Cyber - Attacks on Renewable Energy

Digital Risk Management and Information Security

Sai Teja Bathula

Table of Contents

Abstract

ABC Enterprises, a mid-size offshore wind farm valued at 10 million AUD, with a cybersecurity consultant to advise on information systems security implementation, cyber-attack consequences, and establishing it within their organization. The company has recently moved from an onshore wind farm to an off-shore (water) wind farm without sufficient cybersecurity measures. In this paper, we develop a report that highlights the importance of robust security practices and the potential impact of cyber-attacks. In addition to that, the paper will also suggest ways to integrate a comprehensive security policy into their organizational structure. The report includes key concepts such as the global effects of cyber-attacks on wind-renewable energy, the number of employees, location, employee skills, and information assets. The paper will be presented as a professional business report, making reasonable assumptions about ABC Enterprises.

Highlights:

- Renewable energy industry rise in cyber-attacks.

Keywords:

- Cyber-attacks, Renewable energy.

1. Introduction

One evidence that the renewable energy industry is growing is that it is becoming more vulnerable to hackers. According to reports, the utility industry had a 46 per cent year-over-year increase in cyberattacks in 2021, with an average of 736 attacks per week. These new resources are increasingly being targeted as renewable deployment expands.

Source: https://action.deloitte.com/insight/3157/renewable-energy-grows-in-stature-and-in-cyber-risk

2. Case Studies (Part-1)

Cyberattacks on Renewable energy resources are on the rise, but according to an IEA analysis, utilities are having difficulty detecting them.

Case Study 1:

In 2023, Queensland Solar electricity generator CS Energy was nearly brought to its knees after a devastating ransomware attack on its ICT network by criminal Russian hackers.

Impact on organization:

The attempted attack on the Queensland power station nearly affected millions of homes. Furthermore, it had an impact on the business network.

Mitigation:

By separating the corporate network from other internal networks and implementing business continuity procedures, CS Energy acted swiftly to mitigate this event.

Type Of Attack:

Ransomware

Case Study 2:

In 2019, A US renewable energy firm was attacked by using the Cisco firewall. Cyber-attack hits Utah wind energy.

Impact on organization:

Caused a power utility in the United States to have disruptions in its electrical system.

Mitigation:

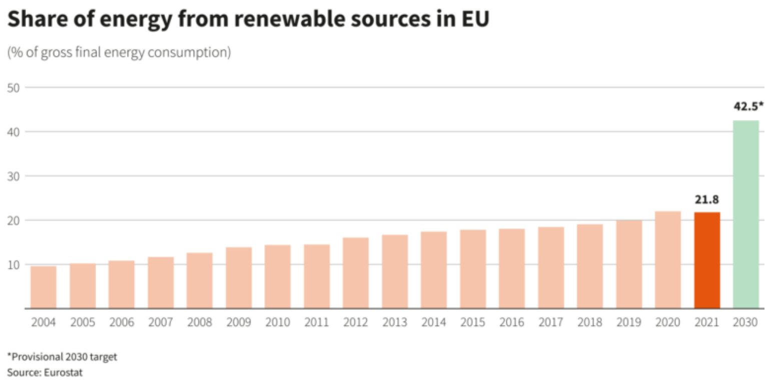
Fixing vulnerabilities in devices that were no longer up to date.

Type Of Attack:

DDOS.

Case Study – 3:

In 2023, Europe's Power Industry's Fear amid the Chaos of Conflict.



Share of energy from renewable sources in EU

(% of gross final energy consumption)

*Provisional 2030 target

Source: Eurostat

Impact on organization:

They knock out digitalized energy grids.

Mitigation:

Monitoring the logs frequently.

Type Of Attack:

Malware.

Case Study – 4:

Alarming wind-energy cyber-attacks in Europe.

Impact on organization:

Turn off the remote controls for nearly two thousand wind turbines for a day.

Mitigation:

Fixing vulnerabilities.

Type Of Attack:

Ransomware.

Case Study – 5:

In 2022, 11GW of German wind turbines are rendered inoperable by a satellite cyberattack.

Impact on organization:

The Viasat-owned KA-Sat communication satellite failed.

Mitigation:

Using Auto-pilot mode.

Type Of Attack:

TCP/IP Hijacking.

Case Study 6:

In 2023, Pro-Russian group claims responsibility for cyberattack against Hydro-Québec Utah wind energy.

Impact on organization:

Shut down the website of the company Hydro-Québec, responsible for the production and transportation of electricity in Quebec.

Mitigation:

Using Intrusion Detection Systems.

Type Of Attack:

DDOS.

Case Study 7:

In 2014, Korea Hydro and Nuclear Power is a nuclear and hydroelectric enterprise based in South Korea.

Impact on organization:

Network Infrastructure through phishing email.

Mitigation:

Implemented network infrastructure.

Type Of Attack:

Brute-force Attack.

Case Study 8:

In 2021, Colonial Pipeline hack.

Impact on organization:

Network Infrastructure.

Mitigation:

Implemented network infrastructure.

Type Of Attack:

Ransomware.

Case Study 9:

In 2021, Florida water utility hack.

Impact on organization:

SCADA Systems.

Mitigation:

Implemented Firewall and good password security.

Type Of Attack:

Ransomware (TeamViewer).

Case Study 10:

In 2018, Hackers hit Norsk Hydro with ransomware.

Impact on organization:

The data breach would ultimately have a financial effect of around $71 million.

Mitigation:

Rebuild Infrastructure.

Type Of Attack:

Ransomware through phishing emails.

No	Year & Attack Name (Use case)	Attack Type	Industry Sector	How the attacks occurred	Their Impacts	Security measures in place before the attacks	How the attacks were managed	Any security control measures implemented post-attack	If any vulnerabilities persisted in the targeted organizations after these security measures were implemented.
1	In 2022, CS Energy of Queensland plans to close two power plants.	Ransomware	Solar Energy	ICT networks.	Affected corporate network	Corporate network integrated with other internal networks	Separating additional internal networks from the corporate network.	Implemented Network Architecture	No.
2	In 2019, Cisco Firewall Exploited.	DDOS	Wind And Solar	Firewalls	Caused a power utility in the United States to have disruptions in its electrical system.	Not updated Firewall systems.	Fixing vulnerabilities in devices that were no longer up to date.	Updating Firewalls.	No.
3	In 2023, Cyberattacks on Renewables: Europe.	Malware	Hydro	IoT	They knock out digitalized energy grids.	Grids connected with IoT.	Monitoring the logs frequently.	Increasing the size of its 200-person cyber security team to safeguard grid and wind energy operations.	No.
4	In 2022, Alarming wind-energy	Ransomware	Wind	SCDA systems	For a day or so, turn off the remote	Not updated Firewall	Fixing vulnerabilities.	Updating Firewalls.	No.

	cyber-attacks in Europe.				controls for around 2,000 wind turbines.			
5	In 2022, Satellite cyber-attack in Germany.	TCP/IP Hijacking.	Wind	Satellite Networks	The Viasat-owned KA-Sat communication satellite failed.	Not updated Access control lists.	Using Auto-pilot mode.	Updating Access control lists.	No.
6	In 2023, Pro-Russian group claims responsibility for cyberattack against Hydro-Québec.	DDOS Attack	Hydro	Network Infrastructure.	Shut down the website of the company Hydro-Québec, responsible for the production and transportation of electricity in Quebec.	Network traffic is not monitored.	Using Intrusion Detection Systems.	Automate network monitoring.	No.
7	In 2014, Korea Hydro and Nuclear Power is a nuclear and hydroelectric enterprise based in South Korea.	Brute-force attack	Hydro	Network Infrastructure through phishing email.	Pilfer critical information, such as nuclear reactor blueprints and instructions.	Network traffic is not monitored.	Implemented network infrastructure.	Heightened understanding of the significance of cybersecurity.	No.
8	In 2021, Colonial Pipeline hack.	Ransomware	Solar.	Network Infrastructure.	Halt the pipeline's operation.	No Critical Infrastructure Protection standards.	Using system backups.	Implemented Critical Infrastructure Protection standards.	No.
9	In 2021, Florida	Ransomware (TeamViewer)	Hydro Power.	Firewalls.	Disrupted SCADA Systems.	Bad firewall system and poor	Implemented good firewall system and	Identity-based regulations	No.

	water utility hack.					password security.	better password security.	set in tandem with remote access programs, multi-factor authentication, military-grade encryption, and remote access via encrypted tunnels.	
10	In 2018, Hackers hit Norsk Hydro with ransomware.	Ransomware	Hydro	Phishing emails.	The financial impact would eventually approach $71 million due to data breach.	No Employee awareness training.	Re-build the infrastructure.	Introduced Employee awareness training.	No.

B) ABC Enterprises faces various cybersecurity threats, including ransomware, DDoS attacks, malware, and TCP/IP hijacking. To prevent these incidents, the company should implement various cybersecurity measures and best practices. These include regular data backups, keeping software and security systems updated, educating employees on phishing and social engineering, and implementing strong access controls and network segmentation. The Company should also use DDoS mitigation solutions, maintain up-to-date firewall systems, deploy robust endpoint security solutions, and conduct regular security scans and audits. Network infrastructure attacks should be addressed through comprehensive security measures, ensuring network traffic is monitored, and maintaining awareness of evolving threats. Company should also comply with Critical Infrastructure Protection (CIP) standards, use intrusion detection systems, and conduct regular security audits. Additionally, the company should secure remote access through encrypted tunnels, use multi-factor authentication, and conduct security training for employees.

3. Risks that ABC Enterprises may face if they move their operations offshore (to the sea).

No	Threats	Attack location/device in Wind Farm.	Onshore Wind Farms (Land).	Offshore Wind Farms (Water).
1	Ransomware.	Network Devices.	Routers and Switches.	Marine grades Routers and Switches.
2	DDOS	Firewalls	Application layer, and Access control for Onshore Wind Farms	Application layer (NGFW), and Access control for Offshore Wind Farms
3	Malware	IoT	Wind turbine sensors and vibration sensors.	Marine – grade wind turbine sensors and Marine environmental sensors.
4	TCP/IP Hijacking.	End points. (load balancers, switches, Routers, and firewalls).	Yaw control systems, Grid connection points.	Offshore wind turbines, Marine communication infrastructure.
5	Physical Security	CCTV Cameras, Access control systems like Biometric, Access control logs.	Access control measures are primarily land-based and may involve physical security devices.	Offshore farms require specialized access controls to secure sea-based access points and offshore structures.

B) The top five dangers that the ABC Company may encounter because of its offshore transitions.

- **Ransomware**: Ransomware attacks could target the ABC company's offshore networks.

- **DDOS:** DDoS attacks can overwhelm the offshore network, making systems and services unavailable, impacting energy production and grid connection.
- **Malware:** Malware, such as spyware or Trojan horses, could infect the wind farm's systems, potentially allowing attackers to gain unauthorized access or control.
- **TCP/IP Hijacking:** TCP/IP hijacking can result in attackers intercepting and manipulating communication sessions within the offshore wind farm's network, potentially disrupting energy production or gaining unauthorized access.
- **Physical Security:** Physical security threats may involve unauthorized access by sea or maritime vessels to the offshore wind farm infrastructure, potentially leading to equipment damage, tampering, or theft.

4. Potential security control methods and their implementation costs to handle such risks.

Possible security control strategies to manage the identified threats for the ABC company's offshore wind farm transition, along with a brief outline of the cost associated with each strategy:

Ransomware:

- **Security Control Strategy:** Implement a robust backup and recovery system, including regular data backups, offline storage, and automated backup testing. Additionally, deploy advanced endpoint protection and email filtering solutions to prevent ransomware infections.
- **Cost:** Install Backup servers $750,000 USD

DDOS:

- **Security Control Strategy:** Employ a dedicated DDoS mitigation service or solution that can detect and block malicious traffic during an attack. This may involve working with a third-party service provider or implementing on-premises DDoS protection hardware.
- **Cost:** Deploy Cloud WAF services that cost $8400/year.

Malware:

- **Security Control Strategy:** Deploy advanced endpoint security solutions with real-time threat detection and prevention capabilities. Regularly update and patch software and operating systems to address vulnerabilities that malware may exploit. Additionally, conduct employee training to raise awareness about malware risks.
- **Cost:** Deploy an automation script for updating the software's automatically to minimize the cost ($600). Employee training awareness costs ($6000).

TCP/IP Hijacking:

- **Security Control Strategy:** Implement network segmentation to isolate critical systems, and use strong access controls, including firewalls and intrusion detection systems.
- **Cost:** Deploy intrusion detection systems ($4000/ year), Deploy a firewall ($8000) and IAM roles for authorized users for least privilege access by hiring 10 administrators. ($8,00,000/year).

Physical Security:

- **Security Control Strategy:** Strengthen physical security measures to deter and detect unauthorized access by sea or maritime vessels. Measures may include video surveillance, access control systems, biometrics, and maritime patrols.
- **Cost:** Deploy CCTV Cameras ($4000) and biometric systems ($1000).

5. Budget Constraints.

Control	Annualized cost of Security (ACS) ($/year)
Install Backup servers	$750,000
Deploy WAF services.	$8400
Automation Script	$600
Employee training awareness	$6000
Intrusion detection systems	$4000
Deploy a firewall	$8000
Admins	$8,00,000
CCTV Cameras	$4000
Biometric Systems	$1000
Total	$1,582,000

Control	Year 1	Year 2	Year 3	Year 4	Year 5	Total Cost
Install Backup servers	$350,000	$350,000				
Deploy WAF services	$8400	$8400	$8400	$8400	$8400	$8400
Automation Script	$600	-	-	-	-	-
Employee training awareness	$6000	$6000	$6000	$6000	$6000	$6000
Intrusion detection systems	$4000	-	-	-	-	-
Deploy a firewall	$8000	-	-	-	-	-
Admins	$4,00,000	$4,00,000	$4,00,000	$4,00,000	$4,00,000	$4,00,000
CCTV Cameras	$4000	-	-	-	-	-
Biometric Systems	$1000	-	-	-	-	-
Annual Budget	$7,82,200	$764,400	$4,14,400	$4,14,400	$4,14,400	$4,14,400
Remaining	$800,000	$817,600	$1,168,000	$1,168,000	$1,168,000	$1,168,000

6. Business continuity plan (BCP) for ABC Enterprises affected by a cyber-attack that caused a significant data breach (Part – 2)

Objective:

Source: https://www.cyber.gov.au/sites/default/files/2023-03/ACSC%20Cyber%20Incident%20Response%20Plan%20Guidance_A4.pdf

- Outline the procedure to be taken in the event of a attack, with a focus on mitigating the impact, ensuring regulatory compliance, and minimizing downtime.
- The true cost of a data breach is not just financial; it can also result in reputational damage and loss of trust from customers.
- The report emphasizes the importance of data protection and being proactive and prepared when it comes to cyber risks.

Roles and Responsibilities:

- Report the details to the individuals responsible for incident response.
- Report to the Cyber Incident Response Team that manage organizations telecommunications systems.

Incident Identification:

- Identify the attack using Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).

Isolation and Containment:

- Disconnect compromised systems from the network to prevent them from communicating with the attacker's infrastructure.
- Physically disconnect devices from the network, if necessary.
- Use network access control (NAC) or firewall rules to block traffic to and from compromised systems**.**
- Update Security Policies.
- Monitor the Environment.

Follow Standard Operating Procedures (SOPs):

Source: https://www.oaic.gov.au/__data/assets/pdf_file/0017/1691/data-breach-preparation-and-response.pdf

- Provide a list of Standard Operating Procedures (SOPs) that were created to assist the incident response efforts of the company.
- The program for Notifiable Data Breaches (NDB) scheme

  According to the Privacy Act, organizations must alert the Commissioner and any impacted parties to specific data breaches.

Data Breach Investigation:

- Investigate the breach, including the forensic analysis process.

Legal and Compliance Response:

- Report to the Sector, Jurisdictional & National Incident Response Arrangements.
- Report the information about the relevant sector arrangements, and the organization's policy and process for implementing these arrangements.
- Report the organization's stance and the procedure for informing state and/or territory law enforcement and/or requesting assistance.
- Report the organization's stance and the procedure for reporting to Australian government agencies and/or requesting aid from them.

Data Recovery and Restoration:

- Determine the extent of the data breach, including what data was compromised, how it was accessed, and how long the attacker had access.

- Begin the restoration process by recovering data from your backup systems.
- Validate that the restored data is complete and accurate.

Incident Notification and Reporting:

- **Legal and Regulatory Requirements:**

  Assist the compliance and legal team of the company in making sure the cyber incident response strategy complies with all applicable laws and regulations.

- **Insurance:**

  Report the details about the organization's insurance policy for cyber incidents.

Training and Awareness:

- Highlight the importance of continuous training for employees and creating awareness of data security best practices.

Testing and Drills:

- Emphasize the need for regular testing and drills to ensure the BCP is effective.

Post-Incident Analysis:

- Continue to monitor systems and networks to detect any signs of further intrusions or suspicious activity.
- Perform a post-incident study to see where the security posture needs to be strengthened and to comprehend the underlying reasons of the breach.

Document Storage and Accessibility:

- BCP will be stored and made accessible to authorized personnel.

7. References

- Deloitte (2023) Renewable energy grows in stature (and in cyber risk), Insights2Action TM, 19th October 2023. (https://action.deloitte.com/insight/3157/renewable-energy-grows-in-stature-and-in-cyber-risk)
- ABC (2022) Australia's electricity grid increasingly vulnerable to hackers via solar panels, smart devices, ABC Australian website, 19th October 2023. (https://www.abc.net.au/news/2022-03-14/australia-electricity-grid-vulnerable-hackers-solar-panels-smart/100892044)
- 7News (2022) Millions of homes almost impacted by hackers' attempt on QLD power station, 7 News website, 19th October 2023. (https://7news.com.au/news/qld/hackers-targetted-qld-power-stationreport-c-4858121)
- Zdnet (2019) Cyber-attack hits Utah wind and solar energy provider, Zdnet website, 19th October 2013. (https://www.zdnet.com/article/cyber-attack-hits-utah-wind-and-solar-energy-provider/)
- Security week (2019) Cisco Firewall Exploited in Attack on U.S. Renewable Energy Firm, Security week website, 19th October 2023. (https://www.securityweek.com/cisco-firewall-vulnerability-exploited-attack-us-renewable-energy-provider/)
- Reuters (2023) Insight: Cyberattacks on renewables: Europe power sector's dread in chaos of war, Reuters website, 19th October 2023. (https://www.reuters.com/business/energy/cyberattacks-renewables-europe-power-sectors-dread-chaos-war-2023-06-15/)
- Insurance journal (2023) Cyberattacks on Renewables: The Stuff of Nightmares for Europe's Power Sector, Insurance journal website, 20th October 2023. (https://www.insurancejournal.com/news/international/2023/06/15/725342.htm)
- Cyber talk (2022) Alarming wind-energy cyber-attacks in Europe, Cyber talk website, 20th October 2023. (https://www.cybertalk.org/alarming-wind-energy-cyber-attacks-in-europe/)
- PV-magazine (2022) Satellite cyber-attack paralyzes 11GW of German wind turbines, PV Magazine website, 22nd October 2023. (https://www.pv-magazine.com/2022/03/01/satellite-cyber-attack-paralyzes-11gw-of-german-wind-turbines/)
- Montreal gazette (2023) Pro-Russian group takes responsibility for cyberattack on Hydro-Québec, Montreal gazette website, 22nd October 2023. (https://montrealgazette.com/news/local-news/hydro-quebec-website-and-app-blacked-out-in-cyberattack)
- Industrial cyber security pulse (2023) Throwback Attack: Korea Hydro and Nuclear Power highlights the vulnerability of critical systems, Industrial cyber security pulse website, 22nd October 2023. (https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-korea-hydro-and-nuclear-power-highlights-the-vulnerability-of-critical-systems/)
- Utility dive (2021) Colonial Pipeline hack highlights grid disruption risks even with IT-focused cyberattack, Utility dive website, 22nd October 2023. (https://www.utilitydive.com/news/colonial-pipeline-hack-highlights-grid-disruption-risks-even-with-it-focuse/)
- Utility dive (2021) Electric sector can learn from the Florida water utility hack, Utility dive website, 22nd October 2023. (https://www.utilitydive.com/news/electric-sector-can-learn-from-the-florida-water-utility-hack-say-experts/594914/)
- Australian Cyber Security Center (2022) Cyber incident response plan, Australian Signals Directorate website, 22nd October 2023. (https://www.cyber.gov.au/sites/default/files/2023-03/ACSC%20Cyber%20Incident%20Response%20Plan%20Guidance_A4.pdf)
- Office of the Australian Information Commissioner (2019) Data breach preparation and response, Office of the Australian Information Commissioner website, 22nd October 2023.

(https://www.oaic.gov.au/__data/assets/pdf_file/0017/1691/data-breach-preparation-and-response.pdf)

- Microsoft (2018) Hackers hit Norsk Hydro with ransomware, Microsoft news website, 25th October 2023. (https://news.microsoft.com/source/features/digital-transformation/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/)