Assignment 3 – Strategy Execution Document

Subhikaran GANESH KUMAR - 10609551

Department of Science: Edith Cowan University

CSI6130 – Cyber Security Management

Dr David COOK

17th May 2024

**Introduction**

Alinta Energy (2023) has mentioned in their sustainability report of the year 22/23 that they recognise the cyber risks of the power sector. Alinta Energy (2023) claimed that they implemented solid security complying with the regulatory standards of Security of Critical Infrastructure Act (SOCI). Furthermore, Alinta Energy complies with the Australian Energy Sector Cyber Security Framework (AESCSF). Additionally, Alinta Energy (2023) have mentioned that they collaborated with security firms to improve overall security posture of the company. Alinta Energy (2023) claimed to have taken the steps to mitigate the actions that could lead to data breach and cyber-attacks. However, from the previous report, it was found that Alinta Energy has compromised customers’ critical data. Additionally, from reddit forums, it came to light that there have been cases of digital meter hacks leading to billing frauds and inconsistent meter readings. Despite the steps taken by Alinta Energy, there are vulnerabilities relating to customers privacy and digital electric meters. This proves that Alinta Energy need to improve their cyber defence and preparedness. With the implementation of solid strategy and approach, Alinta Energy can counter against potential cyber threats and develop adaptability to constantly evolving cyber risks environment.

**The business case for strategy**

Cyber attacks targeting the power sectors are on the rise and are constantly evolving. This claim is supported by the General Electric article written by Hetz (n.d.). Furthermore, he also stated that the number of threat actors are increasing and constantly improving their tactics to break into the systems to their advantage. In the case of colonial pipeline attack, important credentials are stolen to access critical data which resulted in considerable financial losses (Hetz, n.d.). Conclusively, the presence of cyber security is crucial for protecting power and utility sector. Hetz (n.d.) mentioned that ransomware is the leading cyber threat in the sector. Industrial control systems (ICS) attacks are riskier and can lead to the damage of public safety (Hetz, n.d.). In the article by Hetz (n.d.), it was claimed that in 2021 that increasing number of vulnerable ICS products are manufactured by big power organisations. Over 70% of the products were rated as critical or high severity. Consequently, this gives an opportunity for an attacker to exploit this for his own profit and cause significant damage to the reputation of the organisation. Furthermore, there has been numerous attacks on remote controls on wind farms and disabled prepaid digital meters leading information and privacy breaches like credit card details and phone numbers (Casanovas & Nghiem, 2023). The average loss concurred due to data breaches is around 4.72 Million USD in the energy sector (Casanovas & Nghiem, 2023). In the article by IEA (2021) stated that entire protection of organisation from cyber threats is impossible but it is essential to continue the critical infrastructure operations. The article stated the importance of key roles needed to be taken by policy makers and regulators to ensure cyber resilience of the organisation. In conclusion, it is essential for Alinta Energy to give more attention to the side of cyber security when it comes to Industrial control systems (digital power meters) and data protection to avoid potential financial losses and reputation damage to the organisation.

**The Strategy for the Leadership Team**

Threat actors targeting Industrial control systems and data are one of the largest threats to power and utilities sectors. It is essential for Alinta Energy to follow Cyber security best methods and practices to protect the organisation’s business continuity and safeguard from cyber-attacks. This is further supported by Hetz (n.d.) in his article in General electric. Therefore, the investment on cyber security from the top management is essential to ensure the smooth running of the business from Alinta.

In the United States, regulatory frameworks like North American Electric Reliability Corporation also insist to respond to evolving cyber threats so that the organisation can work efficiently during any cyber incidents. And also, the article stated that mitigating cyber risks is constant evolving process and is reliant on an organisation to implement certain steps ( United States Energy Association [USEA], 2021).

Alinta Energy needs a 24/7 monitoring solution to alert the security team in case of any failures or major incident. Consequently, detecting any failure in smart digital meter as quickly as possible reduces the impact of financial losses to customers and the organisation. This is further supported by Hetz (n.d.) in his article. Also, it was mentioned in his article that AmeriGas organisation were able to prevent the data breach with the help of this continuous monitoring system in eight seconds. With the deployment of tactical threat intelligence can help the organisation to get insights immediately on the attacks and stop them (Bailey et al., 2020). Consequently, it is effortless for the company to mitigate risks to the operations. Investments to enhance the security of smart meters are required to prevent the exploitation of customers data and billing fraud. As smart meters require encryption-based algorithms to safely transfer the customer data to the organisation without any third parties accessing the data. This claim is further supported by Tupe (2023) in her article in EE power. It is vital for Alinta Energy to have regular software and firmware updates for the smart meters and intrusion detection systems to avoid any potential data breaches as mentioned by Cormack (2017) in the Sydney Morning Herald magazine.

ISO 22301 standard will aid in the process of improving cyber resilience of Alinta Energy by protecting the customers’ privacy and maintaining the reputation of the organisation. ISO 22301 improves risk management and business continuity even in cases of any cyber breach.

As a result, this can prevent the manipulation of Energy usage data increasing the reliability and efficiency of Alinta’s smart meters. Finally, employee training and awareness is essential to educate the employees on data security best practices. Accordingly, Alinta Energy can adapt a culture of awareness and vigilance within the organisation.

**The strategy for your Cyber Team**

Alinta Energy’s internal cyber security team has a very important role of strengthening the cyber resilience of the organisation using strategy ensuring alignment with company’s objectives and principles. The strategy is divided into four step process.

Risk Assessment and Planning: Regular risk assessment is essential to get a detailed view of cyber risks to an organisation (Unni, 2022). In Alinta Energy, risk assessment is conducted to know about the data protection measures and the current smart meter security. Additionally, it is important to decide on certain areas of improvement.

Technical Improvement on Smart meters: After the risk assessment steps, it is vital to incorporate technologies like access control, data encryption and anomaly detection of any malicious intentions to smart meters to make it secure enough (Tupe, 2023).

Regular updates on smart meters: Implementation of regular software and firmware updates is needed to keep smart meters free of any vulnerabilities even after deployment.

Continuous monitoring and logging: Strong monitoring and logging mechanism to monitor and analyse the data traffic going in and out from the smart meters. This would help identify potential threats and malicious activities. Additionally, it enables to act as quickly as possible.

It is needed to assess the skill set of the cyber security team to identify any gaps in knowledge. Also, it would be necessary to arrange specific training programmes to enhance the skill set of the employees. This would also be helpful to identify if additional resources are required for the team.

The annual cybersecurity budget of a large energy company, like Alinta Energy, may be anywhere from $10 million to $15 million. This funding supports a robust infrastructure for cybersecurity, encompassing advanced monitoring systems, comprehensive employee training, incident response capabilities, continuous risk assessments, and strict security measures intended to safeguard vital data and infrastructure in a high-risk industry. To protect the energy sector from frequent, serious threats, this funding is essential. Therefore, investing in cyber security can protect the organisation and can bring safety to the customers and their privacy.

The timeline of this strategy implementation will depend on complexity of the technical challenges and resource availability. However, the approximate timeline for the implementation is expected to be around 15 months.

**The Strategy for the organisation/staff/employees/stakeholders**

Cyber security should recognize every member of the organisation as a integral part to protect against cyber risks (Institute of Data, 2024). By adapting a culture of security awareness and training, it can ensure that everyone in Alinta Energy understands their responsibility in protecting Alinta Energy’s digital assets.

The first step is educating employees by conducting training sessions for employees for good password practices, phishing and safe browsing practices (Institute of Data, 2024). Additionally, it is essential to provide specialised training for employees with elevated privileges.

Clear communication is essential to keep employees updated about the cyber risks and practices that are best for Alinta Energy. With the help of cyber security updates in the magazines, newsletters and a committed email to communicate across would be vital (EC Council, 2023). Staff should be encouraged to speak out about any security incidents or any suspicious activities through the provided communication channels.

Incentive programs to reward and recognize employers who follow cyber security best practices and who contribute to the development of cyber resilience in Alinta Energy (Australian Signals Directorate, 2023). These programs can motivate employees to develop a sense of collective ownership in contributing to the overall cyber security of the organisation.

With the help of regular feedback from the employees, evaluation of the efficiency of the policy can be done. Employee involvement can encourage the staff members to be a part of protecting the organisation from cyber threats. By adapting a sense of cyber security awareness, collaboration and ownership, Alinta Energy can become more resilient in terms of cyber security and protect the reputation and values of Alinta Energy.

**Conclusion**

The security strategy for strengthening smart power meters and protecting the customers’ privacy has been explained in an understandable manner. The strategy to protect digital meters should help mitigate the risk of unauthorised access and data manipulation leading billing fraud and inaccuracy. With the usage of encryption protocol in smart meter can help keep the customers’ sensitive information safe. The strategy also highlights the importance of involvement of all members in Alinta Energy. The strategy focuses on strengthening the relationship and mutual understanding between staff members and the cyber security team. This helps Alinta Energy foster a sense of culture in emphasising the shared responsibility of keeping the organisation cyber resilient.

**References**

Alinta Energy. (2023). *Sustainability Report 22/23*. Alinta Energy | Australian Energy Supplier - Alinta Energy. <https://www.alintaenergy.com.au/content/dam/alinta/documents/sustainability-reports/Alinta%20Energy%20FY23%20Sustainability%20Report.pdf>

Australian Signals Directorate. (2023). *Protecting your staff*. <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/protecting-your-business-and-employees/protecting-your-staff/>

Bailey, T., Maruyama, A., & Wallance, D. (2020, November 3). *The energy-sector threat: How to address cybersecurity vulnerabilities*. McKinsey & Company. <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-energy-sector-threat-how-to-address-cybersecurity-vulnerabilities>

Casanovas, M., & Nghiem, A. (2023, August 1). *Cybersecurity – is the power system lagging behind?* IEA. <https://www.iea.org/commentaries/cybersecurity-is-the-power-system-lagging-behind>

Cormack, L. (2017, April 26). *Smart meters questioned for their security and privacy safeguards*. The Sydney Morning Herald. <https://www.smh.com.au/business/consumer-affairs/smart-meters-questioned-for-their-security-and-privacy-safeguards-20170426-gvsoxx.html>

EC Council. (2023, June 15). *Effective communication in cybersecurity law: Best practices for organizations*. Effective Communication in Cybersecurity Law: Best Practices for Organizations. <https://www.eccu.edu/blog/technology/how-to-effectively-communicate-cybersecurity-best-practices/>

Hetz, M. (n.d.). *Managing cyber risks in the power sector | GE gas power*. General Electric. <https://www.gevernova.com/gas-power/resources/articles/2021/managing-cybersecurity-risks-in-power-sector>

IEA. (2021). *Enhancing cyber resilience in electricity systems*. <https://www.iea.org/reports/enhancing-cyber-resilience-in-electricity-systems>

Institute of Data. (2024, April 3). *The importance of cyber security in the workplace*. <https://www.institutedata.com/blog/cyber-security-in-the-workplace/>

Tupe, S. (2023, March 23). *Mitigating Smart Meter Security Risk: A Privacy-preserving Approach*. EE POWER. <https://eepower.com/technical-articles/mitigating-smart-meter-security-risk-a-privacy-preserving-approach/>

Unni, A. (2022, March 28). *How to develop a strong cybersecurity strategy*. Australia's #1 Cybersecurity Services Company | StickmanCyber. <https://www.stickmancyber.com/cybersecurity-blog/how-to-develop-a-strong-cybersecurity-strategy>

United States Energy Association. (2022, June 16). *USEA releases cybersecurity and Digitalization Handbook for Electricity Sector*. <https://usea.org/article/usea-releases-cybersecurity-and-digitalization-handbook-electricity-sector/>