# **Cybersecurity Threat Model Report for Endeavor Energy (Australia)**

**1. Executive Summary**

This report addresses the critical need for a comprehensive cybersecurity threat model tailored to Endeavor Energy's electricity distribution network in New South Wales, Australia. As a major operator within the Australian National Electricity Market (NEM), Endeavor Energy is designated as critical infrastructure, making the security of its operational technology (OT) and information technology (IT) systems paramount. The increasing frequency and sophistication of cyber threats targeting the energy sector globally and within Australia necessitate a proactive and robust approach to risk management. Furthermore, Endeavor Energy is subject to regulatory obligations under the Security of Critical Infrastructure Act 2018 (SOCI Act) and is expected to align with frameworks such as the Australian Energy Sector Cyber Security Framework (AESCSF) and the Australian Cyber Security Centre (ACSC) Essential Eight.

The scope of this assessment encompasses Endeavor Energy's key OT systems, including Supervisory Control and Data Acquisition (SCADA) systems, which provide real-time visibility and control over the electricity network 1; Distribution Management Systems (DMS), used for real-time network management and optimization 2; protection relays, vital for grid stability; and Remote Terminal Units (RTUs), which acquire data from field devices. The assessment also covers the IT systems that support operations, such as enterprise resource planning (ERP) systems like Ellipse, used for financial and asset management, and customer information systems like Banner, which manages customer databases and billing 1. The communication networks facilitating these operations, including SCADA communication networks potentially utilizing private radio, fiber optics, or cellular technologies 3; corporate IT networks; field crew communication systems; and IoT networks connecting embedded devices, are also within the scope. Finally, the report considers embedded devices such as smart meters, part of the Advanced Metering Infrastructure (AMI) 4; Intelligent Electronic Devices (IEDs) located in substations; and other field devices deployed across Endeavor Energy's network.

Open-source intelligence (OSINT) analysis reveals significant threats targeting the Australian energy sector, including ransomware attacks on both IT and OT systems, and supply chain attacks 6. Incidents such as the ransomware attack on CS Energy in Queensland highlight the real-world impact of these threats 8. The increasing interconnectedness of OT and IT systems, a trend noted in ACSC reports 6, presents a substantial attack vector. The ongoing modernization of the grid, with its growing reliance on software and third-party vendors 10, further expands the potential attack surface. This necessitates a security strategy that addresses vulnerabilities across all these interconnected domains.

To mitigate these risks, several key strategies are recommended. Implementing robust network segmentation to isolate IT and OT networks 13 is crucial to prevent lateral movement of attackers. Strengthening identity and access management, particularly for administrative privileges 15, will limit the potential impact of compromised accounts. Enhancing vulnerability management and patching processes, especially for OT systems where operational uptime is critical 17, is essential to address known weaknesses. Finally, developing comprehensive incident response plans specifically tailored for OT environments will ensure that Endeavor Energy is prepared to effectively manage and recover from cyber incidents. These recommendations align with Australian standards such as the Essential Eight, the AESCSF, and the requirements of the SOCI Act.

**2. Introduction**

Endeavor Energy operates the electrical distribution network for Greater Western Sydney, the Blue Mountains, the Southern Highlands, and the Illawarra region of New South Wales, Australia 19. This network connects over 2.7 million people to both traditional and renewable energy sources across a significant geographic area 20. As a critical participant in the Australian National Electricity Market (NEM) 19, Endeavor Energy plays a vital role in ensuring the reliable supply of electricity to a substantial portion of NSW. The company is currently transitioning from a traditional 'poles and wires' business model to that of a distributed system operator, embracing new technologies and working collaboratively with customers, stakeholders, and regulators to facilitate a clean energy future 10. This evolution involves the integration of advanced technologies such as smart meters and distributed energy resources, which, while offering significant benefits, also introduce new complexities and potential security vulnerabilities.

The need for robust cybersecurity within Australia's energy infrastructure, including Endeavor Energy's distribution network, is paramount. Disruptions to electricity supply can have far-reaching consequences, including blackouts that impact essential services, safety risks arising from the potential malfunction of critical equipment, and significant economic disruption affecting businesses and the broader community. The ACSC's 2023-24 report highlights the increasing number of cyber threats targeting the energy sector and critical infrastructure, with over 11% of incidents they responded to affecting this sector 6. Endeavor Energy, given its extensive service area and the number of people reliant on its network, represents a critical component of this infrastructure. The Australian government recognizes the severity of these risks through legislation such as the SOCI Act 23, which mandates enhanced security protocols and incident reporting for essential services like energy. Recent amendments to the SOCI Act, including those in the Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024 24, further underscore the importance of a proactive and comprehensive approach to safeguarding critical infrastructure assets. The increasing digitization of the energy sector, driven by the adoption of smart grids, renewable energy integration, and initiatives like Endeavor Energy's Advanced Metering Infrastructure (AMI) 4 and flexible export capabilities 3, introduces new cyber vulnerabilities that must be addressed effectively. The rise in cybercrime, as detailed in ACSC reports 26, and the specific targeting of critical infrastructure necessitate a strong security posture for Endeavor Energy to protect its operations and the communities it serves.

The primary objectives of this report are to provide Endeavor Energy with a comprehensive analysis of potential cybersecurity threats to its OT and IT infrastructure. This will be achieved through the application of the MITRE ATT&CK framework for ICS 27 to understand adversary tactics and techniques relevant to its operational environment. The report will also utilize the EMB3D Threat Model 32 to specifically analyze threats targeting embedded systems within Endeavor Energy's infrastructure, such as smart meters, RTUs, and IEDs. Furthermore, open-source intelligence (OSINT) methodologies will be employed to gather information on relevant cyber threats, threat actors, and vulnerabilities specific to the Australian energy sector and potentially Endeavor Energy itself. The findings of this analysis will be aligned with relevant Australian cybersecurity regulations and frameworks, including the SOCI Act, the AESCSF 37, and the Essential Eight 15. Ultimately, the goal of this report is to provide actionable security improvements and mitigation strategies for Endeavor Energy's engineering, operations, and security teams, enabling them to enhance the resilience of their critical infrastructure against evolving cyber threats.

**3. Methodology**

The cybersecurity threat model developed in this report leverages a combination of established frameworks and intelligence gathering techniques to provide a comprehensive analysis of potential risks to Endeavor Energy's infrastructure.

The MITRE ATT&CK framework for Industrial Control Systems (ICS) serves as a foundational element of this methodology. This framework is a globally accessible knowledge base that meticulously catalogs adversary tactics and techniques observed in real-world attacks against industrial control systems 27. It provides a structured taxonomy of these behaviors, enabling security teams to better understand, assess, and ultimately improve the resilience of critical operational technology (OT) environments against cyber threats 27. The relevance of this framework to Endeavor Energy lies in its ability to provide a structured lens through which to analyze threats targeting its specific control systems, such as SCADA and DMS, as well as its broader operational processes 27. By mapping potential attack scenarios against the various tactics outlined in the framework, which include Initial Access, Execution, Persistence, Privilege Escalation, Evasion, Discovery, Lateral Movement, Collection, Command and Control, Inhibit Response Function, Impair Process Control, and Impact 27, Endeavor Energy can gain a deeper understanding of the potential progression of an attack within its OT environment. This understanding is crucial for developing a proactive and threat-informed defense strategy. Focusing on key aspects like real-time visibility, comprehensive logging, and robust network segmentation are essential for effectively leveraging the MITRE ATT&CK for ICS framework 27.

Complementing the MITRE ATT&CK for ICS framework is the EMB3D Threat Model. This model is specifically designed to address the unique security challenges associated with embedded devices, which are increasingly prevalent in critical infrastructure and other sectors 32. For Endeavor Energy, this model is particularly relevant to securing embedded systems such as Remote Terminal Units (RTUs), smart meters that form part of the Advanced Metering Infrastructure (AMI) 4, and Intelligent Electronic Devices (IEDs) deployed across its network. The EMB3D model functions by mapping known cyber threats to specific properties of these embedded devices and proposing corresponding mitigation strategies 33. Its key components include the enumeration of Device Properties, such as hardware architecture, system software, and networking capabilities 33, as well as physical hardware, network services and protocols, software, and firmware 32; the identification and description of Threats, detailing how threat actors can achieve their objectives or cause specific effects 32; and the provision of Mitigations, categorized into foundational, intermediate, and leading tiers based on their complexity and effectiveness 33. Given the increasing number of security advisories related to industrial control systems issued by organizations like CISA 34, a targeted approach to securing embedded devices, as offered by the EMB3D model, is essential for Endeavor Energy.

Open-source intelligence (OSINT) gathering forms a critical part of this threat modeling process, providing valuable real-world context and insights specific to Endeavor Energy and the Australian energy sector. This involves the systematic collection and analysis of publicly available information from a variety of sources. Searches are conducted for information on threats specifically targeting Australian energy utilities, leveraging keywords related to "Australian energy cyber attacks" and "ICS security Australia." Efforts are also made to identify any publicly disclosed vulnerabilities related to Endeavor Energy's technology stack. Furthermore, the OSINT process includes a thorough analysis of regulatory reports issued by key Australian bodies, such as the Australian Energy Market Operator (AEMO), which publishes reports on cyber security preparedness within the energy sector 40 and incident reports 41; the Australian Energy Regulator (AER), which provides regulatory oversight of the energy sector and may publish relevant information on network assets and regulations 1; and the Australian Cyber Security Centre (ACSC), which issues government cybersecurity advisories, including annual threat reports 6 and principles for OT cyber security 13. Additionally, Australian energy sector news articles and industry publications are reviewed to identify reports of cyber incidents or emerging threats 7. This focus on Australian sources ensures that the threat model is aligned with the specific threat landscape and regulatory environment within which Endeavor Energy operates.

The threat modeling process itself involves a structured approach to identify, analyze, and prioritize potential cybersecurity risks. Information gathered through OSINT is used to inform the application of both the MITRE ATT&CK for ICS and EMB3D frameworks, ensuring that the analysis is grounded in real-world threats and vulnerabilities. Potential attack vectors are mapped against Endeavor Energy's likely system architecture, as detailed in Section 4 of this report, using the constructs provided by these frameworks. Risk assessment methodologies are then employed to evaluate the likelihood of different threats materializing and to assess the potential severity of their impact on Endeavor Energy's operations, considering factors such as safety, reliability, compliance with regulations, and overall business operations. This systematic approach allows for the prioritization of mitigation efforts, focusing resources on addressing the most significant risks to Endeavor Energy.

It is important to acknowledge certain assumptions and limitations inherent in this assessment. Due to the reliance on open-source information, assumptions may have been made regarding specific network configurations or technology deployments within Endeavor Energy's environment, based on typical architectures observed in Australian distribution networks 3. The assessment is also limited by the lack of direct access to Endeavor Energy's internal systems and security posture. As a result, the threat model presented in this report should be considered a snapshot in time, reflecting the current understanding of the threat landscape based on publicly available information. The cybersecurity threat landscape is constantly evolving, necessitating regular updates and reviews of this threat model to ensure its continued relevance and effectiveness.

**4. Endeavor Energy System Overview**

Understanding the architecture and key components of Endeavor Energy's operational environment is crucial for effectively identifying and mitigating potential cybersecurity threats. Based on typical Australian electricity distribution network structures and available public information, the following provides an overview of Endeavor Energy's likely system architecture and operational roles.

At the core of Endeavor Energy's operations are its Network Operations Centre(s), which serve as the central hub for monitoring and controlling the vast electricity distribution network. Within these centres, Supervisory Control and Data Acquisition (SCADA) systems play a critical role in providing real-time visibility into the status of the network and enabling remote control of field devices such as circuit breakers and transformers 1. This information from the SCADA system often feeds into an Outage Management System (OMS), which is used for logging outages and other network events, as well as for calculating reliability reporting information 1. Complementing the SCADA system is the Distribution Management System (DMS), which is used for real-time management and optimization of the distribution network. DMS functionalities likely include advanced applications for outage management, load forecasting, voltage control, and network analysis 2. Systems like ETAP ADMS offer an integrated platform for these functions, providing intelligent situational awareness and decision support 2. The integrity and availability of these control rooms and their associated SCADA/DMS systems are paramount, as their compromise could lead to a loss of operational visibility and control over the electricity network, potentially resulting in widespread power disruptions.

The electricity distribution grid infrastructure itself comprises a complex network of substations, feeders, poles, wires, and transformers. Endeavor Energy's network includes over 202 major substations and 32,600 distribution substations 20, which step down high-voltage electricity for distribution to consumers. Protection systems, including sophisticated protection relays, are strategically deployed throughout the grid to automatically detect and isolate faults, ensuring the safety and stability of the electricity supply. These protection systems are critical for preventing cascading failures and minimizing the impact of electrical faults. Within substations and along the distribution network, various control and monitoring devices are deployed, including Remote Terminal Units (RTUs), Programmable Logic Controllers (PLCs), and Intelligent Electronic Devices (IEDs). These devices collect data from the field and execute control commands issued from the Network Operations Centre. Cyberattacks targeting these devices could potentially disrupt their operation, leading to incorrect grid operation or even physical damage to equipment. Endeavor Energy's achievement of ISO 27001:2022 certification for its information security management system, covering sixteen critical substations and control rooms 49, highlights the company's recognition of the importance of securing these physical locations and the systems they house.

Endeavor Energy has implemented an Advanced Metering Infrastructure (AMI) program, which involves the deployment of smart meters across its service area 4. These smart meters digitally measure energy consumption, typically in 30-minute intervals, and communicate this data remotely to Endeavor Energy and energy retailers 4. This eliminates the need for manual meter reading and provides near real-time data on power usage. The communication infrastructure for AMI likely utilizes a combination of technologies, such as cellular networks and radio frequency (RF) communication. Endeavor Energy is actively leveraging the data and technology associated with smart meters to plan for the future of the grid, including the seamless integration of distributed energy resources 20. While AMI offers numerous benefits for both Endeavor Energy and its customers, the sheer number of deployed smart meters and their communication links create a significant attack surface that requires careful security considerations.

The operation of Endeavor Energy's electricity distribution network relies on a variety of communication networks. SCADA communication networks are essential for the real-time exchange of data between the Network Operations Centre and field devices. These networks may utilize industrial protocols such as DNP3 or IEC 60870-5-104. Corporate IT networks support business operations, including email communication, data storage, and access to various enterprise systems. Endeavor Energy utilizes several IT systems for different functions, including Cognos for business reporting, Ellipse for financial and asset management, TM1 for budgeting and forecasting, eFrams for telecommunication billing and inventory, Remedy for IT service management, Autocad for computer-aided design, Banner for customer database and billing, and Figtree for worker's compensation claims 1. Field crews and technicians rely on communication systems, potentially including mobile radio and cellular networks, to coordinate their activities in the field. Finally, IoT networks connect smart meters and other distributed devices, enabling the flow of operational data. The security of each of these communication networks is critical, and potential vulnerabilities in one network could be exploited to gain access to other, more sensitive parts of Endeavor Energy's infrastructure.

Effective operation of this complex system requires a diverse range of operational roles. Grid operators and controllers are responsible for the real-time monitoring and control of the electricity network using the SCADA and DMS systems. Field crews and technicians perform essential maintenance, repairs, and installations on the distribution grid infrastructure, often utilizing mobile devices and requiring access to network information. Protection engineers are responsible for the design, configuration, and maintenance of the critical protection systems that safeguard the grid. IT and OT security staff are tasked with implementing and maintaining cybersecurity measures across both the information technology and operational technology environments. Billing and customer service personnel handle customer accounts and billing processes, potentially interacting with data obtained from smart meters. Third-party contractors and suppliers may be granted access to Endeavor Energy's systems for various purposes, such as maintenance, upgrades, or specialized services. Finally, Endeavor Energy interacts with external stakeholders, including the Australian Energy Market Operator (AEMO) for market operations, the Australian Energy Regulator (AER) for regulatory compliance, and its customers for service provision, often through online portals and data exchange platforms. Understanding the roles and responsibilities of these different personnel and their levels of access to critical systems is essential for implementing effective security controls based on the principle of least privilege.

Potential operational disruptions resulting from cyberattacks on Endeavor Energy's systems could have significant impacts. A loss of visibility and control over the network due to a compromise of the SCADA or DMS systems could lead to instability and widespread power outages. Manipulation of protection systems could result in incorrect grid operation, such as unnecessary tripping of circuits or a failure to shed load during emergencies, exacerbating power outages. The most direct and visible impact would be power outages and blackouts affecting residential, commercial, and critical infrastructure customers. Data integrity issues, particularly affecting metering and billing systems, could lead to inaccurate billing and customer disputes. Safety hazards could arise if cyberattacks cause equipment malfunctions, posing risks to both the public and field staff. Furthermore, successful cyber incidents could lead to compliance breaches under the SOCI Act and AEMO rules, resulting in regulatory penalties. In extreme scenarios, sophisticated cyberattacks could potentially cause physical damage to critical grid equipment by manipulating control system parameters. Recognizing these potential operational disruptions and their wide-ranging impacts underscores the critical importance of establishing and maintaining a robust cybersecurity posture for Endeavor Energy.

**5. Threat Landscape Analysis (Australian Energy Sector Focus)**

The Australian energy sector, including electricity distribution network operators like Endeavor Energy, faces an increasingly complex and dynamic cyber threat landscape. This analysis outlines the prevalent threats targeting Industrial Control Systems (ICS) and Operational Technology (OT) within the sector, with a specific focus on the Australian context.

Ransomware attacks pose a significant threat to both IT and OT systems within the energy sector. These attacks can encrypt critical data and lock down essential systems, potentially leading to significant operational disruptions and financial losses as organizations attempt to recover their systems and data. The incident at CS Energy in Queensland 8 serves as a stark example of the impact of ransomware on an Australian energy provider. Globally, the energy sector has witnessed numerous ransomware attacks 50, highlighting the attractiveness of this sector to cybercriminals seeking financial gain. Data breaches represent another major concern, with threat actors targeting both customer data, potentially stored in billing systems or collected through smart meters, and sensitive operational data, such as network configurations and control logic. The compromise of such data can lead to reputational damage, financial penalties, and potential risks to the security and reliability of operations. Denial of Service (DoS) attacks can also be employed to disrupt the availability of critical control systems, preventing operators from effectively monitoring and managing the electricity network, or to take down customer-facing portals, impacting customer service and potentially causing widespread frustration. Supply chain attacks are an increasingly sophisticated threat vector, where adversaries compromise hardware or software used within the energy sector to gain access to their target's systems 11. Given the reliance on specialized vendors and technologies within the energy industry, these attacks can be particularly challenging to detect and mitigate. Furthermore, the threat from malicious insiders, whether intentional or unintentional, cannot be overlooked, as individuals with authorized access to critical systems can pose a significant risk. Finally, the potential for misinformation and disinformation campaigns, leveraging cyber means to spread false or misleading information about the energy supply, could cause public panic and undermine trust in the sector. The interconnectedness of IT and OT environments within the energy sector amplifies these threats, as a breach in one domain can potentially be leveraged to gain access to the other.

Various types of threat actors are known to target energy infrastructure. Nation-state actors, often referred to as Advanced Persistent Threat (APT) groups, are highly sophisticated and well-resourced, with the potential to conduct espionage, sabotage, or pre-position for future disruptive attacks on critical infrastructure like the energy sector 6. Cybercriminal groups, primarily motivated by financial gain, frequently employ tactics such as ransomware and data theft to extort victims 6. Hacktivist groups may target energy companies for ideological reasons, potentially causing disruptions or defacing public-facing websites to promote their agendas. While perhaps less common, terrorist groups could also potentially seek to disrupt energy infrastructure through cyberattacks to cause significant harm and disruption. Finally, insider threats, whether from disgruntled employees or those who have been compromised, represent a persistent risk due to their authorized access to sensitive systems and information. Understanding the motivations and capabilities of these different threat actors is crucial for developing effective defense strategies.

Open-source intelligence (OSINT) analysis provides valuable insights into the specific threats and vulnerabilities relevant to the Australian energy sector. Case studies of cyberattacks on energy distributors and utilities, both globally and within Australia, offer valuable lessons learned. The ransomware attack on CS Energy in Queensland 8 demonstrated the potential for significant disruption, while attacks on Energy Australia and AGL in 2022 7 further highlight the ongoing targeting of the sector. Globally, incidents like the Colonial Pipeline attack 51 illustrate the potential for severe consequences. Analysis of these incidents reveals common Tactics, Techniques, and Procedures (TTPs) employed by attackers against ICS/OT environments, such as phishing campaigns for initial access 6, lateral movement through interconnected networks, exploitation of vulnerabilities in public-facing applications 6, and manipulation of control system parameters 28. Prevalent vulnerabilities commonly found in OT/ICS systems include weak authentication mechanisms, the use of unpatched software 9), and insecure remote access protocols 42. Australian-specific advisories from the ACSC, including their annual cyber threat reports 6, emphasize the persistent targeting of critical infrastructure and provide recommendations for mitigation, such as the implementation of the Essential Eight 9. Reports from AEMO 40 also highlight the state of cyber security preparedness within the Australian energy sector and outline their increasing role in coordinating cyber incident response 54. This comprehensive OSINT analysis underscores the need for a robust and adaptive cybersecurity strategy for Endeavor Energy, informed by the specific threats and vulnerabilities facing the Australian energy sector.

**6. MITRE ATT&CK Mapping for Endeavor Energy**

To provide a structured understanding of potential adversary behaviors within Endeavor Energy's operational technology (OT) environment, this section maps relevant tactics and techniques from the MITRE ATT&CK for ICS framework to the company's likely key systems and protocols. Endeavor Energy's OT environment likely includes SCADA systems utilizing protocols such as DNP3 and IEC 60870-5-104 for communication between control centers and field devices. Industrial control system devices such as PLCs, RTUs, and IEDs are also integral to the operation of the electricity distribution network.

The following table provides an illustrative mapping of relevant MITRE ATT&CK for ICS tactics and techniques to Endeavor Energy's potential environment, based on the threat landscape analysis and system overview:

| **Tactic** | **Technique** | **Description** | **Potential Application to Endeavor Energy** | **Potential Impact** |
| --- | --- | --- | --- | --- |
| Initial Access | Spearphishing Attachment (T0808) | Targeting employees with malicious attachments to gain initial access to the network. | Attackers could target Endeavor Energy employees, including those with access to OT systems, through sophisticated phishing emails containing malicious attachments. | Successful exploitation could provide attackers with a foothold within the IT or OT network. |
| Initial Access | Exploit Public-Facing Application (T0809) | Exploiting vulnerabilities in web-based interfaces or applications exposed to the internet. | With increasing connectivity and remote access requirements, public-facing applications in both IT and OT environments could be targeted by exploiting known or zero-day vulnerabilities. | Allows attackers to gain unauthorized access to internal networks or systems. |
| Execution | Command Injection (T0801) | Injecting malicious commands into control system devices. | If attackers gain access to control system interfaces through compromised accounts or exploited vulnerabilities, they might attempt to inject commands to manipulate devices like RTUs or PLCs. | Could lead to incorrect operation of the grid, equipment damage, or power outages. |
| Persistence | Modify Registry (T0840) | Modifying system registry keys on Windows-based OT systems to maintain persistence. | Many OT environments still rely on Windows-based operating systems. Attackers could modify registry keys to ensure their continued access even after system restarts or credential changes. | Enables attackers to maintain long-term access to compromised systems. |
| Command and Control | Standard Application Layer Protocol (T0857) | Using common network protocols (like HTTP/HTTPS) for command and control to blend in with normal traffic. | Attackers could use standard web protocols to communicate with compromised systems within the OT network, making their traffic harder to detect as it may resemble legitimate network activity. | Allows attackers to remotely control compromised systems and issue commands. |
| Impact | Denial of Service (T0803) | Disrupting the availability of critical control systems or communication networks. | Attackers could launch Denial of Service attacks against critical OT systems like SCADA/DMS servers or the communication networks connecting control centers to field devices, preventing operators from monitoring or controlling the grid. | Could lead to a loss of visibility and control, potentially resulting in instability and outages. |
| Impact | Modify Parameter (T0836) | Altering critical parameters in control system devices to cause equipment malfunction or process disruption 28. | Attackers who gain control over critical control system devices could manipulate parameters that govern the operation of equipment like transformers or circuit breakers, potentially causing them to malfunction or operate outside of safe limits. | Could result in physical damage to equipment, power outages, or safety hazards. |

This mapping provides a foundational understanding of how adversaries might leverage various tactics and techniques from the MITRE ATT&CK for ICS framework to target Endeavor Energy's OT environment. It is important to note that this is not an exhaustive list and further analysis, tailored to Endeavor Energy's specific infrastructure and security posture, would be beneficial.

**7. Applying the EMB3D Threat Model to Endeavor Energy's Embedded Systems**

Endeavor Energy's infrastructure includes a variety of embedded systems that are critical to its operations. These likely include smart meters, which are part of the Advanced Metering Infrastructure (AMI) 4; Remote Terminal Units (RTUs) located in substations for data acquisition and control; Intelligent Electronic Devices (IEDs) also found in substations, performing protection and control functions; and potentially other specialized sensors and controllers deployed throughout the distribution network. Applying the EMB3D Threat Model to these devices helps identify specific vulnerabilities and potential threats based on their inherent properties.

The following table illustrates a mapping of relevant EMB3D threats to the likely device properties of some of Endeavor Energy's embedded systems:

| **Device Type** | **Device Property** | **EMB3D Threat** | **Description** | **Potential Impact** |
| --- | --- | --- | --- | --- |
| Smart Meter (AMI) | Wireless Communication (e.g., RF, Cellular) | Unauthorized Command Injection over Wireless Interface | Attackers might attempt to exploit vulnerabilities in the wireless communication protocols used by smart meters to inject malicious commands. | Could lead to manipulation of meter readings, disconnection of service, or the meter being used as an entry point to other networks. |
| Smart Meter (AMI) | Firmware Storage | Firmware Modification or Corruption | Attackers could try to overwrite or corrupt the firmware of smart meters. | Could render the meter inoperable, allow for manipulation of data, or provide persistent access for malicious activities. |
| Remote Terminal Unit (RTU) | Serial Communication Interfaces (e.g., Modbus) | Exploitation of Insecure Serial Protocols | If RTUs utilize serial communication protocols like Modbus without proper authentication or encryption, attackers with physical or network access could exploit these weaknesses. | Could allow unauthorized control of the RTU, leading to manipulation of connected equipment or disruption of data flow. |
| Remote Terminal Unit (RTU) | Real-Time Operating System (RTOS) | Exploitation of RTOS Vulnerabilities | Vulnerabilities in the Real-Time Operating System running on the RTU could be exploited by attackers. | Could grant attackers complete control over the RTU's functionality, potentially impacting critical grid operations. |
| Intelligent Electronic Device (IED) | Configuration File Storage | Tampering with Configuration Files | Attackers could attempt to modify the configuration files of IEDs. | Could lead to incorrect operation of protection functions, potentially causing false trips or failures to operate during faults, impacting grid stability and safety. |
| Intelligent Electronic Device (IED) | Network Services (e.g., Telnet, SNMP) | Exploitation of Insecure Network Services | If IEDs expose insecure network services, attackers could exploit vulnerabilities in these services. | Could provide attackers with unauthorized access to the device for configuration changes or other malicious activities. |

This mapping highlights the specific threats that Endeavor Energy's embedded systems might face based on their inherent properties. It underscores the importance of implementing security measures tailored to the unique characteristics and vulnerabilities of these devices to ensure the overall security and reliability of the electricity distribution network.

**8. Open-Source Intelligence Analysis: Threats and Vulnerabilities Targeting Endeavor Energy and the Australian Energy Sector**

The open-source intelligence (OSINT) analysis conducted for this report has yielded several key findings relevant to the cybersecurity risks facing Endeavor Energy and the broader Australian energy sector.

Known threat actors targeting the Australian energy sector include both state-sponsored groups and cybercriminal organizations. ACSC reports indicate persistent targeting of Australian critical infrastructure by state actors for espionage and potential disruptive purposes 6. Cybercriminal groups are also actively targeting the sector, primarily for financial gain through ransomware attacks and data theft 6. While specific APT groups targeting Endeavor Energy have not been publicly identified, the general trend of nation-state interest in critical infrastructure suggests this remains a potential threat.

OSINT did not reveal any specific, publicly disclosed vulnerabilities directly linked to Endeavor Energy's proprietary technology stack. However, analysis of common OT/ICS vulnerabilities indicates prevalent issues such as weak authentication, the use of unpatched software, and insecure remote access protocols 42. These vulnerabilities are common across the energy sector and could potentially be present in Endeavor Energy's environment if not adequately addressed through robust security practices.

Case studies of cyberattacks on Australian energy companies provide valuable insights into the tactics, techniques, and procedures (TTPs) used by threat actors. The 2021 ransomware attack on CS Energy 8 involved the Conti ransomware group targeting corporate networks and email systems. While the power generation systems were ultimately unaffected due to rapid isolation, this incident highlights the potential for significant disruption. In 2022, Energy Australia and AGL were also reported to have been targets of cyberattacks 7, further underscoring the ongoing threat to the sector. These incidents, along with global examples like the Colonial Pipeline attack 51, often involve phishing for initial access, followed by lateral movement within the network and the eventual deployment of ransomware or other malicious payloads.

Australian government sources, particularly the ACSC and AEMO, provide crucial advisories and recommendations for the energy sector. ACSC annual cyber threat reports consistently highlight critical infrastructure, including the energy sector, as a prime target and emphasize the importance of implementing foundational security controls like the Essential Eight 6. AEMO is taking an increasingly active role in enhancing the cyber security posture of the energy sector, including coordinating incident response plans and providing expert advice 54. They also developed the AESCSF to provide a sector-specific framework for managing cyber security risks 37.

Analysis of Endeavor Energy's public footprint, including its website 3 and procurement portal 20, reveals general information about its operations, service area, and technology initiatives, such as the Advanced Metering Infrastructure (AMI) program 4. While no specific sensitive information that could be directly exploited by attackers was readily apparent, publicly available job postings or procurement documents could potentially provide insights into the types of technologies and systems in use, which could be leveraged by more sophisticated threat actors during reconnaissance. The security posture of Endeavor Energy's public-facing digital assets appears to be generally sound, but a more in-depth technical assessment would be required to provide a definitive evaluation.

The information gathered through OSINT analysis aligns with and reinforces the threats identified through the MITRE ATT&CK for ICS and EMB3D framework mappings. The prevalence of ransomware attacks in the Australian energy sector, as highlighted by OSINT, directly correlates with the "Impact" tactic in MITRE ATT&CK for ICS. Similarly, the identified TTPs, such as phishing and exploitation of public-facing applications, map to the "Initial Access" tactic. The focus on embedded device security in the EMB3D model is particularly relevant given the widespread deployment of smart meters and other field devices within Endeavor Energy's infrastructure, as revealed through OSINT.

The following table summarizes the key findings from the OSINT analysis:

| **Source** | **Date** | **Key Finding/Threat** | **Relevance to Endeavor Energy** |
| --- | --- | --- | --- |
| ACSC Annual Cyber Threat Report 2023-2024 13 | Nov 2024 | Critical infrastructure, including energy, is a prime target; compromised accounts, malware, and compromised assets are common incident types; phishing and exploitation of public-facing applications are common attack vectors. | Highlights the general threat landscape for Endeavor Energy, indicating likely attack methods and incident types to prepare for. |
| ACSC Annual Cyber Threat Report 2022 42 | Mar 2023 | Increased sophistication of cyber threats; critical infrastructure is an attractive target for both state actors and cybercriminals; inadequate patching is a major cause of incidents. | Emphasizes the need for robust patching practices and awareness of sophisticated threats targeting critical infrastructure. |
| AEMO Cyber Security Roles and Responsibilities 55 | Dec 2024 | AEMO's role in coordinating cyber incident response and supporting industry preparedness is formalized. | Indicates a growing focus on sector-wide cyber security coordination that Endeavor Energy should be aware of and participate in. |
| CS Energy Ransomware Attack 8 | 2021 | Ransomware attack on a Queensland energy generator disrupted corporate networks. | Provides a specific example of a successful cyberattack on an Australian energy company, highlighting the potential impact and the importance of incident response. |
| Energy Australia & AGL Cyber Attacks 7 | 2022 | Publicly reported cyberattacks on major Australian energy retailers. | Shows that even large energy companies in Australia are targets, indicating the broad nature of the threat. |
| SecurityScorecard Report on Energy Sector Breaches 11 | 2024 | 67% of energy sector breaches linked to software and IT vendors, highlighting supply chain risks. | Underscores the importance of managing risks associated with third-party vendors and the software they provide to Endeavor Energy. |

This OSINT analysis provides valuable context and specific examples of the threats and vulnerabilities that Endeavor Energy needs to consider in its cybersecurity strategy.

**9. Risk Assessment and Prioritization of Identified Threats**

To effectively allocate resources and focus mitigation efforts, a risk assessment and prioritization of the identified cybersecurity threats is essential. The methodology used for this assessment considers both the likelihood of a threat materializing and the potential impact it could have on Endeavor Energy's operations. Likelihood is assessed based on factors such as the capability of the threat actor, the prevalence of the threat within the Australian energy sector, and the presence of known vulnerabilities that could be exploited. Potential impact is evaluated across several dimensions, including safety of the public and staff, financial implications, operational disruptions, and regulatory compliance.

Based on this methodology, the identified threats can be prioritized to focus on those posing the highest risk to Endeavor Energy. The following table presents a prioritized list of key threats:

| **Threat** | **Likelihood** | **Potential Impact** | **Overall Risk Level** | **Relevant Framework(s)** | **Relevant OSINT Findings** |
| --- | --- | --- | --- | --- | --- |
| Ransomware Attack on OT/IT Systems | High | High | Critical | MITRE ATT&CK for ICS (Impact), EMB3D | CS Energy Ransomware Attack 8, ACSC Threat Reports 13 |
| Loss of Visibility/Control of SCADA/DMS | Medium | High | High | MITRE ATT&CK for ICS (Impact) | ACSC Threat Reports 13 |
| Exploitation of Vulnerabilities in Public-Facing Applications | Medium | Medium | High | MITRE ATT&CK for ICS (Initial Access) | ACSC Threat Reports 13 |
| Supply Chain Attack Introducing Malware or Backdoors | Medium | High | High | MITRE ATT&CK for ICS (Initial Access, Persistence), EMB3D | SecurityScorecard Report 11 |
| Unauthorized Access to Embedded Devices (Smart Meters, RTUs, IEDs) | Medium | Medium | High | EMB3D |  |
| Data Breach of Customer or Operational Data | Medium | Medium | Medium |  | Energy Australia & AGL Cyber Attacks 7 |
| Denial of Service Attack on Critical Systems | Low | High | Medium | MITRE ATT&CK for ICS (Impact) | ACSC Threat Reports 6 |
| Malicious Insider Activity Leading to System Compromise | Low | High | Medium | MITRE ATT&CK for ICS (Initial Access, Execution) |  |

This prioritization highlights the most critical threats that Endeavor Energy should focus on mitigating to protect its operations and ensure the reliable supply of electricity to its customers. The following section will provide actionable mitigation strategies aligned with Australian standards and frameworks to address these prioritized risks.

**10. Actionable Mitigation Strategies and Recommendations Aligned with Australian Standards**

Based on the prioritized threats identified in the previous section, this part of the report provides specific and actionable mitigation strategies for Endeavor Energy. These recommendations are aligned with the requirements of the Security of Critical Infrastructure Act 2018 (SOCI Act), the Australian Energy Sector Cyber Security Framework (AESCSF), and the Australian Cyber Security Centre (ACSC) Essential Eight strategies.

To meet the obligations of the SOCI Act 23, Endeavor Energy should ensure it has a comprehensive Critical Infrastructure Risk Management Program (CIRMP) in place. This program should address the prioritized threats identified in this report, outlining processes and systems to identify hazards, minimize risks, and ensure the security and resilience of its critical infrastructure assets. Regular reviews and updates of the CIRMP are essential, as are the development and testing of incident response plans specifically tailored to cyber incidents affecting OT environments. Compliance with mandatory cyber incident reporting requirements to the ACSC is also crucial.

Alignment with the AESCSF 37 can be achieved by addressing the framework's key domains in the context of the prioritized threats. For example, to mitigate the risk of ransomware and loss of control, Endeavor Energy should focus on the Risk Management domain by establishing and maintaining a robust cybersecurity risk management program informed by threat intelligence. The Asset Management domain is relevant to securing embedded devices, requiring comprehensive asset inventory and management practices. Strengthening Identity and Access Management with multi-factor authentication and the principle of least privilege, as recommended below, aligns with the corresponding AESCSF domain. Proactive Threat and Vulnerability Management, including regular patching and vulnerability assessments, is crucial for reducing the likelihood of exploitation. Finally, a well-defined and tested Incident Response plan, tailored to OT environments, is essential for effective management of cyber incidents.

Implementing the ACSC Essential Eight mitigation strategies 15 will provide a foundational level of cybersecurity across both IT and OT environments. Endeavor Energy should aim for an appropriate maturity level based on its risk profile and the sensitivity of its systems. Key recommendations aligned with the Essential Eight include:

* **Application Control:** Implement application whitelisting to ensure only approved applications can execute on critical systems, helping to prevent the execution of malicious software, including ransomware 15.
* **Patch Applications:** Establish a rigorous process for patching applications, especially those with known vulnerabilities, in a timely manner 15.
* **Configure Microsoft Office Macro Settings:** Disable or restrict the use of macros in Microsoft Office documents, a common vector for malware delivery 15.
* **User Application Hardening:** Harden web browsers and other user applications to reduce their attack surface 15.
* **Restrict Administrative Privileges:** Limit the number of users with administrative privileges and ensure these privileges are only used when necessary 15.
* **Patch Operating Systems:** Implement a robust process for patching operating systems across both IT and OT environments, addressing known vulnerabilities that could be exploited by attackers 15. Given the criticality of OT systems, patching should be carefully planned and tested in non-production environments before deployment 18.
* **Multi-Factor Authentication (MFA):** Implement MFA for all users, especially those with access to critical systems, including OT environments and embedded devices. Phishing-resistant MFA should be prioritized where possible 15.
* **Regular Backups:** Establish a comprehensive backup strategy for critical data and systems in both IT and OT environments, ensuring regular backups are taken and tested for restorability 15. Backups should be stored offline and in a separate location to protect against ransomware attacks.

In addition to these Essential Eight strategies, the following specific technical and procedural recommendations are provided:

* **Network Segmentation:** Implement robust network segmentation to isolate IT and OT networks, as well as segmenting the OT network into logical zones based on criticality and function 13. This will limit the potential for lateral movement by attackers if one segment is compromised.
* **Enhanced Vulnerability Management:** Implement a comprehensive vulnerability management program that includes regular vulnerability scanning and penetration testing of both IT and OT environments 14. This program should prioritize the remediation of identified vulnerabilities based on their severity and potential impact.
* **Secure Remote Access:** Implement secure remote access solutions with strong authentication and encryption protocols for any remote connections to OT systems 13. Access should be granted on a need-to-know basis and closely monitored.
* **Embedded Device Security:** Enhance the security of embedded devices by implementing measures such as firmware integrity checks, secure boot processes, and secure communication protocols. Consider network segmentation to isolate these devices where possible.
* **Incident Response Plan for OT:** Develop and regularly test a comprehensive incident response plan specifically tailored to address cyber incidents in the OT environment 14. This plan should include clear roles and responsibilities, communication protocols, and procedures for containment, eradication, and recovery. Collaboration with external cybersecurity experts and participation in industry exercises can enhance preparedness.
* **Supply Chain Risk Management:** Implement a robust supply chain risk management program to assess and mitigate cybersecurity risks associated with third-party vendors and the software and hardware they provide 11. This should include due diligence during vendor selection and ongoing monitoring of vendor security practices.
* **Security Awareness Training:** Conduct regular cybersecurity awareness training for all employees and contractors, emphasizing threats relevant to the energy sector, such as phishing attacks targeting OT personnel 14. Training should also cover safe browsing habits, password security, and the importance of reporting suspicious activity.
* **Enhanced Logging and Monitoring:** Implement robust logging and monitoring capabilities for both IT and OT systems to detect and respond to suspicious activity in a timely manner 13. Security Information and Event Management (SIEM) systems can be used to aggregate and analyze logs from various sources.

The following table summarizes the key mitigation strategies and their alignment with Australian standards and frameworks:

| **Prioritized Threat** | **Recommended Mitigation Strategy** | **Alignment with SOCI Act** | **Alignment with AESCSF Domain(s)** | **Alignment with Essential Eight Strategy(s)** |
| --- | --- | --- | --- | --- |
| Ransomware Attack on OT/IT Systems | Implement Application Control, Patch Applications, Regular Backups, Network Segmentation, Enhanced Logging and Monitoring | CIRMP, Incident Response | Risk Management, Asset Management, Threat and Vulnerability Management, Event and Incident Response | Application Control, Patch Applications, Regular Backups |
| Loss of Visibility/Control of SCADA/DMS | Network Segmentation, Restrict Administrative Privileges, Enhanced Logging and Monitoring, Incident Response Plan for OT | CIRMP, Incident Response | Risk Management, Asset Management, Identity and Access Management, Situational Awareness, Event and Incident Response | Restrict Administrative Privileges |
| Exploitation of Vulnerabilities in Public-Facing Applications | Patch Applications, User Application Hardening, Implement Web Application Firewall, Multi-Factor Authentication | CIRMP | Risk Management, Threat and Vulnerability Management | Patch Applications, User Application Hardening, Multi-Factor Authentication |
| Supply Chain Attack Introducing Malware or Backdoors | Implement Application Control, Supply Chain Risk Management Program, Enhanced Logging and Monitoring | CIRMP | Risk Management, Supply Chain and External Dependencies Management | Application Control |
| Unauthorized Access to Embedded Devices (Smart Meters, RTUs, IEDs) | Implement Multi-Factor Authentication, Network Segmentation, Secure Remote Access, Firmware Integrity Checks | CIRMP, Asset Management | Asset Management, Identity and Access Management, Cyber Security Architecture | Multi-Factor Authentication |
| Data Breach of Customer or Operational Data | Restrict Administrative Privileges, Multi-Factor Authentication, Enhanced Logging and Monitoring, Data Loss Prevention Measures | CIRMP | Risk Management, Identity and Access Management, Australian Privacy Management | Restrict Administrative Privileges, Multi-Factor Authentication |
| Denial of Service Attack on Critical Systems | Network Segmentation, Implement Intrusion Prevention Systems, Enhanced Monitoring | CIRMP | Risk Management, Cyber Security Architecture |  |
| Malicious Insider Activity Leading to System Compromise | Restrict Administrative Privileges, Multi-Factor Authentication, Enhanced Logging and Monitoring, Security Awareness Training | CIRMP, Personnel Security | Risk Management, Identity and Access Management, Workforce Management | Restrict Administrative Privileges, Multi-Factor Authentication |

By implementing these mitigation strategies, Endeavor Energy can significantly enhance its cybersecurity posture and reduce the risk of successful cyberattacks on its critical infrastructure.

**11. Conclusion**

In conclusion, this cybersecurity threat model report highlights the significant and evolving cyber threats facing Endeavor Energy as a major electricity distribution network operator in Australia. The analysis, utilizing the MITRE ATT&CK framework for ICS, the EMB3D Threat Model, and open-source intelligence, reveals a complex threat landscape characterized by sophisticated state-sponsored actors and opportunistic cybercriminals targeting critical infrastructure for various motives, including financial gain and potential disruption. The increasing digitization of the energy sector, while offering numerous operational benefits, also expands the attack surface and introduces new vulnerabilities that must be proactively addressed.

The key findings of this report underscore the importance of a proactive and adaptive cybersecurity approach for Endeavor Energy. Ransomware attacks, the potential loss of visibility and control over critical systems, the exploitation of vulnerabilities in public-facing applications, and supply chain risks represent significant threats that require immediate attention. The analysis of Endeavor Energy's likely system architecture and the application of the MITRE ATT&CK for ICS and EMB3D frameworks provide a detailed understanding of potential attack vectors and the specific threats targeting both OT systems and embedded devices. The OSINT analysis further contextualizes these threats within the Australian energy sector, highlighting relevant case studies and the guidance provided by Australian government agencies like the ACSC and AEMO.

To effectively mitigate these risks, the report recommends a series of actionable mitigation strategies aligned with Australian standards and frameworks, including the SOCI Act, AESCSF, and the Essential Eight. These recommendations emphasize the need for robust network segmentation, strengthened identity and access management, enhanced vulnerability management and patching processes, comprehensive incident response planning, and a strong focus on securing embedded devices and managing supply chain risks. Implementing these measures will not only help Endeavor Energy meet its regulatory obligations but also significantly enhance its overall cybersecurity posture, improving the reliability and safety of its operations.

The cybersecurity landscape is constantly evolving, and it is therefore crucial for Endeavor Energy to adopt an ongoing and adaptive approach to its cybersecurity program. This includes continuous monitoring of the threat landscape, regular security assessments and penetration testing, and a commitment to adapting security measures in response to emerging threats and vulnerabilities. By proactively implementing the recommendations outlined in this report and maintaining a strong security culture, Endeavor Energy can significantly enhance its resilience against cyber threats, ensuring the continued reliable and safe delivery of electricity to the communities it serves and protecting critical infrastructure for the benefit of all Australians.

#### Works cited

1. Endeavour Energy, accessed March 26, 2025, <https://www.aer.gov.au/system/files/Endeavour%20Energy%20-%20RIN0.05%20Basis%20of%20Preparation%20-%2030%20April%202018%20-%20Public.pdf>
2. Advanced Distribution Management System ADMS - ETAP, accessed March 26, 2025, <https://etap.com/solutions/advanced-distribution-management-system>
3. Endeavour Energy, accessed March 26, 2025, <https://www.endeavourenergy.com.au/>
4. Advanced Metering Infrastructure | Endeavour Energy, accessed March 26, 2025, <https://www.endeavourenergy.com.au/modern-grid/projects-and-trials/advanced-metering-infrastructure>
5. Network Investments | Endeavour Energy, accessed March 26, 2025, <https://www.endeavourenergy.com.au/modern-grid/creating-the-modern-grid/network-planning/distribution-annual-planning-report/dapr/network-investments>
6. Australia's Cyber Defense report highlights evolving threats and strategic countermeasures, accessed March 26, 2025, <https://industrialcyber.co/reports/australias-cyber-defense-report-highlights-evolving-threats-and-strategic-countermeasures/>
7. Is Australia's energy sector at risk? - eftsure, accessed March 26, 2025, <https://eftsure.com/en-au/blog/cyber-crime/is-australias-energy-sector-at-risk/>
8. Safeguarding critical infrastructure | Community support ..., accessed March 26, 2025, <https://www.qld.gov.au/community/your-home-community/cyber-security/cyber-security-for-queenslanders/case-studies/safeguarding-critical-infrastructure>
9. ASD Cyber Threat Report 2022-2023 | Cyber.gov.au, accessed March 26, 2025, <https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023>
10. Modern grid | Endeavour Energy, accessed March 26, 2025, <https://www.endeavourenergy.com.au/modern-grid>
11. 67% of Energy Sector Breaches Linked to Software and IT Vendors, SecurityScorecard Reports, accessed March 26, 2025, <https://securityscorecard.com/company/press/67-of-energy-sector-breaches-linked-to-software-and-it-vendors-securityscorecard-reports/>
12. Cyber Security and IT Leadership: A Growing Threat to Australia's Renewable Energy Efforts - TechRepublic, accessed March 26, 2025, <https://www.techrepublic.com/article/cyber-security-renewable-energy-australia/>
13. Annual Cyber Threat Report 2023-2024 | Cyber.gov.au, accessed March 26, 2025, <https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024>
14. Stop OT Disruptions: 5 Ways to Improve Your Operational Technology Security - CyberProof, accessed March 26, 2025, <https://www.cyberproof.com/blog/stop-ot-disruptions-5-ways-to-improve-your-operational-technology-security/>
15. Essential Eight Explained - Australian Cyber Security Centre, accessed March 26, 2025, <https://www.cyber.gov.au/sites/default/files/2023-11/PROTECT%20-%20Essential%20Eight%20Explained%20%28November%202023%29.pdf>
16. The ACSC's Essential Eight & Privileged Access Management (PAM) - BeyondTrust, accessed March 26, 2025, <https://www.beyondtrust.com/solutions/compliance/essential-8>
17. Best Practices for OT Firewall Management | Rockwell Automation | UK, accessed March 26, 2025, <https://www.rockwellautomation.com/en-gb/company/news/blogs/ot-firewall-management.html>
18. The Importance of Testing & Validating Software Updates in OT, Including Security Patches, accessed March 26, 2025, <https://www.industrialdefender.com/blog/ot-considerations-for-the-global-crowdstrike-microsoft-outage>
19. Endeavour Energy - Wikipedia, accessed March 26, 2025, <https://en.wikipedia.org/wiki/Endeavour_Energy>
20. Welcome to Endeavour Energy E-Tendering, accessed March 26, 2025, <https://www.tenderlink.com/endeavourenergy>
21. About us | Endeavour Energy, accessed March 26, 2025, <https://www.endeavourenergy.com.au/about>
22. Endeavour Energy | Australian Energy Regulator (AER), accessed March 26, 2025, <https://www.aer.gov.au/industry/networks/entities/service-providers/endeavour-energy>
23. SOCI Act Explained: Compliance Rules & Requirements | UpGuard, accessed March 26, 2025, <https://www.upguard.com/blog/soci-act-2018>
24. Australia's latest Security of Critical Infrastructure Act amendments ..., accessed March 26, 2025, <https://www.pinsentmasons.com/out-law/analysis/security-critical-infrastructure-act-amendments-explained>
25. SOCI Act | Critical infrastructure assets protection - KPMG Australia, accessed March 26, 2025, <https://kpmg.com/au/en/home/topics/critical-infrastructure-reforms.html>
26. Australia's cyber threats: ACSC report insights 2023-2024 - BDO Australia, accessed March 26, 2025, <https://www.bdo.com.au/en-au/insights/cyber-security/australia-s-cyber-threats-key-insights-from-the-acsc-report-2023-2024>
27. MITRE ATT&CK ICS: Tactics, Techniques, and Best Practices ..., accessed March 26, 2025, <https://www.exabeam.com/explainers/mitre-attck/mitre-attck-ics-tactics-techniques-and-best-practices/>
28. MITRE ATT&CK for ICS Detections in the Dragos Platform, accessed March 26, 2025, <https://www.dragos.com/mitre-attack-for-ics/>
29. Glossar | Mitre Att&ck ICS? - Rhebo, accessed March 26, 2025, <https://rhebo.com/en/ressourcen/glossar/mitre-att-ck-ics-25258/>
30. MITRE ATT&CK for Industrial Control Systems in IriusRisk, accessed March 26, 2025, <https://www.iriusrisk.com/resources-blog/mitre-attck-for-industrial-control-systems-in-iriusrisk>
31. Defend your ICS systems with the MITRE ATT&CK framework - Armis, accessed March 26, 2025, <https://www.armis.com/solutions/mitre-attck-for-ics/>
32. MITRE EMB3D™, accessed March 26, 2025, <https://emb3d.mitre.org/>
33. Elevating Embedded Device Security: The EMB3D™ Threat ..., accessed March 26, 2025, <https://www.iriusrisk.com/resources-blog/elevating-embedded-device-security-mitre-emb3d>
34. MITRE releases enhanced EMB3D Threat Model with new mitigations, ISA/IEC 62443-4-2 alignment - Industrial Cyber, accessed March 26, 2025, <https://industrialcyber.co/control-device-security/mitre-releases-enhanced-emb3d-threat-model-with-new-mitigations-isa-iec-62443-4-2-alignment/>
35. What is the MITRE EMB3D Framework and Why It Matters - Asimily, accessed March 26, 2025, <https://asimily.com/blog/what-is-the-mitre-emb3d-framework/>
36. MITRE Releases EMB3D™ – A Cybersecurity Threat Model for Embedded Devices, accessed March 26, 2025, <https://www.businesswire.com/news/home/20240513302654/en/MITRE-Releases-EMB3D-A-Cybersecurity-Threat-Model-for-Embedded-Devices>
37. AESCSF framework and resources - AEMO, accessed March 26, 2025, <https://aemo.com.au/initiatives/major-programs/cyber-security/aescsf-framework-and-resources>
38. Strengthening OT Security: Aligning with the Australian Energy ..., accessed March 26, 2025, <https://www.dragos.com/blog/strengthening-ot-security-aligning-with-the-australian-energy-sector-cyber-security-framework-aescsf/>
39. ACSC Essential Eight - Learn Microsoft, accessed March 26, 2025, <https://learn.microsoft.com/en-us/compliance/anz/e8-overview>
40. Australian Energy Sector Cyber Security Framework - AEMO, accessed March 26, 2025, <https://aemo.com.au/initiatives/major-programs/cyber-security>
41. Power system operating incident reports - AEMO, accessed March 26, 2025, <https://aemo.com.au/energy-systems/electricity/national-electricity-market-nem/nem-events-and-reports/power-system-operating-incident-reports>
42. Annual Cyber Threat Report, accessed March 26, 2025, <https://www.cyber.gov.au/sites/default/files/2023-03/ACSC-Annual-Cyber-Threat-Report-2022_0.pdf>
43. ACSC's First Annual Cyber Threat Report Records 59,806 Cybercrimes in One Year, accessed March 26, 2025, <https://cisomag.com/acsc-first-annual-cyber-threat-report/amp/>
44. ACSC Annual Cyber Threat Report, accessed March 26, 2025, <https://www.cyber.gov.au/sites/default/files/2023-03/ACSC%20Annual%20Cyber%20Threat%20Report%20-%202020-2021.pdf>
45. The Impact of Cyber Attacks on the Utilities Sector in Australia - SAP News Center, accessed March 26, 2025, <https://news.sap.com/australia/2022/06/20/the-impact-of-cyber-attacks-on-the-utilities-sector-in-australia/>
46. Aussie Energy Giant Fears Losing Billions to Cyberattacks - BankInfoSecurity, accessed March 26, 2025, <https://www.bankinfosecurity.asia/aussie-energy-giant-fears-losing-billions-to-cyberattacks-a-25308>
47. Australian Energy Software Firm Energy One Hit by Cyberattack - SecurityWeek, accessed March 26, 2025, <https://www.securityweek.com/australian-energy-software-firm-energy-one-hit-by-cyberattack/>
48. Energy sector most targeted for cyber attacks, accessed March 26, 2025, <https://esdnews.com.au/energy-sector-targeted-cyber-attacks/>
49. Australia's Endeavour Energy gains information security certification, accessed March 26, 2025, <https://www.smart-energy.com/industry-sectors/cybersecurity/australias-endeavour-energy-gains-information-security-certification/>
50. Ransomware Attacks against the Energy Sector on the rise - Nuclear and Oil & Gas are Major Targets in 2024 - Resecurity, accessed March 26, 2025, <https://www.resecurity.com/blog/article/ransomware-attacks-against-the-energy-sector-on-the-rise-nuclear-and-oil-gas-are-major-targets-2024>
51. Unraveling Iconic Data Breaches in the Energy Industry - ProcessUnity, accessed March 26, 2025, <https://www.processunity.com/iconic-data-breaches-in-energy-industry/>
52. Cyberattacks on Energy Infrastructure | GE Vernova, accessed March 26, 2025, <https://www.gevernova.com/gas-power/resources/articles/2021/energy-cyber-attack>
53. OT/ICS Security for Oil & Gas: A Comprehensive Guide - Sectrio, accessed March 26, 2025, <https://sectrio.com/blog/complete-guide-ot-ics-cybersecurity-oil-and-gas/>
54. Final rule to help mitigate cyber threats on the electricity system ..., accessed March 26, 2025, <https://www.aemc.gov.au/news-centre/media-releases/final-rule-help-mitigate-cyber-threats-electricity-system>
55. Cyber security roles and responsibilities | AEMC, accessed March 26, 2025, <https://www.aemc.gov.au/rule-changes/cyber-security-roles-and-responsibilities>
56. Australia's Essential Eight and the UK's Cyber Essentials – An Overview - CYRISMA, accessed March 26, 2025, <https://cyrisma.com/essential-eight-cyber-essentials/>
57. Essential Eight: A Guide to the ACSC's Cybersecurity Framework - Datto, accessed March 26, 2025, <https://www.datto.com/blog/essential-eight/>
58. Reaching Essential Eight maturity on AWS: Security and compliance for Australian organizations - AWS Prescriptive Guidance - AWS Documentation, accessed March 26, 2025, <https://docs.aws.amazon.com/prescriptive-guidance/latest/essential-eight-maturity/introduction.html>
59. ACSC - Essential 8 Maturity Model | Atlassian, accessed March 26, 2025, <https://www.atlassian.com/trust/compliance/resources/essential8>
60. Essential Eight Maturity Model - Australian Cyber Security Centre, accessed March 26, 2025, <https://www.cyber.gov.au/sites/default/files/2023-11/PROTECT%20-%20Essential%20Eight%20Maturity%20Model%20%28November%202023%29.pdf>