Assignment 2 – Written Report

Subhikaran GANESH KUMAR - 10609551

Department of Science: Edith Cowan University

CSI6130 – Cyber Security Management

Dr. David COOK

19th April 2024

# **Alinta Energy Evaluation**

**Introduction**

Alinta is one of the biggest power companies, investors, generators and developers (Alinta Energy, 2024a). Since the last decade, they have grown from being the big gas retail company in Western Australia to sell power and gas for over 1 million homes and businesses in Australia (Alinta Energy, 2024a). Furthermore, Alinta Energy owns power stations operating in Australia and New Zealand (Alinta Energy, 2024a).

Alinta Energy recognises the importance of cyber security within its operational framework (Alinta Energy, 2024a). They have implemented a cyber posture that is designed to address evolving digital threats (Alinta Energy, 2024a). Additionally, they try to maintain the trust of their customers. However, there seems to some flaws in their existing cyber security posture that lead to various data breaches and vulnerabilities that affect their digital meters.

**Asset Management**

The focus of the organisation is centered on the entire energy value chain which includes energy generation, storage, transmission, distribution and energy retailing (Alinta Energy, 2023a). Alongside, Alinta Energy works on the innovative management of energy storage solutions (Alinta Energy, 2023a). Evidently, it can be concluded that Alinta produces energy in various form (electricity and gas) to wide range of customers, which includes individuals and large businesses. Moreover, Alinta is interested in developing sustainable and efficient energy solutions for the customers (Alinta Energy, 2023a).

Asset management within Alinta Energy is primarily focused with safeguarding and optimizing these crucial operational assets: the physical infrastructure for energy production ,storage (battery systems), and the networks that allow for the effective transmission and distribution of energy (Alinta Energy, 2023b). Therefore, these assets are very critical for maintaining and developing the organisation’s market capitalisation in a very competitive environment. As Alinta Energy directly deals with customer to provide their services, maintaining and safeguarding users’ data becomes one of the important aspects in asset managements (Alinta Energy, 2023b). Consequently, the asset management is not only for compliance for legal and regulatory standards but also required for maintaining trust and integrity in customer relationships.

**Business Environment**

Alinta is one of the key players in the Australian power sector, navigates a complex business environment characterized by the many-sided challenges and opportunities presented by the evolving energy market (Alinta Energy, 2023b). Competition is inevitable among the energy sector in the Australian market to provide value for the customers in the long run (Independent Pricing and Regulatory Tribunal [IPART], 2023). In the absence of competition, there are less incentives for businesses to become more efficient and reliable over time (IPART, 2023). Alinta Energy is in the top eight leading energy companies in Australia, both production and distribution of electricity and gas to residential and commercial clients (Savvy, 2023). According to Savvy (2023), Alinta Energy offers services in New South Wales, Queensland, Victoria, South Australia and Western Australia. This is further supported by the Alinta Energy (2023b) in their sustainability report for the year 2022/2023. The main competitors to Alinta energy according to the article by Wringley (2023) are AGL Energy, Origin Energy, Energy Australia. From the Australian Energy Regulator’s report in 2023, Alinta Energy services over 366,520 retail energy clients, and they own around 5.40% of the market share in the electricity sector. Alinta have about 84,300 customers for gas retail, representing 3.7% of the retail gas market share as mentioned by Savvy (2023). The key stakeholders as mentioned by Alinta Energy (2021) in their sustainability report are customers, employees, suppliers, government, industry associations and the public.

**Governance**

Alinta Energy Pty Ltd and Renewable Energy Infrastructure Fund Pty Ltd (known as Alinta Energy) are owned by a Hong Kong-based company named Chow Tai Fook Enterprises Limited and Pioneer Sail Australia Pty Limited (Alinta Energy, 2024b). Alinta Energy is a major player in the Australian power sector, which operates under an organised governance framework designed to ensure accountability, strategic oversight, and compliance with industrial rules (Alinta Energy, 2024a). Additionally, Alinta Energy (2024b) has a diverse range of board members with skills and experience to enhance decision making processes in fields of energy, trading, finance, retail markets, information security etc, Alinta Energy’s board consists of 9 members (Alinta Energy, 2024b). The organisation consists of 4 independent non-executive directors including the Chair, 4 non-executive directors, and a Managing Director and additionally they have a Chief Executive Officer named Jeff Dimery (Alinta Energy, 2024b). The board have a monthly meeting in order to discuss about the governance across the organisation (Alinta Energy, 2024b). Furthermore, it was stated by Alinta that Chief Information Officer is Nick Smith.

As it can be inferred that Alinta Energy has a strong presence of cyber security in their board of committee. The inclusion of cyber security on the board is critical as it ensures strategic approach of cyber risk management, protecting clients’ data and critical infrastructure from potential cyber threats (Horne, n.d.).

**Risk Assessment**

Alinta Energy's approach to risk management specifies a low tolerance for privacy risks, emphasizing protection, compliance and vigilance (Alinta Energy, 2023a). Alinta Energy’s approach is aligned with best practices for protecting sensitive data in the power sector, where data security is critical to maintaining customer trust and meeting regulatory expectations (Alinta Energy, 2023a). This demonstrates a low risk appetite concerning the customer’s data. Despite having a strong presence of cyber security in the board and complying with the Australian Energy Sector Cyber Security Framework, Alinta Energy has failed to protect customers’ data from breaches as mentioned in the Morning Sydney Herald magazine (Ferguson & Gillett, 2020). Alinta seemed to have collected sensitive information like medicare, passport and credit card details through its retail operations according to Ferguson and Gillett (2020) in the magazine. They mentioned that it was found out from the audit done by EY that Alinta Energy got a very high cyber risk ranking on the aspects of privacy. The EY audit report further stated that there were no policies/frameworks to handle the company’s sensitive information (Ferguson & Gillett, 2020). Energy sector organisations are prone to cyberattacks, but an organised process that involves communication, organizational, and process frameworks can considerable mitigate cyber risks (Bailey et al., 2020). Especially with the introduction of technology in the power sector, the industry is more exposed to data theft, billing fraud and ransomware (Bailey et al., 2020). ‘Smart meters’ can be a major threat when it comes to billing fraud and information theft (Bailey et al., 2020). Consequently, after the introduction of smart meters by Alinta Energy has faced some heat from the customers regarding the billing frauds. Imjordo (2023) claimed that the electricity bills were significantly even though the electric usage in app is considerably shown low. He also seemed to find out that there were a lot of inconsistencies in amount bills regularly. Similarly, an 80-year old pensioner named Mary has been faced with billing fraud leading to a bill of $23000 dollars as mentioned by Herst (2023). Evidently, Alinta Energy seems to fail to protect user’s data and prevent billing frauds on smart/digital meters despite having a strong presence of cyber security in board.

**Risk Management Strategy**

Alinta Energy (2023b) claimed that they use AS/NZS ISO 31000 in their financial disclosures report. Since Alinta Energy handles personal and sensitive customers’ information it is critical to implement a standard that aligns with industry best practices. From the risk assessment of Alinta Energy, it is inferred that they are prone to cyber attacks and data theft. It is vital to have a basic understanding of how a smart/digital meter communicates with the network and disable any foreign network connections and devices (CISA, n.d.). To protect smart meters from cyber risks it is critical to ensure they are connected only to intended systems and consider the smart meters for regular security fixes and software updates (CISA, n.d.). It is important to provide awareness for system engineers who work on smart meters or IIoT environments on the importance of cybersecurity in a connected IIoT environment (CISA, n.d.). Evidently, Alinta Energy requires a vital cyber resilience plan. ISO 22301 is a standard that looks exclusively to business continuity management (International Organization for Standardization [ISO], 2019). The ISO 22301 standard highlights potential risks to a company as well as the consequences of the risks to business functioning caused by those vulnerabilities (ISO, 2019). It provides a plan/framework to make the organisation resilient and could provide an efficient response that will protect the organisation’s brand, reputation and its customers (ISO, 2019). ISO 22301 also gives a clear and descriptive picture of how a company should function, highlighting details that are important for strategic planning, cyber risk management, supply chain management, business transformation and resource handling (ISO, 2019). This framework helps the company to recover quickly and be competitive in the market compared to its competitor companies (NQA, n.d.). In the long run, a company can reap reputational benefits that will lure the customers as well as benefit from good financial abilities (NQA, n.d.).

**Conclusion**

Alinta Energy is one of major power companies in Australian energy sector. They strive to protect customers’ data and have a cyber presence in their board of committee. Alinta Energy follows ISO 31000 standard for their risk management. However, it is recommended to the ISO 22302 standard (Business continuity management) to help identify with potential threats and quick recovery in case of any cyber-attacks. Additionally, Alinta Energy should focus on the cyber risks caused by digital power meters.

Top of Form

**References**

Alinta Energy. (2021). Sustainability Report 2020/2021. <https://www.alintaenergy.com.au/-/jssmedia/alinta-website/documents/about/ae-sustainability-report-fy21.pdf?rev=5aa29f14c5f8473fa3e4e1f10ed1a6a7>

Alinta Energy. (2023a). Alinta Energy Climate-related Financial Disclosures Report. <https://www.alintaenergy.com.au/content/dam/alinta/documents/sustainability-reports/FY23-TCFD-Report%20FINAL%20TO%20PUBLISH.pdf>

Alinta Energy. (2023b). Sustainability Report 2022/2023. <https://www.alintaenergy.com.au/content/dam/alinta/documents/sustainability-reports/Alinta%20Energy%20FY23%20Sustainability%20Report.pdf>

Alinta Energy. (2024a). About us | Energy company. <https://www.alintaenergy.com.au/content/alinta/au/en/about-us/who-we-are.html>

Alinta Energy. (2024b). Governance, risk management and compliance. <https://www.alintaenergy.com.au/about-us/who-we-are/governance-risk-management-and-compliance>

Alinta Energy. (n.d.). Smart Meters | Meters & Connections. Alinta Energy | Australian Energy Supplier - Alinta Energy. <https://www.alintaenergy.com.au/content/campaigns/alinta-energy/master/personalise-by-state/nsw_users/smart-meters-experiencefragment3/jcr:content/par.html>

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>

CISA. (n.d.). Cyber-Physical Security Considerations for the Electricity Sub-Sector. <https://www.cisa.gov/sites/default/files/publications/Sector%20Spotlight%20Cyber-Physical%20Security%20Considerations%20Electricity%20Sub-Sector%20508%20compliant.pdf>

Ferguson, A., & Gillett, C. (2020, March 1). Credit cards, addresses and phone numbers vulnerable: More than one million energy customers’ privacy at risk. The Sydney Morning Herald. <https://www.smh.com.au/business/companies/credit-cards-addresses-and-phone-numbers-vulnerable-more-than-one-million-energy-customers-privacy-at-risk-20200228-p545bw.html>

Hirst, A. (2023, May 26). 80-year-old pensioner's win after battling energy company over $23k bill. 9Now - Watch Channel 9 Live and On Demand. <https://9now.nine.com.au/a-current-affair/victorian-pensioners-win-after-battling-alinta-energy-over-23k-bill/c8132f47-b77a-478d-bb73-28342bdd2474>

Horne, R. (n.d.). Cyber security governance. PwC UK. <https://www.pwc.co.uk/issues/cyber-security-services/insights/governing-cyber-security-risk.html>

Imjordo. (2023). Incredibly high bills. Reddit. <https://www.reddit.com/r/AusFinance/comments/17voxf3/incredibly_high_power_bill/>

Independent Pricing and Regulatory Tribunal. (2023). Competition in the energy markets. <https://www.ipart.nsw.gov.au/competition-energy-markets>

International Organization for Standardization. (2019). Business continuity ISO 22301. <https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100442.pdf>

NQA. (n.d.). ISO 22301:2019 BUSINESS CONTINUITY STANDARD IMPLEMENTATION GUIDE. <https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/NQA-ISO-22301-Implementation-Guide.pdf>

Savvy. (2023, August 14). Alinta energy. <https://www.savvy.com.au/energy/alinta-energy/>

Wrigley, K. (2022, December 5). Largest energy companies in Australia – Canstar blue. Canstar Blue. <https://www.canstarblue.com.au/electricity/largest-energy-companies-australia/>