaps only controlling things if there is an incident: the ability to concern isolated cases when they arise. Once isolated, it considerably minimizes the scope and potential influence of a related breach in the area. Network security management contributes to network communication integrity and confidentiality so that an organization can respond effectively and in a timely manner to incidents and risks in general.

IV. Endpoint Protection Management

Endpoint Protection Management encompasses some essential core competencies that support cybersecurity capabilities for incident management, its key scope being protection for individual computers, phones, etc., against possible perils on the web. Accordingly, its purpose would include running an antivirus program on devices and detecting intrusion and/or preventing the intrusion in collaboration with security software for safety features of all the endpoint devices. It provides continuous monitoring and threat detection on individual devices in the context of incident management, thus helping to identify security incidents quickly. This capability helps contain incidents by stopping, identifying, and responding to threats at the device level and minimizes the potential harm of incidents. Endpoint Protection Management is vital in the general cybersecurity strategy to ensure strength and efficiency within an organization's incident management processes.

V. System Security Management

The Security Management of Systems improves incident management in cybersecurity. This mainly aims at the safety and dependability of an organization's overall system infrastructure, configuration oversight, access controls, and security policies of varied systems. It plays a critical role in the timely detection and response to security incidents within incident management. It makes the system more resistant to unauthorized access, reduces vulnerability, and assists in containing the incident quickly by implementing reasonable security at the system level. This will also assist in forensic analysis, post-incident review, and continuous process improvement related to cybersecurity strategies. Management of security at the system level within an organization makes it robust in its defense and better prepared to manage and mitigate cybersecurity incidents.

VI. Understanding the cyber kill chain

Understanding the cyber kill chain helps cybersecurity professionals manage incidents effectively. The cyber kill chain describes the different stages of a cyber-attack, from gathering information to extracting data. By knowing this chain, a cybersecurity expert can identify, disrupt, and mitigate the identified threats at each stage by being more active. With this level of understanding comes even better incident response through the abilities of quick cyber threat detection and successful prevention before the actual damage occurs. Understanding the Kill Chain involves framing robust defenses where several preventative strategies target hardening any weak points. This allows custom incident response plans focused around discrete steps on that chain to preserve resources and lessen reaction time. Eventually, through this, a greater understanding of the cyber kill chain will also improve an organization's capability for active prevention and threat management.

VII. Security Architecture and Engineering

Security Architecture and Engineering are complementary to cybersecurity capabilities, reinforcing Incident Management. They aim to design and maintain an effective security structure that can foresee and reduce all kinds of eventualities. Security Architecture involves a secure system design, definition of security controls, and their integration. Engineering focuses on the implementation of such controls and technologies. Combined, the two improve incident management by offering a foundation for prevention, detection, and response. Good security architecture supports vulnerability identification and offers effective incident containment. Engineering ensures proper deployment of security measures to ensure a proactive stance in security. Both disciplines contribute to limiting the impact of incidents in creating a resilient cybersecurity environment through careful design and implementation of security measures.

VIII. Identity and Access Management (IAM)

IAM is very important in cybersecurity operations, and it generally deals with issues of controlling the access of authentic users. It includes the assurance regarding the appropriate, timely access of the valid person to specific systems, information, and applications. IAM supports incident management by detecting and mitigating unwanted access attempts more quickly, mitigating insider risks, and allowing better security practices. It comprises robust authentication, authorization, and privilege management. IAM will also help analyze after an incident to provide insights on compromised access that inform future preventive actions. IAM handles proactive cybersecurity by properly handling identities and access privileges; thus, the incidents of unauthorized activities are minimal, reducing impacts from any security incidents.

IX. Security Awareness Training

Improvement of cybersecurity protection in smart-grid operations is called for, and great significance is attached to Security Awareness Training. Training programs to develop and strengthen practical skills are meant to help operators of all ranks detect such evolving cyber security threats in intelligent grid systems supported by complicated or interconnected information structures and take immediate action in time. The training content is specially crafted, keeping in view the roles and responsibilities of each employee at the workplace, and all should be crystal clear about their contribution to robust cybersecurity measures. The training curriculum identifies phishing attempts, recognizes social engineering tactics, and safely handles sensitive information. Additionally, the training involves technical aspects of cybersecurity that make personnel understand the vulnerabilities of advanced technologies and communication systems inherent in the smart grid. This also includes frequent training sessions of not less than quarterly to enable them to understand recent threats and best practices within the dynamically changing environment that cybersecurity represents. These would be refresher sessions that review key concepts and introduce new strategies and tools for staying ahead of adversaries. Targeted training for groups at very high risk and possessing key systems, control center operators, and system administrators to make them cognizant of various sophisticated attack vectors and their countermeasures. A well-informed and watchful workforce is the best defense one can have against any form of cyber threat. Security Awareness Training creates a culture in which the proactive identification and reporting of threats are encouraged among employees to respond to suspicious activities as soon as possible. It is by such means that the potential for successful cyberattacks is greatly minimized. An organization will be fully

prepared to react rapidly and efficiently once a security incident happens, enhancing the resilience and responsiveness of the smart grid environment. Furthermore, Security Awareness Training is not an event but a process that needs continuous evaluation and refinement. The training needs to change with that, catching modern trends, tactics, and technologies cybercriminals use. Helping organizations keep their employees constantly up to date and informed of the trends increases the chances that they will be able to defend the critical infrastructure of the smart grid against ever-growing and increasingly sophisticated cyber threats.

X. MITRE ATT&CK

ATT&CK, in full, means Adversarial Tactics, Techniques, and Common Knowledge, which is all about building cybersecurity competencies. At the core, the ATT&CK framework enables incident management by providing a structured way to describe and classify cyber threats. ATT&CK offers a common language by cataloging tactics, techniques, and procedures that adversaries use, thus enabling cybersecurity professionals to enhance threat intelligence, detection, and response strategies. Threat intelligence plays an important role in protection and effective response. Collect information from internal logs of IT and OT systems, network traffic, alerts on SIEM and IDS/IPS tools, and feeds from threat intelligence providers, ISACs, and OSINT. Intelligence analysis shall be done with a correlation of internal and external data to find potential threats and vulnerabilities; MITRE ATT&CK will be applied while understanding the attack methods. Risk-scoring techniques prioritize the threats in order of their potential impact, while behavioral analysis uncovers anomalies that could point to a breach. Integration into incident management includes automating responses to identified threats, developing and refining incident response playbooks based on insights from threat intelligence, and sharing information throughout IT, OT, security, and operations via secure communication channels. Moreover, this periodic update, including feedback, means that the relevant threat intelligence that the product provides will be constantly developed with greater perspective and more actual value for all incident management within the framework in general, the resilience of a Smart Grid.

ATT&CK in incident management shall attribute the observed behavior to the technique from threat actor methods and thus might help quickly recognize any potential threat and planned responses toward mitigation. This will be a massive assistance for the security teams on each side, preventing cyber threats from entering through different variants of evolving malware types. Any organization can use the ATT&CK framework defensively by proactive Incident Detection, Containment, and Mitigation.

Approach and Metrics

The Incident response process starts with threats targeting Power Grid assets (Production, Transmission, Distribution, Market, Retail), where decisions need to be identified and executed to permit limited allow

- Awareness completion per segment /
- Resource availability per segment /
- Business Impact Reduction / RTO / RPO

Chapter FIVE

5. Evaluating and validating the framework

Security and integrity are key issues concerning smart grid systems in the light of providing an uninterrupted and reliable electricity supply to homes, businesses, and industries. Increased digitization and interlinking of the power grids make them prone to cyber threats, such as DDoS and Ransomware attacks. The sophistication of the cyber-attack threat is growing daily and is seen as a highly challenging issue these infrastructures face. Such DDoS and Ransomware attacks may bring the grid operations down, leading to citywide power outages with more significant economic and social consequences. Utilities in the power sector should be capable of providing appropriate cybersecurity incident management frameworks for detecting, responding to, and mitigating DDoS and Ransomware attacks.

The depth of analysis in DDoS and ransomware attack vectors and vulnerabilities of smart grid systems is essential to developing effective mitigation strategies. Power utilities can contribute to making the systems resilient against DDoS and Ransomware attacks by addressing the vulnerabilities in generation, transmission, and distribution networks and systems for the reliable operation of smart grid systems. Regular security assessments, continuous monitoring, and collaboration with industry partners are key components of a robust cybersecurity strategy for utilities.

However, power firms are often not in a situation where they cannot invest in heavy cybersecurity solutions owing to financial constraints. Other flaws in their security incident response ecosystem include staffing problems, such as insufficient numbers or being adept at monitoring and responding. Many utilities still use outdated technology and legacy systems not designed to function against modern-time cyber threats, and integrating a new security solution with these working infrastructures always presents enormous challenges. Besides, since power companies are mandated to operate without interruption, adopting security measures that will disrupt operations is limited. The various regulatory binding requirements limit the extent to which security measures can be applied. Power companies must consider resource allocation on a strategic level through a thorough risk assessment to determine the critical assets and allocate resources appropriately. Cost-effective security solutions, including open-source tools, can be implemented to provide substantial protection without significant financial investments.

It finds that spot between security and operational resilience, with adequately designed incident response strategies to continue the most critical assets even in a security breach. The redundant systems and channels ensure continuity of service in case part of the network goes down. The introduction of security controls can also be done phase by phase to reduce the impact on operations and to ease them into autonomous security measures. The presented chapter evaluates the effectiveness of a cybersecurity incident management framework for smart grid systems. Enhanced DDoS and Ransomware Attack Mitigation for Power Utility Smart Grid Systems incorporates quantitative metrics with empirical validation.

- MTTD is the average time to detect the DDoS and Ransomware attack beginning in turn. Apply the methodology of continuous network monitoring with anomaly detection capabilities for quick detection in timely response and mitigation. Implement real-time feeds of threat intelligence to enhance the identification process of known patterns in such attacks. Regular training and simulation exercises are necessary to improve team readiness and detection.
- Mean Time to Respond (MTTR): The average time taken to respond and mitigate a DDoS and Ransomware attack after it has been detected. Fast response minimizes the impact of the attack and restores normal operations faster. This can be achieved by establishing and updating incident response plans relevant to DDoS, applying automated DDoS mitigation tools to deploy countermeasures rapidly, and resourcing required resources such as people and tools for quick incident response that minimizes MTTR accordingly.
- Extent of Damage: This measures the impact of the DDoS and Ransomware attack, including the duration of outages, the number of affected customers, and the economic losses. Quantifying the damage helps in understanding the attack's severity and the mitigation measures' effectiveness. Such strategies include implementing redundancy within critical systems so that operations can continue uninterrupted during an attack, using load balancers that distribute traffic to reduce any single point of failure, and regularly reviewing security measures with updates based on past incidents and emerging threats.

DDoS and Ransomware can breach critical communication and control in the smart grid, causing cascading failures throughout the utility infrastructure. Moreover, prolonged outage or failure of one part could impact contiguous systems, thereby raising the overall impact on operational and customer service. Utilities should use electronic means of providing redundant communications paths and backup systems to avert single-point failures. Critical system segmentations would prevent the spread of an attack to all networks, thereby limiting its impact. Finally, disaster recovery plans should be fully developed to restore operations if the attack caused citywide disruption.

Utility-wide customer satisfaction may witness a massive nosedive following DDoS-induced outages and power disturbances as the eroded confidence eats into a utility's hard-won reputation. Damaged trust makes it difficult to retain clients and generally invites regulatory reviews, leading to more struggles for the utility trying to win customers in. Thus, when utilities manage these incidents, information disclosure is beneficial for maintaining full transparency and timely communication. Showing an estimated timeline for when the facilities may be back is beneficial. Educating the customers on what they can do to protect against cyber threats will go a long way in gaining this trust, reassuring them that this utility is fully committed to resilience and security. Continuous improvement processes based on post-incident reviews may serve to identify the lessons learned and improvements in communication strategies for future incidents. The continuous monitoring of network traffic and system behavior has to be pursued to identify any potential threats and anomalies before widespread incidents occur. Advanced monitoring tools, intrusion detection systems, and security information and event management solutions will help improve threat detection. Integrating threat intelligence feeds informs about emerging threats and attack vectors while deploying AI/ML-based analytics detects abnormal patterns indicative of a potential DDoS attack.

Regular security testing, penetration testing, and vulnerability scanning reveal and fix the weak points in the infrastructure. A good patch management process ensures that all systems and devices are timely security patched and updated. Periodic security audits ensure cybersecurity standards and best practices are followed, while continuous risk management enables them to reassess and prioritize risk according to evolving threats and business impact assessments. This consists of cybersecurity best practices and incident response procedures for all levels of employees, including network security responsibilities. The training of employees on how to spot phishing attempts and social engineering teaches them evasive actions to be taken so that

such attacks do not lead to the compromise of the network. Incident response plans and preparedness include regular tabletop exercises and simulation tests. The training sessions and campaigns instill cybersecurity awareness within the organization through continuous training.

Human mistakes lead to security vulnerabilities and enhance the severity of an attack due to DDoS and Ransomware. These include errors such as weak security settings configuration, failure to install updated patches, and failure to manage security incidents. To address this issue, thorough cybersecurity awareness must be instilled within every employee properly, focusing on why the follow-through on security protocols and best practices matters. Automating routine security tasks minimizes the risk of human error, and strict role-based access control can make employees access no more than required by their roles and responsibilities. Insider threats refer to hostile actions by workers or contractors that may have some privileges to critical systems and information. Examples include intentional misuse of privileges, unauthorized access to sensitive data, or inadvertently sharing credentials. Mitigation strategies include implementing behavioral analytics to detect anomalies in employee behavior that may indicate insider threats, monitoring and auditing privileged access to critical systems and sensitive data and conducting periodic audits of user activity logs and access permissions to detect and prevent insider threats.

In such cases, the attackers will use social engineering to influence employees to reveal sensitive information or take specific actions to perpetrate the attacks. Examples include phishing emails, pretexting over phone calls, or even physical intrusions whereby a person may pretend to be from within legitimate personnel. Mitigation strategies involve training employees in the most common social engineering tactics, how to recognize them, and how to react in case of an incident; 2FA, to minimize the chance of unauthorized access even in cases where credentials have been compromised through social engineering; and social engineering incident response procedures should be part of the overall incident response plan, focusing on immediate reporting and investigation.

Human factors should be mitigated through comprehensive training programs, including periodic training in cybersecurity aspects and human factors, such as recognizing phishing attempts and social engineering tactics. Simulated phishing and tabletop exercises that simulate social engineering attacks will test employee preparedness. Strict policies regarding data handling, access control, and incident reporting can help minimize the possibility of human error and insider threats. Incident response plans should identify and, when possible, list specific human-factor incidents, such as accidental disclosure or insider threat. Secondly, providing mechanisms for employees to report security concerns or incidents anonymously would encourage proactive engagement in security. Monitoring employee adherence to security policies and the effectiveness of the training programs through reducing human-factor security risks is very important.

A holistic approach toward DDoS and Ransomware attacks against utility smart grid systems includes considering all stakeholders. Electricity is used by customers uninterruptedly in daily applications; hence, disruption to supplies can cause dissatisfaction and economic losses. Utilities shall have comprehensive communication plans for informing customers about the causes of outages, estimated time for restoration, and mitigation actions taken. It is very important to establish clear service level agreements that detail compensations or service recovery measures in case of prolonged outages. Implementing redundancy in power distribution and backup systems can minimize the impact of disruptions.

Other considerations aside from these involve regulation and compliance issues. The regulator has indeed specified the reliability and safety of cybersecurity standards in terms of incident response and reporting about power utilities. Non-compliance with these may result in risks of fines, reputational damage, and increased scrutiny over the practice of cybersecurity. The power utilities in Ethiopia must ensure they observe respective industry-specific standards, such as the NERC CIP and IEC62443 standards, among others, promulgated by relevant authorities as part of local regulatory requirements. It would involve regular audits, comprehensive incident reporting required for compliance, and proactive cybersecurity. The engagement is at a reasonable level about the participation of regulatory bodies, where active discussions of challenges regarding cybersecurity, best practices, and policy developments shall be discussed.

It also relates to the public perception and trust in the form of adverse media attention, public outcry, and a loss of confidence in the utility's ability to protect critical infrastructure. Utility communications must be transparent during and after an incident, and timely dissemination of mitigation and lessons learned from the incident must be disseminated. Cybersecurity education for local communities and resiliency commitment build confidence in the general public. Investing in continuous cybersecurity development evidences proactive behavior in terms of protecting the interests of the citizens.

Integrating stakeholder feedback will be essential to implement an integrated approach to cybersecurity. Creating channels for direct stakeholders to provide feedback on cybersecurity practices and the effectiveness of incident response could lead to continuous improvement. Extended cybersecurity awareness programs for internal teams and customers, regulators, and community stakeholders help improve general awareness. Skilling staff in crisis communication for effective communication during a cybersecurity incident reduces misinformation. The risk assessments must be scenario-based, considering the consequences of cybersecurity incidents on various stakeholders to have comprehensive risk management.

Present threat scenarios of DDoS and ransomware attacks, which are prevalent today, and identify how well the framework addresses such cyber threats. Map the DDoS and ransomware scenarios to the various components of the cybersecurity incident management framework and analyze the framework's strengths and weaknesses in combating those threats. Moreover, performance against the threat scenarios above will enable stakeholders to identify what needs further improvement and validation to make the smart grid systems more resilient and secure against cyber-attacks.

5.1 DDoS Attacks Validation Scenario

In becoming both more digital and interconnected, power grids are rapidly becoming more vulnerable to cyber-attacks, which include DDoS. The particular class of cyberattack can disrupt grid operations, thus leading to an outage that would have massive-scale economic and social effects. Having necessary protective features that threaten its security is why all power utilities will have to maintain cybersecurity incident management frameworks to safeguard against this type of threat by analyzing and responding on their own to DDoS attacks and mitigating them on time; hence, based on the below table, the DDoS analysis of different types of attacks may be listed as given below:

Table 6: Types of DDOS Attack

Different type of DDOS attack	Description	Impact	Mitigation
Volumetric Attacks	These attacks aim to consume the network's bandwidth by flooding it with massive traffic. Examples include UDP floods, ICMP floods, and DNS amplification attacks.	The network becomes congested, leading to degraded performance or complete unavailability of network services.	• Rate Limiting: Implement rate limiting on network traffic to control data flow. • Traffic Filtering: Use firewalls and Intrusion Detection/Prevention Systems (IDS/IPS) to filter out malicious traffic.
Protocol Attacks	These attacks exploit weaknesses in network protocols to consume server resources or network equipment; examples include SYN floods, Ping of Death, and Smurf attacks.	The attack causes the targeted devices to become unresponsive, disrupting communication within the smart grid.	• Protocol Hardening: Secure configurations of network protocols and services to resist abuse. • Stateful Firewalls: Deploy firewalls to monitor active connections and detect anomalies. • TCP Connection Management: Use SYN cookies and other techniques to manage TCP connections efficiently.

Application-Layer Attacks	These attacks target specific applications or services, sending requests that appear legitimate but aim to exhaust server resources.	Critical services and applications become overwhelmed, affecting their ability to process legitimate requests.	• Web Application Firewalls (WAFs): Implement WAFs to inspect and filter HTTP/HTTPS traffic. • Behavioural Analysis: Use AI/ML-based solutions to detect and mitigate abnormal traffic patterns. • Redundancy and Load Balancing: Distribute traffic across multiple servers to prevent overload on a single server.

Scenario: DDoS Attack threat scenarios on Power Utility's Smart Grid Systems

Initial Compromise:

The attack begins with threat actors targeting the power utility's network infrastructure, such as routers, switches, Optical transmission network (OTN), and servers, with a large volume of malicious traffic generated from botnets or compromised devices. The sheer volume of incoming requests overwhelms the network infrastructure, causing it to become unresponsive and unable to process legitimate traffic.

Grid Disruption:

With the network infrastructure overwhelmed by the DDoS attack, communication between critical components of the smart grid, such as SCADA systems, control centers, substation systems, and transmission and distribution networks, is disrupted. Utility operators struggle to monitor and manage grid operations effectively without timely access to operational data and control systems, leading to potential service disruptions and power outages.

Impact:

The DDoS attack causes an unprecedented disruption in the operation of power utilities, which may lead to power outages in vast areas and affect thousands of customers. As businesses go into downtime, economic losses result; critical services that depend on electricity, including hospitals, transportation, and communication systems, also shut down.

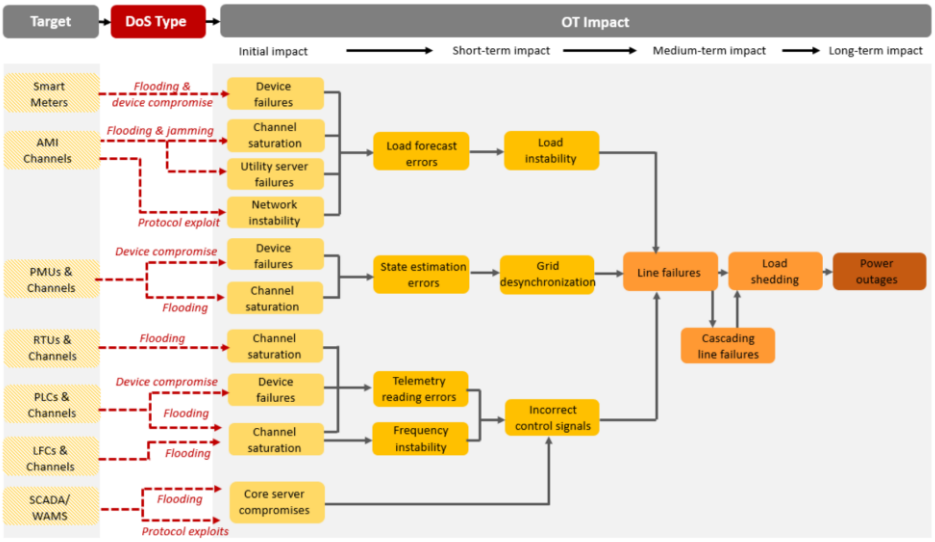
Table 7 : Capabilities sub capabilities DDOS Attacks

Capabilities	Sub Capabilities	DDoS attacks
Smart grid Threat & Risk profile	Incident Response Risk Management	The smart grid systems feed millions of people and power industries; however, integrating physical, operational technologies with IT systems brings numerous security challenges. One of the significant vulnerabilities could be a DoS that may cause great destruction to the smart grid. Though DoS attacks are well-known in IT networks, the smart grid has some unique characteristics that introduce new security challenges. Control the risk by developing a cybersecurity incident management approach: include the scenario in a Risk Matrix and develop strategic and operational responses. Part of the threat profiling of DDoS/DoS could be depicted in a Threat model diagram/Risk heat map. The impact of these attacks can range from disruption of external IT resources and customer services to communication and power outages, including failure of smart meters and control center equipment within the grid network. This table shows where DoS and DDoS can be targeted.

Threat Actors	Corporate	Generation	Trading	Control Center	Transmission	Distribution	Smart Grid	Retail
Nation States	•Sensitive data	•Disrupt production for extortion / political gain, influence, and cyberwarfare	•Disruption for political gain	•Disrupt critical infrastructure through gaining control of EMS/DMS (cyberwarfare)	•Disrupt critical infrastructure through cyber or physical attack	•Disrupt critical infrastructure through cyber or physical attack	•Disrupt smart-grid for political gain / cyberwarfare	•Disrupt consumer IoT smart-device footprint for political gain / cyberwarfare
	for extortion/		•Manipulation of trading position				•Steal intellectual property (technical architecture)	
	unauthorized release		•Regional market manipulation					
	•Economic espionage							
Hacktivist	•Unauthorized disclosure of sensitive information	•Expose sensitive environmental information	•Disrupt trading and financial performance to influence / damage	•Disrupt critical infrastructure through cyber or physical attack	•Disrupt critical infrastructure through cyber or physical attack	•Disrupt critical infrastructure through cyber or physical attack	•Disrupt smart meters to damage revenue	•Fake billing to damage revenue
		•Disrupt production (e.g. fossil fuel)						•Unauthorized disclosure of PII
Cyber Criminals	•Steal PII data	•Disrupt production for extortion / economic gain (e.g. ransomware)	•Insider trading	•Ransomware attacks on critical control systems for financial extortion	•Disrupt production for extortion / economic gain (e.g. ransomware)	•Disrupt production for extortion / economic gain (e.g. ransomware)	•Meter manipulation for financial gain	•Fake billing
	from employees		•Front-running for					•Compromise smart devices for credential theft
	•Steal credentials		trading position					
	•Ransomware		•Trading manipulation					
Insider	•Unauthorized disclosure of sensitive information	•Malicious misuse	•Insider trading for financial gains	•Malicious misuse	•Malicious misuse	•Malicious misuse	•Malicious misuse of smart-grid infrastructure	•Disrupt / misuse commercial customer energy platforms
	•Inside fraud	•Disruption / destruction of operational assets	•Misuse of trading systems for gain or harm	•Disruption / destruction of operational assets	•Disruption / destruction of operational assets	•Disruption / destruction of operational assets		

Table Smart grid threat profiling

The risk matrix show that all power utilities are targeted and critical infrastructure can be disrupt as shown in the diagram.

		 Figure Smart grid DoS attack targets and possible impact events [40]
Cybersecurity Incident Management Strategy and Governance	Governance Structure	The DDoS and DoS threat scenario is managed within the cybersecurity incident management governance structure, mobilizing key stakeholders in case this event occurs. A governance structure at a strategic level will allow senior management and executives to understand, through a series of statuses, periodic simulation results, risks, and reporting, whether the organization and, more importantly, the smart grid segment is ready. At the operation level, governance is described as following through on all the activities at the operational level, including the execution of the cybersecurity program, exercises in simulation, and transformation of key segments.
	Incident Management Strategy & Program	The incident management strategy and program are defined using NIST standards to handle DDoS and DoS attacks in the grid: Identity, Protect and Detect, Response, and Recovery. The scenario and Risk involved are integrated into the cybersecurity strategy with a mitigation plan - Integrating AntiDDoS to detect and mitigate attacks from the Internet. - Integrating Internal AntiDDoS attacks for internal IT and OT Networks. - Integrating the threat scenario into Incident response exercise, simulation, management, and measurement to allow the power utilities to be ready and limit the impact in the Power grid.
	Incident Management Policy	Policies that provide incident management of smart grid systems are responses against DDoS. This provides clear explanation through policies regarding procedures and roles regarding responses to critical events with very well-coordinated escalations paths for these situations, making the enabling power utilities appropriate assessment in making decisions for its incidents, concerning policies related to valid incident management.

	Standard Operation Procedures (SOPs)	A specific standard operating procedure for DDoS attack is integrated into new power grid assets affected, evolving the current system. The procedure includes process handling, standard solutions, and an architecture framework to technically standardize the solution from providers and procurement. It integrates the requirements into the BID process, training, and awareness for all parties to understand their role when this event occurs.
Incident Management Stakeholder	Senior Executive Management	Senior Executive Management is involved, understands the risk of a DDoS attack, its impact, and mitigation plans, and is ready to play its role if this threat scenario happens.
	Legal Team	The legal team understands the risk and legal impact that have already been identified and threatened based on the impacted segment, which could be customer service from exposure over the internet or grid customers if one part of the network is out of service.
	Crisis Management Team	A crisis management plan is invoked for a business-critical system or service in case of complete unavailability, which critically impacts operational activities.
	Incident Response Manager	The incident manager identified the DDoS threat. The response has started, and it includes resources and the appropriate team.
	Communication Team	Various lines of communication have been established to inform customers, regions, and governments about the grid's perimeter.
Real-Time Monitoring	Visibility	The power grid infrastructure is monitored in real-time to ensure complete visibility. This monitoring team utilizes robust asset management solutions that empower the security teams to combat DDoS attacks on smart grid systems. The team uses asset discovery tools to maintain an accurate inventory of all the devices connected to the grid, including critical infrastructure components and IoT devices. This helps in a deep understanding of the landscape of PowerGrid. The data will be fed from the asset management to the network visibility tools to discover possible attack vectors and prioritize the protective measures. By prioritizing visibility through asset management, security teams, and power grid operators will have effective and efficient detection and response related to DDoS attacks, ensuring operations within the sphere of smart grid resilience for non-stop functionality. An overview of all associated assets-whether OT, IT, or IoT, requires frequent monitoring for early detection of changing critical cyber or operations risk.

	Detection	The IT/OT security team has been experiencing weird increases in network traffic from various IP addresses. Anything resembling a DDoS attack is closely watched, mainly spikes in traffic or unusual patterns. It uses intrusion detection systems and anomaly detection tools that send alerts, if necessary, to detect suspicious traffic. They are also updating themselves concerning the newest DDoS threats and attack vectors, as those threats are regularly integrated into defensive capabilities with threat intelligence feeds. As this will serve as a proactive means that facilitate their activity for prioritization, fast identification helps concentrate efforts toward any event of smart grid systems arising from these attacks. Consequently, this avoids disturbances and disruptions within the service and ensures the operation of the pertinent infrastructures continues.
	Analysis	The first thing to mitigate a DDoS attack on smart grid systems is a preliminary analysis done by the security team, which uses logs of network traffic and system events to identify the set of affected devices and infrastructure elements, review features of an attack with its duration to identify the severity of the attack and possible consequences for the smart grid operations. Besides that, the team is coordinating with the internal power utility teams and their external partners to gather more information and insight regarding the DDoS attack. In this context, security teams and operators of the power grid will be able to focus on prioritization in terms of responding correctly by doing a thorough initial analysis to reduce the impact of the attack on smart grid systems.
Incident Response Operation Team	Containment	Cybersecurity incident response immediately leaps into action to identify a DDoS attack to contain its effect and prevent further disruption of their services. The team will configure their network infrastructure immediately to implement traffic filtering rules, blocking traffic flow coming from identified malicious IP addresses. They can also implement rate-limiting measures that limit incoming traffic so that genuine users have unhindered access to the service. The team performs isolation of affected systems and segments within the smart grid network to contain the attack; this helps prevent the DDoS attack from spreading. They implement very strict access controls, firewall rules, and network segmentation, limiting unauthorized communications and thereby limiting the impact on critical infrastructure. It works with the security team, alongside ISPs and DDoS mitigation providers, by merging resources and experiences to ensure minimum disruption of the smart grid operation while effectively containing the DDoS attack.
	Investigation	The incident response team for cybersecurity deeply examines root causality and the damage caused by the DDoS attack in the smart grid systems. They employ advanced digital forensics tools and methodologies to closely analyze network traffic logs, system events data, and other digital artifacts related to the attack. The aim is to find out what specifically were the vulnerabilities or specifically which misconfiguration the attackers had utilized and also the sophistication level of the attack. In cooperation with the in-house and external teams, they collect further intelligence and attribution in order to gain a full understanding of the origins and motivations of this particular attack. They document all their findings and insights in great detail, in order to inform future response efforts and enhance defenses against future DDoS

		attacks. By documenting lessons learned and strengthening their defensive posture, they bolster the resilience of the smart grid infrastructure against potential cyber threats.
	Eradication	After containment and investigation into the DDoS attack, the work of a cybersecurity response team focuses on eradicating it from the root so that such situations are not repeated. The cybersecurity incident response team deeply analyzes the attackers' used attack vectors and vulnerabilities. That would mean network logs analysis, application traffic patterns analysis, and finding those weak points in their infrastructure or OT network utilized by them. Based on the findings, the smart grid security monitoring team takes further steps, such as applying patches, updates, or configuration changes to enhance the resistance level in case of the same type of attack in the future. Further, the response team takes eradication actions to remove all signs of the DDoS attack from smart grid systems. Security patches, updates, and configuration changes are utilized to eradicate the vulnerabilities used by the attackers. These could include endpoint security solution implementations and automated remediation tools that scan and sanitize infected devices. It could involve rigorous system checks and validation to ensure the malicious component has been eradicated. In so doing, the team would further liaise with internal teams and external partners to verify eradication measures and eventual safe states of affected systems. These proactive steps will enhance the smart grid infrastructure against future cyber-attacks.
	Recovery	Once the DDoS attack is mitigated and vulnerabilities fixed, the team restores the smart grid systems to normal operation. Recovery commences with the cybersecurity team using backup and restoration procedures to recover encrypted data and restore the affected systems to a pre-incident state. In an attempt to reduce downtimes and make sure there is continuity of the important operations in the grid, they started implementing redundant infrastructure with failovers. Systems are verified and tested after recovery for their integrity and functionality. In all these stages, stakeholders are briefed about communications regarding the progress of recovery efforts and reassured through transparent communication on the security posture. This is where the cybersecurity team will gradually lift traffic filtering and rate limiting while constantly observing the network for renewed attack activity. They further restore any services or systems that may have been temporarily shut down during the attack and ensure that all is working as it should be. This broad approach ensures speedy and effective smart grid system recovery after the DDoS attack.
	Improvement	Once the incident has been contained, the team continues taking advantage of it to enhance their resilience to such DDoS attacks through continuous improvement strategies. First, they go through an exhaustive after-action review of their efforts in response, carefully considering strengths and weaknesses that may have emanated from their systems' security. The organization secures information through lessons learned about updating its Incident Response plan, improving the organization's capabilities related to monitoring, investing in better protections against future DDoS

		attacks, updating security policies, and providing practical recommendations developed on the lessons they learned from this experience about enhanced access control and better awareness/preparation programs for employees. It develops its incident response plans through regular tabletop exercises and testing, including simulated DDoS attacks. It shares knowledge and promotes team collaboration in proactive risk management and information exchange. The team works to improve its defenses and responses, raising resilience against DDoS attacks and other cybersecurity threats.
	Communication	Cybersecurity incident management should communicate well with the institution's stakeholders throughout the process. The cybersecurity team keeps stakeholders updated on the current state of the incident through regular status reports about mitigation progress, expected downtime, and service adjustments. In this regard, public statements are released to reassure customers, partners, and the relevant regulatory bodies that things are controlled and managed efficiently. These statements identify the actions taken to contain the disruption while adding to the defenses against the attack. A cybersecurity team reassures these stakeholders with frank openness. It demonstrates that their commitment is deep to the resolution of the incident and the protection of the interests of the organization.
Incident management Technology capability & Platform	SIEM	They collect, collate, and analyze the log data received from network devices, servers, and applications through the SIEM systems. They might detect patterns when there is a DDoS attack that defines it as anomalous traffic to indicate in various ways to the security personnel. It can automatically trigger an action with the help of such detection conditions either by blocking the problematic IP addresses or changing configuration settings in the firewall, hence minimizing the scope of the active attack. Reports are also provided, which contain the nature of the attack, systems affected, and the response taken that might be used to get a post-incident analysis to be viable and compliant with compliance regulations.
	UEBA	UEBA solutions are currently attempting to find DDoS-attack-associated anomalous activities based on user and entity behavior. It will include a lot of attempts at logging in, or data transfer may show some atypical pattern. Additionally, specific details about the attack, such as compromised accounts or systems that have taken part in the attack, will also be provided by the UEBA, which would facilitate the creation of a point-to-point response strategy by the security team. By refining baseline behavior profiles, UEBA can also improve the system's ability to identify and respond to future DDoS attacks.
	Ticketing & Case Management	Ticketing systems help the security teams prioritize tasks and organize their work so that they can coordinate with each other by implementing mitigation measures and assigning responsibilities. Case management tools extend this collaboration by allowing team members to document response actions, share information, and communicate with stakeholders throughout the incident lifecycle.

	Threat Vulnerability management	With the help of a vulnerability management solution, an organization can detect and fix potential security gaps that hackers could exploit to perform a DDoS attack. This reduces the possibility of further attacks and the chances of an organization being exposed. In case of a DDoS attack, it may highlight to these tools the potential underlying vulnerabilities or misconfigurations that could have led to such an incident so prompt and efficient remediation may be made.
	SOAR	SOAR platforms automate incident response workflows, thus providing an organization with the capability for real-time detection, analysis, and containment of DDoS attacks. They use machine learning and AI algorithms to spot malicious traffic patterns and behavior that the security teams respond to. The key benefit of having a SOAR platform, generally speaking, is that it allows organizing response actions across disparate security tools and systems for the members of the cybersecurity response team. In such a situation, mitigation becomes swifter and smoother, with less time consumed and less effort needed to contain an attack. They can trigger the response action by the platform's automation capability to block traffic or isolate compromised devices using predefinition. Furthermore, the SOAR platforms afford power utilities a single, uniform view of their security posture, from which they can contextualize any likely vulnerability and address it way ahead. This helps the power utility avoid emerging threats while reducing the risk of cyberattacks.
	Detection/Response sensors	Only a proper tracking of regular traffic flow could detect anomalies and vulnerabilities. That kind of monitoring may be done only through specialized tools for network traffic in the form of NIDS, WAFs, DDoS mitigation appliances, for detection of patterns of attacks in real-time with matching countermeasures. These aforementioned monitoring and other respective systems allow monitoring passively and mirrored traffic with no interference or load on critical processes, alarms, and generation of unwanted traffic. Visualizing the whole operational network hence allows users to identify anomalies and incidents rapidly. Advanced cyber threats and OT network behavior anomalies can be identified and disrupted with a good time to detect them. It provides users with threat information through Yara rules, packet rules, STIX indicators, threat definitions, and vulnerability signatures. It gives an accurate asset inventory of all communicating devices continuously on OT and IoT networks.
	Reporting	Reporting tools would provide consolidated, aggregated information from their varied security systems, generating detailed post-incident incident reports of detected DDoS strikes, including start time, elapsed duration, all impact on upstream services, and response measures among basic measures undertaken. These also provide the basis for post-event review, compliance reporting, and executive communications.
	Simulation Exercise & Training Platform	The Simulation Exercise & Training Platform provides the customer with an environment that is virtual and simulates the actual network and SOC setup, security tools, topology, typical and malicious traffic of a power utilities company. It emulates live scenarios of cyber-attacks which trainees read in books but do not find anywhere to try practically; thus, this offers very effective hands-on training as opposed to conventional means. Packages also cover Incident Response training,

		Penetration Testing, ICS Security, and individual advanced training. Each package contains a few simulated attack scenarios, including SQL injection, DDoS attacks, ransomware, phishing, data exfiltration, and many more. These diverse scenarios provide hard-hitting, high-pressure training that enhances personnel performance substantially.
Incidence Response Process	Incident Response Procedures	Incident Response Procedure The incident response procedures detail step by step how security incidents, including DDoS attacks, are to be responded to. Implementation includes **Identification**: Define a clear symptom and indication of a DDoS attack, such as sudden spikes or abnormal traffic patterns. **Containment**: This will include an explanation of the procedure needed to isolate the infected systems or network segments and stop the attack from spreading further. **Eradication**: Explain what would be done to identify the source of the DDoS attack through log analysis, and then eradicate the problem and apply remediation. **Recovery**: The steps and procedures that will clearly restore all the services and systems concerned to normal must be identified, including the rollback procedure where necessary. **Improvement**: Include mechanisms for post-incident activity review and lessons learned to be assimilated into the continual improvement of incident response capability.
	Incident Response Playbook	**Incident Response Playbook, or IR Playbook, is a predefined set of response actions and** decision trees for DDoS attacks. **Detection:** Establish automated detection rules and thresholds for identifying DDoS attack patterns. Specify pre-defined response actions to mitigate DDoS attacks, such as filtering traffic, rate limiting, or enabling DDoS protection services. Communication: Describe various plans for notice communication to concerned stakeholders, involving internal teams/management, and to customers/regulatory authorities where necessary. Documentation: Include templates for documenting incident details, response actions taken, and post-incident analysis.

	Recovery Plan Procedure	The Recovery Plan Procedure describes the step-by-step procedure that must be followed to return to a normal state those attacked services and systems after a DDoS attack. The RPP is composed of Service Restoration: Describe the ongoing process of restoring affected services to the substation, ensuring critical systems come first. Data Recovery: Describe the processes and actions necessary for data and configurations lost due to the attack, specifying any data backups or replication. Testing: Include a procedure for testing the services that have been restored to work as expected after the attack or intrusion and if they are resistant to future attacks. Communications: Describe the strategy that would be employed to communicate with stakeholders regarding the status of the recovery efforts and estimated downtime.
	SIMULATION EXERCISE	Simulation exercises involve conducting realistic scenarios in a controlled environment to practice incident response procedures and test the effectiveness of response capabilities. Scenario Design: Explain a design of the DDoS attack scenarios, considering conditions of the Power Utilities environment about attack vectors, an overview of the impact on services, and actions taken to respond. Execution: Execute tabletop exercises or simulated drills involving cross-functional teams to simulate response to DDoS attacks and evaluate coordination and communication. The simulations need to be done both internally inside and externally. Debriefing: Conduct a post-exercise debriefing to review performance, identify areas for improvement, and update incident response procedures and playbooks.
Incident Response Response Team support	IT / OT Support	The support team in engaged during simulation and the actual event and in this DDoS attack, they have to Be in support and coordination with the right team impacted: application and service owner, IT expert, and network, and engage the operational based on the procedure and they knowledge on the IT or OT environment (Production Manager, CC manager)
External Partner	State cyber agency	The external parties where involvement is necessary to support during containment (Using Traffic Filtering, traffic scrubbing, anycast routing) and recovery: Service restoration, post-incident analysis, and customer support: - External actions from ISP with the purpose to stop the attack - from AntiDDoS provider - An external action for the OTN network to patch the vulnerabilities.
	IT Technology provider	
	OT Technology Provider	
Infrastructure Monitored	Power Generation systems	

	Power Transmission systems	
	National Load Dispatch Centre	
	Power Distribution systems	
	AMI	
	Enterprise IT systems	

Cybersecurity Capabilities supporting incident management	Asset Management	It should be helpful in managing cybersecurity incidents that occur in smart grid systems when DDoS attacks are perpetrated by identifying critical assets, prioritizing protection measures, and implementing segmentation strategies. This provides visibility into which assets are affected, helping respond as quickly as possible, informs post-attack restoration efforts to further enhance grid resilience and security posture.
	Network security management	Because many protocols face DDoS attacks, good network security management during those attacks is most important in the smart grid. It involves installing intrusion detection, firewall systems, and traffic analysis detection tools to combat possible attack effects. While monitoring network traffic to implement robust security measures, protection will involve important infrastructure, ensuring grids are reliable in becoming resilient against every cyber threat.
	System security management	System security management enhances smart grid cybersecurity during DDoS attacks by securing critical systems and infrastructure. It involves implementing access controls, patch management, and encryption to prevent unauthorized access and data breaches. By fortifying system defence, organizations can mitigate the impact of DDoS attacks and maintain grid functionality and integrity.
	Security architecture and engineering	Designing and implementing resiliency in security architecture and engineering contributes to cybersecurity hardening in smart grids against DDoS attacks. These include strong network segregation policies that provide redundancy and failovers against the DDoS menace. Security integrated into system architecture enhances grid resilience and reduces disruptions.
	Security Awareness and training	Security awareness and training are vital for smart grid cybersecurity during DDoS attacks. Educating employees and stakeholders about cybersecurity best practices enhances their ability to recognize and respond to potential threats. By fostering a culture of vigilance and accountability, organizations can mitigate the impact of DDoS attacks and strengthen overall grid security posture.

	Zero Trust strategy	The Zero-Trust approach empowers smart grid cybersecurity during DDoS attacks by assuming threats lie inside and outside the network perimeter. This strategy reduces the attack surface, confining the spread of DDoS threats via strict access controls, continuous authentication, and micro-segmentation.
	Endpoint protection strategy management	Endpoint protection strategy management enhances smart grid cybersecurity against DDoS attacks by protecting devices that try to access the network. This involves deployment techniques such as antivirus software, intrusion detection systems, and endpoint encryption that find and attempt to prevent malware and other vulnerabilities. In protecting the endpoint, the organization will minimize the threat of a DDoS to maintain the integrity of the grid.
	Understanding the cyber kill chain	The cyber kill chain helps smart grid cybersecurity understand the different stages of an attack, right from reconnaissance to exfiltration in DDoS attacks. Analysis of attack patterns allows organizations to detect and disrupt DDoS campaigns earlier, reducing the impact of such attacks and strengthening incident response strategies that would protect grid infrastructures and operations.
	Identity and access management	IAM is crucial in the smart grid for cybersecurity at the different levels of DDoS attacks because it ensures that no unauthorized user can access critical systems. IAM solutions provide strong authentication, manage user privileges, and detect anomalies to minimize unauthorized access and reduce most DDoS threats on grid operations.
	MITRE ATTACK	The MITRE ATT&CK framework helps reinforce cybersecurity in smart power grid systems to fight these DDoS attacks much more effectively by means of a clear indication of consensus from tactics' knowledge and Techniques, which must have been perpetrated. Mapping in practical DDoS-attack scenarios shows what techniques are included under ATT&CK, facilitating more profound capabilities enhancement and threat detection to improve response processes and mitigate strategies, resulting in the reliability improvement of smart grid systems against serious Cyber threats.

5.2 Ransomware Scenario Validation Scenario

Rapid growth and integration of digital technologies in smart grids make cyber threats grow, particularly those caused by ransomware attacks. A ransomware attack encrypts essential data and seeks a ransom for decryption, which may eventually compromise the functionality and security of the infrastructure of smart grids. Thus, the assessment and confirmation of ransomware threat scenarios should be considered with an appropriate cybersecurity incident management framework in smart grid systems. This paper critically analyzes the ransomware threat scenarios by mapping them to different components of the cybersecurity incident management framework: prevention, detection, response, and recovery strategies important in the mitigation process for the impacts a ransomware attack would have on Smart Grid operations.

Power utilities ensure reliable delivery of electricity to households, businesses, and industries. Since infrastructure has gone digital, smart grid systems are not an addition to modern utility operations but have become necessary components. However, digital transformation increases specific cybersecurity challenges, and ransomware threats are one such problem that threatens smart grid systems. This might be the case with utilities that will implement solid cybersecurity incident management frameworks that would quickly detect, respond to, and recover from ransomware incidents to provide firm assurances of stability and security in the power grid.

Scenario: Ransomware Attack on Power Utilities' Smart Grid Systems

Initial Compromise:

The attack begins with a targeted phishing campaign against power utility company employees. An unsuspecting employee receives an email from a trusted source within the company or a supplier. The email contains a malicious attachment disguised as a document related to grid maintenance or an invoice. By opening the attachment, the employee inadvertently executes malware that exploits a published vulnerability in the utility's network infrastructure, thus gaining the attacker an initial foothold.

Reconnaissance:

The attacker does his or her reconnaissance, trying to uncover some of the important parts of the smart grid system, using network topology to understand and identify where there is either a SCADA system, substation, or a major infrastructure within their centers of distribution.

Escalation and Lateral Movement:

Privileges are escalated, and the attacker moves laterally in the network to reach the control systems and IoT devices connected to the grid. They then leverage poor access controls, unpatched systems, or default credentials to move across the network without detection.

Ransomware Deployment:

Once inside the critical infrastructure, the attacker deploys ransomware designed to encrypt data on SCADA systems, control servers, and other operational technology devices. The ransomware spreads rapidly, encrypting files and disrupting grid operations.

Impact:

Eventually, the ransomware will infect the grid, affecting transformation, transmission, and distribution, leading to blackouts and affecting thousands of customers. The utility operators, who have been denied access to essential systems and data insights, will attempt to retain control over the grid and try to restore the utility services. Thus, the financial impact is severe and generally includes massive losses caused by revenue loss, regulatory penalties, and costs for remediation and recovery for the utility. Piling on top of this is reputational damage: consumers suffer from prolonged outages and lose faith in utilities to protect their energy supply.

Table 8 : Capabilities Sub Capabilities Ransomware attack

Capabilities	Sub Capabilities	Ransomware attack
Risk Management	Incident Response Risk Management	Since ransomware attacks are common in the current digital space, they have now been included in threat profiling and risk impact assessments. These can have profound implications for IT and OT resources; hence, these potential risks must be recognized. For IT resources, ransomware attacks may compromise customer data, billing information, and finance information in retail and corporate settings. This can be catastrophic for organizations because loss of this kind of information results in financial loss, damage to reputation, and sometimes even litigation. Therefore, it becomes important for organizations to ensure their cybersecurity is proper to prevent attacks on IT resources. Ransomware incidents are also targeted against OT resources, such as control center systems that generate, transmit, and distribute energy. Attacks on the Advanced Metering Infrastructure-AMI platform, SCADA/EMS systems on production, and other critical infrastructure lead to considerable disruptions to the energy supply chain and cause extensive damage. This could have catastrophic consequences on the economy and society in general. Thus, it is prudent that such systems are well protected against such attacks. The following table shows the profiling of threats with examples per segment in a ransomware scenario.

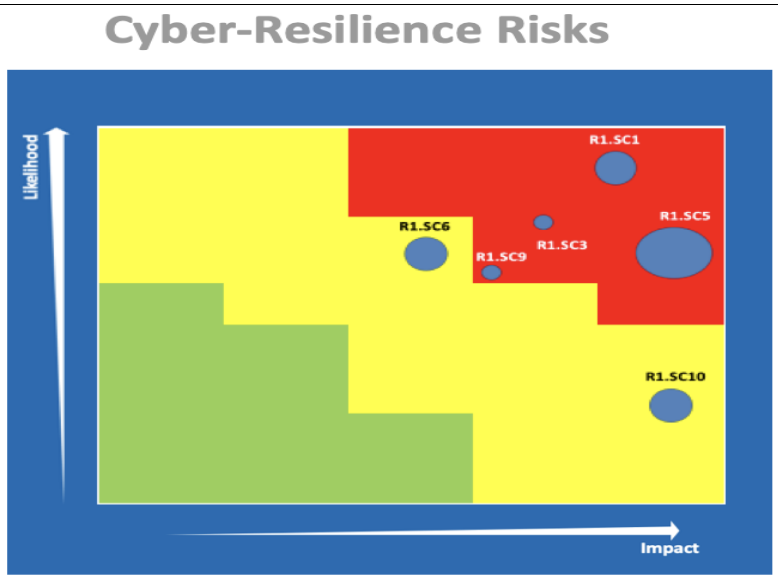
Incident Response risk bases scenario in Smartgrid

Threat Actors	Corporate	Generation	Trading	Control Center	Transmission	Distribution	Smart Grid	Retail
Nation States	•Sensitive data	•Disrupt production for extortion / political gain, influence, and cyberwarfare	•Disruption for political gain	•Disrupt critical infrastructure through gaining control of EMS/DMS (cyberwarfare)	•Disrupt critical infrastructure through cyber or physical attack	•Disrupt critical infrastructure through cyber or physical attack	•Disrupt smart-grid for political gain / cyberwarfare	•Disrupt consumer IoT smart-device footprint for political gain / cyberwarfare
	for extortion/		•Manipulation of trading position				•Steal intellectual property (technical architecture)	
	unauthorized release		•Regional market manipulation					
	•Economic espionage							
Hacktivist	•Unauthorized disclosure of sensitive information	•Expose sensitive environmental information	•Disrupt trading and financial performance to influence / damage	•Disrupt critical infrastructure through cyber or physical attack	•Disrupt critical infrastructure through cyber or physical attack	•Disrupt critical infrastructure through cyber or physical attack	•Disrupt smart meters to damage revenue	•Fake billing to damage revenue
		•Disrupt production (e.g. fossil fuel)						•Unauthorized disclosure of PII
Cyber Criminals	•Steal PII data	•Disrupt production for extortion / economic gain (e.g. ransomware)	•Insider trading	•Ransomware attacks on critical control systems for financial extortion	•Disrupt production for extortion / economic gain (e.g. ransomware)	•Disrupt production for extortion / economic gain (e.g. ransomware)	•Meter manipulation for financial gain	•Fake billing
	from employees		•Front-running for					•Compromise smart devices for credential theft
	•Steal credentials		trading position					
	•Ransomware		•Trading manipulation					
Insider	•Unauthorized disclosure of sensitive information	•Malicious misuse	•Insider trading for financial gains	•Malicious misuse	•Malicious misuse	•Malicious misuse	•Malicious misuse of smart-grid infrastructure	•Disrupt / misuse commercial customer energy platforms
	•Inside fraud	•Disruption / destruction of operational assets	•Misuse of trading systems for gain or harm	•Disruption / destruction of operational assets	•Disruption / destruction of operational assets	•Disruption / destruction of operational assets		

Table Ransomware Threat profiling

This scenario is covered in a risk-based incident management approach, which integrates it into the Risk Matrix and handles it from a strategic and operational point of view.

This example can be considered a risk scenario, and if this fear event happens, it can impact the entire value chain.



Risk Level	Risk category
R1.SC1	Market Cyber-resilience Attack
R1.SC3	TSO Cyber-resilience Attack
R1.SC5	Dispatching Center global collapse

Figure Risk heatmap

The ransomware attack could disrupt the normal operations of the power grid, causing blackouts or brownouts in affected areas.

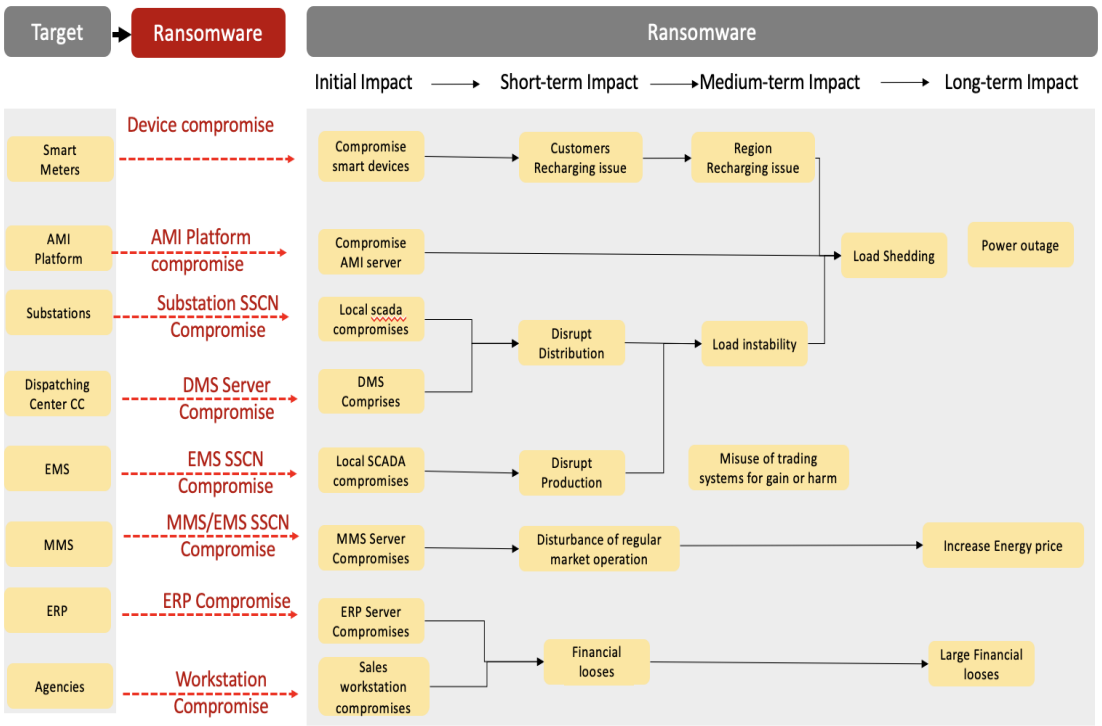


Figure Ransomware attack targets and possible impact events

Cybersecurity Incident Management Strategy and Governance	Governance Structure	The management of a ransomware threat is incorporated into the cybersecurity incident management governance structure, which involves key stakeholders at both strategic and operational levels. At the strategic level, the governance allows senior management and executives to stay informed about the status and results of periodic simulations and reports to assess readiness in the power utilities and smart grid segment. At the operational level, the governance outlines the follow-up of all operational activities, such as programs, simulations, exercises, and transformations, that the key segment should undertake during a ransomware attack.
	Incident Management Strategy & Program	The management strategy for cybersecurity incidents identifies potential scenarios and associated risks. Also, mitigation planning details the adoption of a program for handling the situation in question about ransomware attacks against the grid. To handle the attack on the grid using ransomware, guidelines shall be accorded by adopting criteria according to NIST through identifying, protecting, detecting, responding, and recovering from cyber incidents. This program incorporates scenario and risk management into the cybersecurity strategy, including network segmentation, endpoint protection, backup and recovery, regulatory compliance, training/awareness, and incident response management. By preparing for this type of scenario in particular, the organization will be much more capable of responding and hopefully mitigating some of the impacts that may have resulted from the ransomware attack.
	Incident Management Policy	Power utilities, or more specifically, power grid operators, must develop a proper incident management policy dedicated to ransomware. The policy shall cover all aspects, including preparation, detection, containment, eradication, recovery, and lessons learned. The Cybersecurity Incident Management Policy must also address strategies and programs like network segmentation, backup, regulatory compliance, training, and response planning.
	Standard Operation Procedures (SOPs)	The latest power grid technology comes with a set protocol for dealing with ransomware attacks. This protocol covers all aspects of the attack, including how to handle it, the standard solutions to be used, and the architectural framework necessary to combat it. The solutions are standardized from the providers to the

		procurement process, and the requirements are integrated into the BID process. All participants are trained and made aware of their roles during an attack.
Incident Management Stakeholder	Senior Executive Management	Senior Executive Management is involved, understands the risk of a ransomware attack, its impact, mitigation, and plan, and is ready to play its role if this scenario happens. This scenario is common, and Senior executives need to be ready when it happens.
	Legal Team	The legal team understands the risk and legal impact, which they have already identified and threatened based on the impacted segment, which could be customer service, disruption of operation, financial losses, Data Theft, public safety concerns, or reputation Damage. They need to anticipate the legal framework to be ready when this scenario happens.
	Crisis Management Team	Ransomware attacks are often considered crises because of the public exposure of the attack. The crisis management team needs to be aware and prepared to handle it.
	Incident Response Manager	The incident Manager identified the ransomware Threat, organized the response process, and Led the response by mobilizing the right capabilities and organization.
	Communication Team	Communication has already identified channel and notification mechanisms based on the impacted Grid perimeter (customer, region, government) Communication must be mastered to reconsolidate and reverse the turn of events in the company's direction, showing that it put the necessary means in place to counteract the attack.
	Visibility	This is imperative in real-time monitoring of the power grid infrastructure so that nothing is left unseen. A team operating within a smart grid can be empowered in combating ransomware attacks on its systems by the use of robust asset management solutions. Asset discovery tools keep inventory on all devices connected with the grid, critical infrastructure components, and IoT devices. Understanding the power grid landscape with clarity, the integration of asset management data with network

Real-Time Monitoring		visibility tools will help in the prioritization of appropriate protective measures against the found potential attack vectors. Such prioritization of visibility will make it quite easier to enable security teams and power grid operators to detect and respond to ransomware attacks efficiently, ensuring resilient, continuous smart grid operations. Continuous monitoring of all the connected assets-OT, IT, and IoT devices-along with the detection of changes that may raise the associated cyber and operational risks, form the very foundation of assuring such risk reduction.
	Detection	The security team has also noted an unexpected increase in traffic from unknown sources. Further, they have noticed very unusual activities on the workstations and across the network, suspicious file changes, system scans, and attempts to disable or remove processes and services. Besides, the performers have tried to delete system backups, recovery partitions, and shadow copies in order to make data recovery difficult or impossible. The team continuously monitors for ransomware attacks using intrusion detection systems and anomaly detection tools, which set tarrings on the activities deemed anomalous. The team stays updated about brand new ransomware threats and attack methods by adding threat intelligence feeds to their mechanisms of defense. This proactive approach enables them to channelize their efforts in the right direction and spot ransomware attacks on smart grid systems with seamlessness. By doing this, they minimize disruption and ensure that critical infrastructure remains in service.
	Analysis	The security team approaches the ransomware attack in the smart grid through a preliminary assessment. The security team identifies affected infrastructure and devices using system event data and network traffic logs. Scrutinizing the nature of the attack and the duration will let the security team know the intensity of the situation and the consequences to smart grid operations. Also, they collaborate intensively with internal power utility teams and external partners for further information and insight into the ransomware attack.
	Containment	The security team immediately isolates the infected systems or network segments, disables the compromised accounts, and revokes privileged access in order to prevent ransomware proliferation. They reduce the impact on critical infrastructure by isolating affected systems and parts of the smart grid network through network segmentation. All access controls, firewall rules, and network segmentation are

		employed to block illegitimate communications and data theft. It uses endpoint isolation, automatic network quarantining, or other automated responses in that case to arrest the ransomware and limit the impact on CI. Therefore, security teams are working in great coordination with other teams internally and external partners where top priorities of security posture are focused on how to contain an attack and reduce impact on the grid.
Incident Response Operation Team	Investigation	The incident response cybersecurity team does an in-depth analysis of the ransomware variant for behavior, methods of encryption, and any potential weaknesses. They identify how the ransomware entered the network and identify potential vulnerabilities or misconfigurations that may have led to this attack. To support potential law enforcement investigations, evidence is gathered in the form of log data for forensic analysis. They use digital forensics on a deep basis to understand what really happened: the root cause, extent of the damage, and tactics used by the attackers. This will help them pinpoint which security control vulnerabilities, misconfigurations, or insider threats enabled the attack. The team works with law enforcement agencies, industry partners, and internal stakeholders in collecting intelligence and sharing its findings. They document lessons learned and make recommendations that can be taken to further improve incident response capabilities to avoid attacks of this nature in the future. A collaborative approach like this allows security teams to gather valuable insights for strengthening the defenses against ransomware threats to smart grid systems.
	Eradication	The cybersecurity incident response team takes action in finding remnants of ransomware so that no traces could be left to reinfect the network segment and systems. They perform the scanning and sanitizing of infected devices with automated remediation using endpoint security solutions, address vulnerabilities that were attacked by ransomware with security patches and updates in implementation, and configuration changes are made accordingly. The team will also perform thorough system checks and validation procedures to make sure that the ransomware is eradicated and the affected systems are restored to a safe state. Verification of the effectiveness of eradication measures and residual threat monitoring requires collaboration with internal teams and external partners. Security teams can reduce the chances of further ransomware incidents and protect smart grid systems from

		potential ransomware threats by formulating a plan for data restoration from backups, remediation of infected systems, and rebuilding of affected infrastructure. They also employ additional security controls and hardening measures, and security patches and updates to address known vulnerabilities leveraged by the ransomware.
	Recovery	The cybersecurity incident response team performs the backup and restoration of the affected data in order to bring the affected systems back to the state before this incident. They use redundant infrastructure and failover mechanisms in order to minimize lost time and assure continued operation of critical grid functions. Testing and validation are performed post-recovery to confirm integrity and functionality of the recovered systems. The lessons learnt from the incident include resilience strategies identified to develop and enhance the necessary defenses to help in protecting the smart grid systems against ransomware incidents that could happen in the future. By proactively taking the situation into their control, this approach ensures acceleration in restoring the smart grid system and less disturbance on energy supply and delivery. Post-containment, the team continuously monitors the network for any residual malware or unauthorized activities, and they also re-verify the integrity of restored data and systems to make sure they will not be tampered with during their recovery.
	Improvement	The cybersecurity incident response team will carry out post-incident reviews and deep analysis in order to identify various weaknesses in incident response procedures, security controls, and resilience strategies. Based on lessons learned from the ransomware incident, they institute remediation measures and enhancements such as updating security policies, enhancing access controls, and increasing the level of employee training programs. They test and validate incident response plans through tabletop exercises and simulated ransomware scenarios on a regular basis to be prepared for any future attacks. They inculcate a culture of collaboration and knowledge sharing not only within the security team but throughout the organization to proactively manage risk and share information. This includes strengthening the defense mechanisms and mitigating the risks associated with ransomware attacks against smart grid systems regularly. Lastly, post-incident reviews and lessons-learned sessions will be held to determine what

		can be done to improve the response and provide better preparedness against future incidents, further developing overall organizational resilience related to cybersecurity.
Incident management Technology capability & Platform	Communication	At the time of the ransomware attack, the cybersecurity team would ensure that they communicate transparently with the stakeholders. They should give an elaborate summary detailing the impact of the incident, the mitigations applied to adjust to it, and what post-incident prevention will be done. Public announcements are released to assure customers and partners, reassure regulators that all necessary steps are being taken to minimize disruption and strengthen defenses. Communication is continued to reassure and facilitate full accountability for the organizational response. The ransomware incident is immediately reported to stakeholders, including management, IT personnel, legal representatives, and governmental authorities. The lines of communication within an incident response team must be clear to support the cooperation necessary for containment and mitigation. The cybersecurity team liaises with external cybersecurity experts, incident response firms, and law enforcement agencies to ensure timely and coordinated responses that work collaboratively to ensure prompt and effective measures against ransomware attacks to protect the organization's interests.
	SIEM	Security Information and Event Management) helps fight ransomware attacks by rapidly detecting abnormal behavior, identifying emerging threats, and alerting fast responses in smart grid systems. It monitors and confirms the security incident through SIEM to enable on-time mitigation. With real-time monitoring and correlation from diverse sources, SIEM nets resiliency against ransomware attacks with actionable insights, foregoing forensic analysis, and guaranteed compliance to cybersecurity standards. It thus strengthens the infrastructure in the smart grid against ransomware since it plays a key role in incident management, which is one of the essential security operations that help minimize or reduce disruptions.
	UEBA	User and Entity Behavior Analytics primarily empower smart grid systems to detect users and entities exhibiting specific behavior linked to ransomware attacks. With its intelligence capability for normal behavioral patterning, UEBA provides immediate threat detection on potential ransomware infiltration. It constructs an extended

		evaluation and verification strategy for security incidents with more rapid responses toward remediation by analyzing activity at both the user and entity interaction levels. Carrying out pattern predictions over anomalous activity from these systems and thereby leading to early identification, this framework develops robust strategies for incident management related to ransomware incidents. This proactive approach from UEBA empowers smart grid cybersecurity to respond well against ransomware and strengthen resilience by offering constantly evolving protection by managing incidents.
	Ticketing & Case Management	Ticketing & Case Management enhances responses toward ransomware attacks in smart grid systems because of the unified incident tracking and resolution portal. Thus, triaging, prioritization, and assignment against ransomware-specific incidents can be supported effectively. The details regarding the incidents and response activities are documented with ticket and case management to support an evaluative or even validation process relative to cybersecurity incidents. Incident Management improves in smart grids via a formal approach that helps in reducing in-operability and enhancing restoration activities.
	Threat Vulnerability management	Threat Vulnerability Management strengthens the ransomware attack defense of a smart grid system by continuously assessing and prioritizing remediation based on system vulnerabilities. This points out the weak points that attackers can use to gain access through ransomware, thus allowing mitigations to be taken in time. The threat vulnerability management will allow vulnerability scanning and risk assessment to be performed about the security posture of the intelligent grid systems. This allows the validation of ransomware-related incidents accordingly. It enhances incident management in a proactive way to minimize the occurrence of ransomware attacks within the smart grid cybersecurity framework.
	SOAR	Security Orchestration, Automation, and Response strengthen the defense against ransomware attacks in smart grid systems by automating incident response processes. The SOAR platforms integrate with security tools in orchestrating workflows for the quick detection, containment, and remediation of ransomware incidents. In this way, SOAR speeds up incident resolution by automating repetitive tasks and response activities, reducing ransomware attacks' impact on smart grid operations. It gives real-time visibility into daily activities and analytics with its centralized dashboard,

		hence enabling the assessment and validation of security incidents within the cybersecurity incident management framework.
	DETECTION / RESPONSE SENSORS	Antivirus, EDR, and endpoint management endpoint security solutions act as critical defenses against ransomware infection by detecting and blocking malicious activity at the level of every different device. Detection/Response Sensors are an effective way to combat ransomware attacks in smart grid systems. These sensors continuously monitor network traffic and system activities and can identify, through advanced algorithms and machine learning techniques, the appearance of ransomware- a file encryption pattern or unauthorized attempts to access valuable data. This capability thus enables timely responses, including systems isolation and blocking malicious traffic. Their alerts in real-time and forensic capabilities also help assess and validate ransomware-related incidents and improve the cybersecurity incident management framework.
	REPORTING	Reporting is one of the key activities in this area of the smart grid system for fighting ransomware attacks. It will enable insights into incident trends, impact assessment, and response effectiveness. In particular, it helps to evaluate and approve ransomware-related incidents by codifying incident details, response actions, and lessons learned. Reporting will help stakeholders gauge the effectiveness of cybersecurity measures and further streamline incident management processes within the smart grid ecosystem.
	Simulation Exercise & Training Platform	Simulation Exercises & Training Platforms enhance a smart grid system's defense against ransomware attacks with realistic scenarios through incident response training. Simulation Exercises & Training Platforms simulate these kinds of ransomware attacks, enabling security teams with time to practice responding and test effectiveness. By evaluating and validating response strategies in this controlled environment, Simulation Exercises & Training Platforms can improve incident management capabilities to ascertain their preparedness for responding to ransomware threats within the cybersecurity framework within smart grids.

Incidence Response Process	Incident response Procedure	IR procedures detail the step-by-step process with which entities respond to an incident relating to cyber security. Detection and Identification: Immediately identify the signs of a ransomware attack within the power grid network, such as suspicious encryption activities on critical systems or anomalies in operational data. Verify the nature and extent of the attack, including which control systems, substations, or other essential components of infrastructure have been affected. Incidence Response Team Activation: The power grid incident response team shall be activated and include specialists from IT, cybersecurity, operations, legal, communications, and executive leadership. The team shall be assembled in a specific incident response area or virtual environment with the tools and resources needed to coordinate and communicate. Containment and Mitigation: Isolate the infected systems to prevent the further spread of ransomware within the power grid network—focus suppression toward critical control systems and infrastructure. Segment compromised devices or network segments from operational networks but ensure continuity for essential services to avoid citywide disruption. Notification and Communication: Inform all the stakeholders within the power grid organization, such as senior management, grid operators, cybersecurity teams, and regulatory authorities, regarding the ransomware incident. Clearly define internal and external lines of communication to facilitate coordination, decision-making, and information sharing during the incident response process. Investigations and Analyses: Carried-out thorough investigations might declare the actual impact the ransomware attack caused or did to power grid operations, mentioning the specific control system involved substation or any transmission line involved. Supporting forensic evidence in that respect could include things such as network logs, snapshots of systems operating during runtime, and configuration that can be retrieved for in-depth analysis concerning what vectors the attack used and could be, ways of in-network propagation, or, worst of all, file encryption does or doesn't happen. Recovery and Restoration: Restore the critical power grid systems and control infrastructure from validated backups to minimize service disruptions and ensure the

		grid's reliability and resilience. This shall include prioritizing the restoration of the most critical services and grid functions that are central to stability, such as generation, transmission, and distribution, while meeting customer demands. Monitoring and Validation: Continue monitoring the power grid network for any ransomware activities or unauthorized access after the remediation activities. Validate the response activities by thoroughly testing and verifying restored systems and operational processes. Post-Incident Activity Review and Lessons Learned: Conduct a thorough post-incident activity review to identify the overall effectiveness of the incident response process, recognize its strengths and weaknesses, and document the key lessons learned that should benefit future process revisions. Document findings, recommendations, and best practices for improving the power grid organization's cyber resilience and incident response capabilities. Documentation and Reporting: Document all the actions taken and the timeline of decisions and outcomes of the ransomware incident response to support internal analysis and external reporting requirements. Prepare incident reports and notifications to regulatory authorities, industry partners, and other stakeholders as necessary to provide transparency and accountability in responding to cybersecurity incidents within the power grid environment.

	Incident response Playbook	The playbook will use all parts of incident management technologies from the previous section: Incident Detection and Initial Response Early Indicator Warning: Establish state-of-the-art advanced threat-detecting systems, such as Intrusion Detection Systems, Endpoint detection and response solution, and finally, Security information and event management platforms to support early warnings around potential ransomware attacks at their first stage. Alerting and Monitoring Automation of the alert mechanisms that will trigger the incident response team in case any potential ransomware indicators are identified; these include but are not limited to suspicious file encryption activity, unauthorized access attempts, or suspicious network traffic. Immediate Actions: Activate the incident response team and initiate predefined response activities identified in the ransomware playbook. Isolate the infected systems and segments of the power grid network, preventing further spread of the ransomware. Containment and Recovery Segmentation: Similarly, the different mechanisms of segmentation need to be identified. Network segmentation will help further restrict the lateral movement of ransomware in selected and isolated segments of a power grid network, consequently impacting minimal critical infrastructures and running processes. Backup Restoration: Restoration of vital systems and data that are well backed up to enable the reinstatement of the most critical services with minimum disruption. Patch Management and System Hardening: Apply security patches for known vulnerabilities utilized in the ransomware and enhance the general security posture of the power grid environment. Investigation and Analysis: Forensic Analysis: Conduct in-depth forensics on the compromised systems for detailed network logs to establish the reason for the ransomware attack, extend the compromise, and TTPs of the attackers. Attribution and Intelligence Gathering:

		Gather intelligence on the variant of ransomware used, the identity of the actors who conducted the attack, and their motivations, leveraging that to better posture incident response efforts and develop threat intelligence. Communication and Coordination: Internal Communication: This means open and transparent internal communication, whereby timely information is shared among the incident response team and throughout the organization for decision-making and response execution. External Communication: The respective regulatory authorities, industry peers, customers, and the public should be informed about the ransomware incident and its aftereffects on smooth grid operations. Post-Incident Review and Lessons Learned: Debriefing and Analysis: Provide a formal post-incident review of the response to ransomware to assess effectiveness, identify improvements, and capture lessons for future incident response planning and preparedness. Documentation and Reporting: All ransomware incident response activities shall be documented, including timelines of actions, decisions, and their conclusions, for internal analysis and external reporting. Continuous Improvement: Training and Skills Development: Provide regular training and skills development to the incident response team members to increase their capacity for detecting, responding to, and recovering from ransomware attacks within the power grid environment. Scenario-Based Exercises: Conduct occasional tabletop and simulated ransomware attack scenarios to test the effectiveness of the ransomware playbook, validate all response procedures that are needed or required, and identify areas needing improvement or refinement of processes.
	Recovery plan procedure	Isolate Infected Systems: Immediately isolate infected systems and segments of the power grid network to contain the spread of ransomware and limit its impact on critical infrastructure. Assess the Damage: Deeply analyze the ransomware attack to assess the level of encryption both at a system and a data level; prioritize based on criticality and operational need.

		Restore from Backups: Restoration of critical systems, applications, and data from secure and validated backups enables quick recovery of vital services and minimizes losses because of lost productivity. Patch and harden systems: Apply security patches and updates to known vulnerabilities being exploited by the ransomware; implement additional security controls and hardening measures to strengthen the overall security posture of the power grid environment. Verify Integrity and Functionality: Validate the integrity and functionality of restored systems and data to ensure they have not been tampered with during recovery and can support ongoing operations. Monitor for Residual Threats: Continuously monitor the power grid network for any residual ransomware activity after recovery operations or unauthorized entry and remediate the remaining threats and vulnerabilities in a timely manner. Communication and Reporting: Clearly and openly communicate to internal stakeholders, regulatory authorities, Industry Partners, and customers what was recovered and how the power grid's functionality would be affected. Also, prepare Incident Reports and notifications, if necessary, on binding regulatory requirements and adherence to organizational policies. Lesson Learned and Continuous Improvement: Properly conduct the post-incident review to learn lessons, best practices, and areas for improvement from the ransomware recovery process. Based on the results, update incident response procedures to enhance further cyber resilience and preparedness against ransomware attacks.
	Simulation Exercise	Simulation exercises are practical, real-life incidents in a controlled environment to practice incident response procedures and test the effectiveness of response capabilities. **Scenarios of Design**: Ransomware from different vectors (internal, external) **Implementation**: Tabletop exercises or simulated drills involve cross-functional teams carrying out a mock response to a ransomware attack; this is done to analyze

		coordination and communication. Internal and external simulations must be performed internally and externally. **Debrief**: After the exercise, facilitate a post-exercise debriefing to review performance, identify further improvements, and update incident response procedures and playbooks.
Incident Response Response Team support	IT / OT Support	The support team in engage during simulation and the real event and in this DDoS attack they have to: Be in support and coordination with the right team impacted: application and service owner, IT expert and network and engage the operational based on the procedure and they knowledge on the IT or OT environment (Generation Manager, Control Centre manager)
External Partner	State cyber agency	The external parties are involved in support during containment and recovery (Service restoration, Post-incident analysis, customer support):
	IT Technology provider	
	OT Technology Provider	
Infrastructure Monitored	Power Generation systems	A cyber-attack on the power grid- a ransomware incident- could pose grave public safety, economic stability, and national security threats. For such risks, good prevention, a robust cybersecurity policy, and good contingency planning are in place to protect such critical infrastructure from such cyber-attacks. This threat has to be well understood by all management teams and operation teams in any power grid operation, and they must be very attentive if such an event occurs.
	Power Transmission systems	
	National Load Dispatch Centre	
	Power Distribution systems	
	AMI	

	Enterprise IT systems	
Cybersecurity Capabilities Supporting Incident Management	Asset Management	Asset management is an updated inventory of all devices connected to the smart grid, whether OT or IoT. This would help the security teams understand where the potential vulnerabilities are and allow them to focus on the most important ones. Suppose one knows what assets are in the network. In that case, they can institute appropriate protection strategies, such as patch management and access controls, that minimize the risk of ransomware attacks and protect smart grid systems.
	Network security management	Network security management involves the methods and strategies provided to prevent intrusion into the network of smart grids and other malicious activities. This means the deployment of firewalls, intrusion detection systems, encryption protocols, and others to protect against data theft. Security professionals monitor network traffic continuously to recognize abnormal behavior as an indication of a ransomware attack. Network security management plays a critical role in mitigating the impact of ransomware by preventing its spread and minimizing damage to smart grid systems.
	System security management	This includes hardening the operating system, configuring its security settings, and updating software patches to secure each individual component and software system within the smart grid infrastructure. It ensures the integrity and resiliency of system components and reduces the attack surface for ransomware. System security management plays an important role in smart grid system protection against ransomware attacks through vulnerability mitigation and general cybersecurity posture enhancement.
	Security architecture and engineering	Security architecture and engineering involve setting up and implementing robust security controls and measures to protect the smart grid systems against ransomware attacks. That is, the creation of secure network architecture, implementation of protocols of encryption, and designing the system resilient in nature to resist the cyberattack. By integrating security principles while designing and developing smart grid infrastructure, security teams ensure minimum chances of ransomware attacks or mitigating the impact of such an attack on their occurrence to ensure the reliability and security of grid operations.

	Security Awareness and training	Security awareness and training programs aim to inform employees about the risk of ransomware attacks and teach them good cybersecurity hygiene practices. By making users aware of common attack vectors, such as phishing emails with malicious attachments, the security team provides them with an edge to identify suspicious activities and report them. In addition, training will equip the staff with the knowledge and abilities to act appropriately in case of ransomware attacks, reducing successful cases of these attacks and improving the general security outlook of smart grid systems.
	Zero Trust strategy	The Zero Trust strategy assumes that threats may already exist inside and outside the network. It requires strict identity verification for every user and device accessing resources, regardless of location. This approach minimizes the risk of ransomware attacks by limiting the attack surface and preventing unauthorized access to critical systems and data. By adopting a zero-trust strategy, security teams enhance the resilience of smart grid systems against ransomware threats.
	Endpoint protection strategy management	This refers to endpoint protection strategy management in which security is applied at each computer, server, and IoT device connected to the smart grid network. With endpoint security solutions, such as antivirus software and endpoint detection and response, security teams can focus on finding and mitigating ransomware at the device level, reducing the risk of infection and key grid operations.
	Understanding the cyber kill chain	The cyber kill chain is all about understanding the phases a cyber-attack goes through, from its reconnaissance to data exfiltration, to create an effective strategy of defense. Identifying each stage of the attack lifecycle allows the security teams to employ preventive measures and detection mechanisms at different times to break the attack chain, reduce the impact of ransomware attacks on smart grid systems in particular, and improve cybersecurity resilience in general.
	Identity and access management	IAM refers to controlling and managing how users access resources within the smart grid network. IAM solutions perform strict controls in terms of access, authentication, and monitoring user identities. For this reason, it could support the reduction in unauthorized access to critical systems and data, thereby reducing the impact of ransomware attacks. IAM is at the front line in posturing security and thus helps protect the systems of a smart grid from cyber threats.

	MITRE ATTACK	ATT&CK by MITRE represents a knowledge base of adversary tactics and techniques based on real-world observations. Understanding how the adversary operates will help security teams to defend against ransomware attacks proactively. MITRE ATT&CK offers insight into the standard attack methods employed by ransomware actors; hence, it allows teams to develop effective detection and prevention strategies. This equips the security teams with the necessary wherewithal and information to mitigate the impact of ransomware on smart grid systems.

In mitigating the DDoS and ransomware attacks on power utility smart grid systems, the holistic approach will have to consider the viewpoints and concerns of various stakeholders to take an active role in minimizing customer impact, ensuring regulatory compliance, public perception, and engagement with stakeholders. All these are because of enhancing resilience, maintaining public trust, and managing cybersecurity risks. Continuous tuning of the frameworks with the help of stakeholders and proactive strategies to manage risk will be of utmost importance to safeguard critical infrastructure against evolving cyber threats in service delivery.

The above scenario depicts the need for a critical cybersecurity incident management framework in all the power utilities operating smart grid systems. Further, mapping DDoS threat scenarios could help to assess their effectiveness for any power utility so that required changes can be adopted to make these utilities more resilient against DDoS attacks. It means utilities have to invest in proactive threat detection and incident response capabilities, along with industry collaboration and government agency collaboration, to minimize the risks from such DDoS attacks to guarantee the reliability and security of the power grid.

Furthermore, the emulation of ransomware attacks and testing for the efficiency of management procedures in incidents related to cybersecurity give whole meaning to the call for proactive cybersecurity measures coupled with robust incidence management frameworks. Utilities can identify shortcomings in their cybersecurity posture and make necessary changes to enhance their resilience against future attacks. Utilities will have to continue training, upgrading technology, and collaborating with industry partners and government agencies so

that the threats posed by ransomware and other cyber threats to the integrity and reliability of the power grid are minimized.

Chapter SIX

6. Conclusion and Recommendations

6.1 Conclusion

The integrated cybersecurity incident management framework has been driven into protection, threat detection, and response against various cyber incidents for Power Utilities by developing strategic and operational level threats through a capability-resource combination around the energy value chain. This study presents the conceptual design and develops an integrated framework for Cyber Incident Management, fully adapted to Smart-Grid systems. It encapsulates integral aspects of risk management, threat profiling, security controls, operating models, and governance on how best to approach cybersecurity in the smart grid industry. This will help utilities in the power sector, given their specific challenges and requirements in the energy value chain, to develop the necessary capabilities to manage cyber incidents proactively and to improve their general resilience.

Effective mobilization and integration of this framework into current power utility processes, systems, and organizational culture could be dominated by several competing demands. Power utilities require a breakdown of silos, cross-functional collaboration, and an alignment of stakeholders across all levels for successful framing and getting acceptance on the implementation. Another critical challenge is the framework that keeps pace with an ever-evolving threat landscape. Power utilities should thus make considerations and various threat scenarios through modeling to determine how effective the framework is in adapting to them. This means analyzing whether such a framework may have the potential to identify, respond to, and recover from emerging threats like DDoS attacks and ransomware. It is only through regular testing and simulation exercises that power utilities will be able to prepare for and address cybersecurity incidents as they arise.

To address these challenges, the framework also includes dynamic feedback loops and continuous improvement mechanisms. Power utilities should periodically review and update the composition of the framework assessment, threat profiles, security controls, and response and recovery plans. The culture of vigilance and continuous learning will support the framework as a dynamic and effective enabler in protecting the critical infrastructure of power utilities to sustain reliable energy delivery to customers.

6.2 Recommendations

Based on the insights and conclusions from this study, which highlight the challenges, cybersecurity threats, and incidents affecting critical infrastructure, the following recommendations are provided:

1. Continuous Monitoring and Adaptation

    - Periodically review, update, and integrate the given cyber security framework to adapt to emerging threats, evolutionary technological changes, and regulatory requirements.
    - Seamlessly embed this framework into power utilities' existing processes and culture.
    - Periodically evaluate power utilities' cybersecurity posture and perform quarterly in-depth risk analyses using standardized tools such as the NIST Cybersecurity Framework.
    - Track specific performance metrics, such as the average time to detect and respond to incidents and the number of incidents, which indicate the effectiveness of the cybersecurity measures.
    - Research the implementation of AI/ML-based solutions to detect anomalies in network traffic and strategize for the phase-by-phase replacement of legacy systems with their more secure replacements.
    - Leverage AI and ML to improve the cybersecurity posture by detecting unusual patterns and behaviors in networks and creating automated response protocols.
    - Develop a holistic 5-year defense improvement plan for the framework to stay in step with ever-evolving threats and technological shifts; consider costs in implementation; project the potential ROI by considering the avoidance of incidents or other quantifiable returns such as savings in lost operations, brand maintenance, and avoidance of regulatory requirements.
    - Forge partnerships with technology providers and cybersecurity experts to leverage their experience.

2. Comprehensive Capacity Building

    - Investments in regular training and awareness programs are needed for workers to understand best practices in cybersecurity and their role in managing cybersecurity incidents.
    - Develop comprehensive training programs to enhance the skills and knowledge of IT staff, operational personnel, and executives.
    - Regularly carry out simulated exercises to improve the utilities with power in terms of their capability for detection and response.
    - To further reinforce cybersecurity resilience, focus on developing concrete capabilities such as incident response, threat hunting, and forensic capabilities for a highly enabled team.
    - Encourage the employees to gain relevant certifications to complement their skills.
    - Implement strict access controls and regular audits to minimize the impact of human errors.

3. Collaborative Threat Intelligence

    - Encourage collaboration and information sharing with industry peers, government agencies, and cybersecurity communities to enhance threat awareness and response capabilities.
    - Establish platforms for sharing threat intelligence with industry peers and government agencies.
    - Organize joint cybersecurity exercises to enhance coordination and response capabilities.
    - Develop partnerships with technology vendors and cybersecurity experts to leverage their expertise.

4. Validating Effectiveness:

    - Testing and simulation exercises are done regularly for the Cybersecurity Incident Management Framework.
    - Establish measurable objectives and track key indicators such as incident response time, vulnerability reduction, and level of compliance to determine the adequacy of the cybersecurity framework.
    - KPIs on relevant definition and tracking, such as incident response time, vulnerability reduction, and compliance rates, will accurately measure the effectiveness of the Cybersecurity Framework, enabling informed decisions to be made as part of continuous improvement.

5. Readiness through Drills:

    - Conduct cybersecurity incident response drills involving cross-functional teams to ensure preparedness and coordination during real-world cybersecurity incidents.
    - Regularly conduct simulated exercises to test and improve power utilities' response capabilities.

6. Inclusive Implementation:

The engagement by stakeholders-executives, OT and IT personnel, security teams, and third-party vendors-all plays a part in the implementation of the framework to inculcate a cybersecurity culture of awareness and accountability. Partner with technology providers and cybersecurity experts to share their knowledge base through the process of building a partnership.

The Framework of Cyber Incident Management is designed in order to enable the power companies to take an active role in the management of cyber risks. This will protect the smart grid systems of the critical infrastructure by ensuring their reliability, integrity, and security. Thus, power utilities can reduce cyber threats to a minimum and reduce attacks on the cyber security systems within their smart grid systems to ensure the reliability, integrity, and security of the critical infrastructures.

6.3 Recommendations for Future Research

Key focus areas of future research on business continuity and disaster recovery planning, which will enhance resilience in power utilities, will be integrating robust cybersecurity measures into business continuity and disaster recovery planning to protect the critical infrastructure from ever-evolving cyber threats; resilient communication strategy through stakeholder engagement; and thorough business impact analysis. BIA helps you to find priorities in the effectiveness of disruptions; it aids them in developing strategy plans for feasible recoveries due to those facts. Other valid, important areas include locations chosen geographically far from the normal site versus where reliable backup devices will be installed. In such a case when there are man-made or natural disaster activities, these guarantee the power operates in the reinstatement and has continuity from time to time based on services. Lastly, testing and drilling should be periodically done to ensure that the developed business continuity and disaster recovery plans are effective. This is also to ensure testing of gaps, readiness of the organization towards the implementation, and application of necessary adjustments to keep the plans relevant and effective in case of circumstances that may change.

7. Appendixes

Cyber Security Incident Management Framework Focused Group discussion

Introduction

Focus-group discussions were undertaken with experts selected across various elements of the Cyber Security team, Engineering, and Management operators for and around the Generation, Transmission, and Distribution of Power. Through times and sessions, these undertook to frame or document all-inclusive specific details into what is known as the Cyber Security Incident Management Framework for the EEP Power Grid Systems.

Currently, power utilities in Ethiopia are upgrading and modernizing the OT environment with the latest advancements, such as smart meters installation, changing the RTU substation to a SAS substation, installing ArcGIS, and building a new National Load Dispatch Center. Integrating these digital technologies into our power infrastructure has increased efficiency and control. At the same time, it is this that has introduced new challenges and vulnerabilities to be considered to ensure the security and resilience of our critical infrastructure.

The discussion revolved around:

1. Identification of Current Challenges and Gaps: This was to properly understand our current state of cybersecurity posture and incident management capabilities, including existing challenges and vulnerabilities.
2. Input to Formulate an All-Inclusive Cybersecurity Incident Management Framework: Based on insights into the landscape, the goal was to design a framework that would leverage our competencies in cybersecurity incident detection, response, and restoration. Such a framework would have been actionable, scalable, and customized to unique operational requirements within our power generation, transmission, and distribution facilities.

What the expert views and opinions did instead was to help mold an effective and practical framework that actually conformed to our operational realities. Complementing the discussions from EEP is my role, enabling the incorporation of first-hand observation into the development of the framework.

Discussions with Cybersecurity Teams, Engineering Teams, and Managers & Operators from Generation, Transmission, and Distribution Units

Question 1: **How do you think legacy systems can be secured without causing major disruptions to grid operations?**

Engineering Teams: Engineers stress that upgrades must not interfere with operational stability. They propose phased updates with extensive testing in a simulated environment before deployment. They also highlight the need to balance security with system reliability.

Managers and operators are mainly concerned with the cost and operational risks associated with upgrading legacy systems. They express worries about potential downtime and suggest cautious, incremental changes that don't disrupt daily operations.

Cybersecurity Teams emphasize the critical risks posed by legacy systems, focusing on their lack of built-in security features. They advocate for applying compensatory controls like network segmentation and layered defense strategies. They may also suggest prioritizing the upgrade of the most vulnerable systems.

Question 2: How can outdated protocols be effectively replaced or reinforced in the current environment?

Engineering Teams: The engineers say updating security protocols may require rewriting some software and hardware. They emphasize compatibility issues and advise a gradual upgrade to avoid system disruption.

Managers & Operators: This group finds it hard to understand why the procedures need to change when the system is still working. Generally speaking, they cannot support such changes unless the associated risks and benefits are clearly described.

Cybersecurity teams say that those protocols act as an open door for attackers, and they must be replaced by modern standards of multi-factor authentication and encrypted communications. Continuous assessments are also recommended to find out-of-date components.

Question 3: What strategies can be implemented when vendor support for patches is no longer available?

Engineering Teams: We are concerned that potential untested patches could lead to system crashes. Suggest thorough testing in isolation for all third-party patches before implementing them.

Managers and Operators: Managers and operators are very concerned about the cost and operational risks of applying third-party patches. They would prefer solutions that require minimum intervention and cost.

Cybersecurity teams emphasize patching in a timely manner. When the vendor's patch is unavailable, they advise compensating controls such as intrusion detection systems.

Question 4: How can power grids mitigate the risks associated with global supply chain components?

Engineering Teams: They advocate for increased interaction with procurement teams to ensure security features are attended to when sourcing components. Further, they suggest collaboration with trusted suppliers and frequent audits for security concerns.

Managers & Operators: They may not fully understand the complexity of supply chain security but are concerned about the possible costs and delays involved in changing suppliers or adding extra vetting processes.

Cybersecurity teams underline the need to secure the supply chain by properly onboarding suppliers, establishing policies to procure components securely, and tracking those components throughout their lifecycles to prevent tampering.

Question 5: **How can insider threats be identified and mitigated in a power grid environment?**

Engineering Teams: Engineers recommend controlling access based on the roles assigned to personnel. Only persons who have essential needs to know should access such critical systems. They also suggest that organizations create an environment of security culture.

Managers & Operators: They show much interest in learning ways to uncover these insider threats with minimum possible harm to morale. They believe non-intrusive measures will have a much less psychological impact on their organizations. The more one would have towards awareness and straightforwardness concerning security reasons.

Cybersecurity Teams: They propose strict access control, continuous monitoring, and behavior analytics as ways to detect suspicious insider activities. They also propose regular training to raise awareness.

Question 6: What can be done to prevent unauthorized access due to weak or compromised passwords?

Engineering Teams: Engineers support measures for role-based access control but emphasize the need to make such solutions user-friendly, not to burden the operators with extra tasks. They also suggest integrating password management tools into existing workflows.

Managers & Operators: They are a bit annoyed by the complex password policy and want simple, easily-rememberable passwords. They need to be guided and educated on good password behavior.

Cybersecurity Teams: They advocate strict password policies, password managers, and MFA. Updates on password renewal and credential leakages checking are other key ways.

Question 7: How can power grids defend against malware that targets unpatched systems?

Engineering Teams: Engineers emphasize routine maintenance of systems.

Managers and operators are concerned about malware's operational impacts; however, they depend heavily on cybersecurity teams to manage technical defenses. They support routine updates if they don't interfere with operations.

Cybersecurity Teams: They recommend implementing anti-malware solutions, updating software, and segmenting networks, which can prevent malware outbreaks. They also recommend regular security audits.

Question 8: How can power grid operators be trained to recognize and resist social engineering attacks?

Engineering Teams: Engineers recommend integrating security awareness into everyday operations and incorporating lessons into existing training programs.

Managers and operators: This group often views social engineering as low-risk compared to operational issues. They require clear, practical examples to understand the real-world impact of these attacks and how they can personally contribute to prevention.

Cybersecurity Teams: They stress the need for regular training and awareness programs tailored to non-technical staff. Simulated phishing exercises and role-specific training can help operators recognize and avoid social engineering traps.

Question 9: What steps should be taken to establish a robust cybersecurity incident management framework for power utilities?

Engineering Teams: Engineers support the creation of standardized procedures that are in line with the operational protocols already in place. They prioritize clarity in communication and clear roles in incident response.

Managers and operators will be more interested in understanding how these new frameworks could complicate their established job performance. They will seek clear and concise guidelines that fit into their daily operations.

Cybersecurity teams: This would indicate the team's integrated approach to incident response: detect, contain, and recover. The team would foster collaboration across departments and use incident management tools.

Question 10: How can continuous security monitoring be improved in power utilities?

Engineering Teams: We recommend adding monitoring systems in place of the control room for full visibility and pointing out any issues that need to be escalated with clearly defined procedures.

Managers and operators fear an added workload for alert monitoring. They need a smoothly integrated an operational solution.

Cybersecurity Teams: They are for deploying automated monitoring tools with real-time alerting. Continuous logging, SIEM systems, and threat intelligence help in early detection and response.

Question 11: What role does automation play in improving cybersecurity incident management?

Engineering Teams: Engineers emphasize integrating automated tools with existing systems while ensuring they don’t introduce new risks. They suggest phased implementation to validate the effectiveness of these tools.

Managers and operators worry that automation might introduce complexity or require additional training. They prefer automation solutions that can be easily managed and don’t require extensive reconfiguration of existing processes.

Cybersecurity Teams: They stress that automation is key to efficient threat detection and response. Automated incident response tools, playbooks, and patch management systems reduce human error and speed up response times.

Question 12: What can be done to attract and retain skilled cybersecurity professionals in the power utilities sector?

Engineering Teams: Engineers suggest cross-training existing staff to develop cybersecurity expertise and creating joint task forces to foster collaboration between cybersecurity and engineering teams.

Managers and operators express concern about the budget implications of hiring new talent. To upskill existing employees, they favor cost-effective solutions, such as in-house training programs or partnerships with external experts.

Cybersecurity Teams: They point to the need for competitive compensation, ongoing training, and a clear career progression path to attract top talent. Collaboration with academic institutions and industry partnerships can also help fill the talent gap.

Summary of discussion

Legacy Systems

Many power grid systems use technology that does not have advanced security features. That provides some challenges in providing meaningful cybersecurity to systems like these when this technology is outdated and doing so with continuous operations.

Outdated Security Protocols

Systems developed before the emergence of cybersecurity threats do not have the necessary security components; thus, they are easily vulnerable to all types of cyberattacks, malware infections, and data breaches.

Limited Patching and Updates

When manufacturers cease to release patches and updates, older systems become completely open to exploiting known vulnerabilities. Sometimes, such systems are hardly modified for a relatively long period and are thus pushed into the line of fire of exploitation.

Supply Chain Vulnerabilities

Power grid components are primarily sourced from global supply chains. Threat actors can exploit the components at any stage of manufacturing, transportation, or installation, heightening the attack surface for a cybersecurity attack vector.

Insider Threats

Disgruntled employees or contractors with access to power grid systems pose significant risks. Insider attacks, whether intentional or unintentional, can disrupt power grid operations.

Sniffing, guessing, and cracking of passwords

Poor security policies, unsupported software, and no encryption on power grid networks make sniffing, guessing, and password hash dumps lucrative.

Malware

Expanding upon the previous risk category, malware poses a severe threat to the smart grid environment. Flourishing in unpatched network infrastructure within the power grid, malware can cause substantial damage when left unchecked.

Social engineering

Social engineering attacks are particularly effective against power grid operators, who often prioritize operational efficiency and cost-effectiveness over cybersecurity measures.

Inaccessibility to the Cybersecurity Incident Management Framework for the power utilities industry.

The power utilities industry is vulnerable to a lack of cybersecurity incident management framework. Without any structured approach toward handling cybersecurity incidents, it is challenging for power utilities to detect and assess the threats and take mitigation measures effectively. This deficiency in cybersecurity incident management makes critical energy infrastructure susceptible to cyberattacks that may affect operational continuity and public safety.

Lack of continuous security monitoring

Inadequate continuous security monitoring in electric utilities further heightens cybersecurity incident management challenges. Without timely surveillance, effective detection and response to threats are delayed and inefficient; this, therefore, increases the chances that cyberattacks will be successfully performed, potentially impacting the reliability and integrity of the essential energy infrastructure systems.

Lack of automation and proper tools

Manual handling and the use of inappropriate tools and technologies within the power utility industry disturb this segment of Cyber Security Incident Management. Again, this has made the process manual, delaying threat detection and response, thereby making the systems prone to attacks. This needs a strong drive for automation supported by advanced tools that will ensure timely identification and mitigation of cyber threats and provide resilience to energy infrastructure.

Lack of skilled cybersecurity professionals

One weakness is that the power utilities sector lacks skilled analysts, so it is not in a position to manage cybersecurity incidents with great efficiency. Lack of expertise impacts detection and response and increases the chance of a successful cyberattack. Hiring and retaining qualified professionals will improve incident management capability and protect critical energy infrastructure against evolving threats.

8. References

1. Fabro, T. Roxey, and M. Assante, “No grid left behind,” IEEE Security & Privacy, vol. 8, no. 1, pp. 72–76, 2010g.
2. D. Batchelder, J. Blackbird, D. Felstead, P. Henry, J. Jones, and A. Kulkarni, “Microsoft Security Intelligence Report,” Microsoft, 2014.
3. A. Lemay, J. Calvet, F. Menet, and J. M. Fernandez, “Survey of publicly available reports on advanced persistent threat actors,” Computer. Secure., vol. 72, pp. 26–59, 2018.
4. Lloyds and University of Cambridge, “Business Blackout The insurance implications of a cyberattack on the US power grid Emerging Risk Report-2015 Innovation Series,” 2015.
5. National Institute of Standards—Computer Security Resource Centre, Malware, p. 2021, https://csrc.nist.gov/glossary/term/malware.
6. Alberts, C., Dorofee, A., Killcrece, G., Ruefle, R., and Zajicek, M. 2004. "Defining Incident Management Processes for Csirts: A Work in Progress,"
7. ISO/IEC, BS ISO/IEC 27035-1:2016, 2016.
8. ISO/IEC, BS ISO/IEC 27035-2:2016, 2016.
9. ENISA, Good Practice Guide for Incident Management, Technical Report, European Network, and Information Security Agency, 2010.
10. Mitropoulos, S., Patsos, D., and Douligeris, C. 2006. "On Incident Handling and Response: A State-of-the-Art Approach," Computers & Security (25:5), pp. 351-370.
11. Line, M. B., Tondel, I. A., and Jaatun, M. G. 2014. "Information Security Incident Management: Planning for Failure," IT Security Incident Management & IT Forensics (IMF), 2014 Eighth International Conference on IEEE, pp. 47-61.
12. Chiu, C-C; Lin, K-S. ‘Importance Performance Analysis Based Evaluation Method for Security Incident Management Capability’. Paper presented at the Asian Conference on Intelligent Information and Database Systems, 2017.
13. Tøndel, IA; Line, MB; Jaatun, MG. ‘Information security incident management: Current practice as reported in the literature’. Computers & Security, 45, 2014, pp.42-57.
14. Manworren, N; Letwat, J; Daily, O. ‘Why you should care about the Target data breach’. Business Horizons, 59(3), 2016, pp.257-266.

15. Wang, P; Johnson, C. 'Cyber security Incident Handling: A Case Study of the Equifax Data Breach'. Issues in Information Systems, 19(3), 2018.
16. Zou, Y; Mhaidli, AH; McCall, A; & Schaub, F. 'I've Got Nothing to Lose: Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach'. Paper presented at the 14th Symposium on Usable Privacy and Security (SOUPS), 2018
17. P. Cichonski, T. Millar, T. Grance, K. Scarfone, NIST Special Publication 800-61: Computer Security Incident Handling Guide, Technical Report, National Institute of Standards and Technology, 2012.
18. ISO/IEC 27035:2011 Information technology - Security techniques - Information security incident management, 2011.
19. NIST, 7628-1: Guidelines for Smart Grid Cyber Security, National Institute of Standards and Technology, 2010.
20. NIST, 7628-3: Guidelines for Smart Grid Cyber Security, National Institute of Standards and Technology, 2010
21. P. Kral, Information Security Reading Room: Incident Handler's Handbook, Technical Report, SANS Institute, 2019.
22. ISO/IEC 27000:2012(E). Information technology - Security techniques – Information security management systems - Overview and vocabulary - Second edition. International Organization for Standardization, 2012.
23. J. Creasy, I. Glover, Cyber Security Incident Response Guide, Technical Report, Council for Registered Ethical Security Testers, 2013.
24. IEC, BS IEC 62443-2-1:2011, 2011.
25. IEC, BS EN IEC 62443-4-2:2019, 2019.
26. National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Technical Report, 2018.
27. NERC, CIP-008-6 - Cyber Security - Incident Reporting and Response Planning, Technical Report, North American Electric Reliability Corporation, 2019.
28. Critical mass cyber security requirement standard, 2009.
29. K. Stougger, V. Pillitteri, S. Lightman, M. Abrams, A. Hahn, NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security, Revision 2, Technical Report, National Institute of Standards and Technology, 2015.

30. M.Bartock, J. Cichonski, M. Souppaya, M. Smith, G. Witte, K. Scarfone, NIST Special Publication 800-184: Guide for Cybersecurity Event Recovery, National Institute of Standards and Technology, 2016.
31. Akhtar, M. I. (2016). Research Design. Research in Social Science: Interdisciplinary Perspectives
32. Kothari, C.R.. (2004). Research methodology: Methods and techniques (2nd revised edition). New Delhi: New Age International (P) Limited, Publishers.
33. Line, M.B., Tøndel, I.A., Jaatun, M.G.: Current practices and challenges in industrial control organizations regarding information security incident management - Does size matter? Information security incident management in large and small industrial control organizations. Int. J. Crit. Infrastructure. Prot. 12, 12-26 (2016)
34. A. Staves, T. Anderson, H. Balderstone, B. Green, A. Gouglidis, and D. Hutchison, "A Cyber Incident Response and Recovery Framework to Support Operators of Industrial Control Systems,".
35. I. Tøndel, M. Line and M. Jaatun, Information security incident management: Current practice as reported in the literature, Computers, and Security, vol. 45, pp. 42–57, 2014.
36. M. Jaatun, M. Bartnes, I. Tøndel: Zebras and Lions: Better Incident Handling Through Improved Cooperation
37. M.Bartnesa, N. Moeb, P. Heegaarda: The future of information security incident management training: A case study of electrical power companies
38. M. Line, I. Tøndel and M. Jaatun, Information security incident management: Planning for failure, Proceedings of the Eighth International Conference on IT Security Incident Management and IT Forensics, pp. 47–61, 2014.
39. M. B., Line E. Albrechtsen, (2016), "Examining the suitability of industrial safety management approaches for information security incident management", Information & Computer Security, Vol. 24
40. M. B. Line, "A study of resilience within information security in the power industry," 2013 Africon, Pointe aux Piments, Mauritius, 2013, pp. 1-6, doi: 10.1109/AFRCON.2013.6757799.
41. Acarali, D., Rajarajan, M., Chema, D. & Ginzburg, M. (2020). "Modelling DoS Attacks & Interoperability in the Smart Grid. 2020 29th International Conference on Computer Communications and Networks (ICCCN) ".
42. https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2023/05/smarter-grids.pdf

43. https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q2-2024/
44. https://ics-cert.kaspersky.com/publications/reports/2023/03/15/h2-2022-brief-overview-of-main-incidents-in-industrial-cybersecurity/