# **Executive Summary: Quantifying and Managing Cyber Risk in Australian Energy M&A**

A venture capital firm's potential acquisition of energy distribution assets in Australia, including power lines and smart meters, requires a proactive and in-depth cybersecurity due diligence process. The traditional M&A focus on financial and operational metrics is no longer sufficient; cybersecurity has emerged as a material line item that can significantly alter deal valuation, introduce substantial liabilities, and jeopardize the success of the transaction itself.1

The Australian energy sector is an attractive and increasingly vulnerable target for malicious actors, from profit-motivated cybercriminals to state-sponsored entities.3 The convergence of legacy Operational Technology (OT) and modern Information Technology (IT) networks has created a complex and expanded attack surface, exposing critical physical infrastructure to threats never considered in its original design.4 Furthermore, the Australian government is systematically strengthening the regulatory environment through the Security of Critical Infrastructure (SOCI) Act 2018, which imposes mandatory and non-negotiable security obligations on owners of critical assets.5

This report provides a comprehensive, multi-phased roadmap for the venture capital firm. It outlines a diagnostic methodology that extends beyond a passive review of documents to include practical readiness exercises. It details the specific threats to SCADA systems and smart meters, explains the mandatory Australian regulatory landscape, and formalizes a model for quantifying cyber risk to inform deal valuation and negotiation. Finally, it presents a plan for post-acquisition integration, ensuring the acquired asset's value is protected and enhanced for long-term resilience.

### **I. The New Frontier of Energy M&A: Beyond the Balance Sheet**

#### **1.1. The Strategic Imperative for Cyber Due Diligence**

Mergers and acquisitions are among the most critical steps a company can take, but they present significant security threats in addition to opportunities for business growth.6 A target company, or even its supply chain, may harbor a host of hidden security risks, from undiscovered data breaches to regulatory compliance omissions.6 The failure to uncover these issues in a timely manner can result in costly fines, reputational damage, and even the disruption of the merger or acquisition itself.6

For this reason, cybersecurity due diligence has become an essential component of a successful M&A strategy. It provides comprehensive insight into the existing and potential risks associated with the target company, enabling better-informed decision-making and reducing the likelihood of expensive security issues in the future.6 The process highlights specific vulnerabilities and capability weaknesses that can inform the terms and conditions of an agreement, such as price adjustments or remediation requirements.6 Relying solely on the target organization's self-disclosed information is an insufficient and risky approach.6

The financial consequences of inadequate due diligence are well-documented. In one of the most widely cited examples, Verizon negotiated a $350 million reduction in its acquisition price for Yahoo after discovering two massive data breaches that had affected billions of accounts.1 This demonstrated that cyber risk is no longer a peripheral concern but a material line item in M&A valuation. Similarly, Marriott's acquisition of Starwood Hotels resulted in significant fines and reputational damage after a pre-existing breach compromised 383 million guest records.7 These cases underscore the risk of inheriting what are often called "dormant threats," which can lie undetected within an acquired company's infrastructure and become costly liabilities for the new owner.1

#### **1.2. Australia's Heightened Threat Landscape**

The Australian energy sector is a crucial component of the country's critical infrastructure and economy, making it a primary target for various cyber threats.3 According to the Australian Cyber Security Centre (ACSC), the energy sector broke into the top 10 most targeted industries in Australia in 2022, with reports indicating a substantial rise in attacks against utilities and energy companies.3 The threat landscape is complicated by state-sponsored actors operating alongside profit-motivated cybercriminals, with both groups targeting critical infrastructure for intelligence collection, service disruption, or financial gain.4 Data from the Australian Signals Directorate (ASD) shows that over 11% of all cyber incidents responded to in a single year affected critical infrastructure sectors, including energy.4

A significant factor contributing to this escalating risk is the blending of Operational Technology (OT) and Information Technology (IT) systems.4 Legacy OT systems, such as Supervisory Control and Data Acquisition (SCADA) systems used to manage physical assets like power lines and distribution, were not originally designed to withstand modern cyber threats.4 As these systems become increasingly interconnected with corporate IT networks and the internet to enable greater efficiency, they create new vulnerabilities and a much larger attack surface for malicious actors to exploit.3 This is a core risk for a venture capital firm acquiring physical energy infrastructure, as the security posture of the physical assets is inextricably linked to the security of the digital systems that control them.

Specific incidents in Australia highlight these tangible threats. In 2021, CS Energy Ltd, which generates a significant portion of electricity for the National Electricity Market, was hit by a ransomware attack that targeted its corporate network and email systems.10 While the company responded quickly to isolate the affected servers and prevent disruption to electricity supply, the incident demonstrated the sector's vulnerability to these types of attacks.10 In 2022, Australian energy provider AGL also reported a cyber incident on its "My Account" platform, where attackers used credentials acquired externally to log into customer accounts, underscoring the risks to customer data.3 These cases provide a concrete demonstration of the threats a new owner in the Australian energy sector is likely to face.

### **II. Pre-Acquisition: A Multi-Layered Approach to Diagnostic Activities**

#### **2.1. Foundational Due Diligence Activities: The Checklist Approach**

A comprehensive cybersecurity due diligence process begins with a foundational review of the target's policies, procedures, and existing controls.6 This initial, or "light-touch," evaluation provides a high-level overview and helps to identify obvious red flags.6 Key areas of inquiry for this phase include:

* **Risk Governance and Profile:** It is essential to review the target company's risk profile to determine when its last comprehensive information security risk assessment was conducted and the steps taken to mitigate the identified risks.13 A company that cannot effectively articulate its own risk profile or demonstrate a history of addressing vulnerabilities is a significant warning sign for a potential acquirer.14
* **Incident History and Readiness:** The review should investigate whether the target has experienced any past security breaches, how they were handled, and if the company is currently subject to any fines or government consent orders for security incidents.13 It is also critical to review their incident response, business continuity, and disaster recovery plans to understand their preparedness for a future event.6
* **Asset Management:** A complete asset inventory is fundamental. This includes identifying all physical and logical assets, such as computers, servers, legacy systems, data, and applications.13 This activity is crucial for understanding the full scope of what is being acquired and for identifying any obsolete, outdated, or unsupported systems that will require a remediation plan.13
* **Supply Chain and Third-Party Risk:** The target company's third-party risk exposure must be evaluated. This involves identifying critical vendors and assessing the security of their supply chain, as a vulnerability in a single third-party provider can grant an attacker lateral access to the entire combined entity.2
* **Compliance and Certifications:** The review should determine the target's readiness to comply with industry standards and regulations.6 Identifying existing security certifications or attestations, such as ISO 27001 or SOC 2, can demonstrate a proactive approach to risk management.6

While this checklist-based approach is a necessary starting point, it is insufficient on its own. It provides a static picture of a company's posture, and the knowledge gained is limited to the information that the target is willing and able to provide.6

#### **2.2. The Power of Practical Readiness Exercises**

To move beyond a passive document review and gain a true understanding of a target's cyber resilience, a multi-layered approach that includes practical, diagnostic exercises is necessary.17 These exercises objectively test the effectiveness of a company's people, processes, and technologies.

* Tabletop Exercises (TTX): The Strategic Test  
  A tabletop exercise is a discussion-based, simulated event where key stakeholders—from executive leadership and legal counsel to IT and communications teams—walk through an imagined cyberattack scenario.20 In an M&A context, a pre-acquisition TTX can simulate a ransomware attack that encrypts critical OT systems or a data breach that affects a large volume of customer billing data. The exercise reveals critical gaps in communication, decision-making authority, and the incident response plan that are not apparent from simply reviewing a static document.20 It provides a safe environment to identify where a plan might fail in practice, highlighting a lack of coordination between departments and clarifying who is authorized to make critical decisions during an incident.21
* Red Team Assessments: The Adversarial Test  
  A red team assessment is a goal-based, adversarial activity that simulates a real-world attacker's holistic approach to compromising an organization's most valuable assets.22 Unlike a traditional penetration test, a red team assessment has a broader scope and can combine multiple attack vectors, including technical exploitation, social engineering (e.g., phishing campaigns), and even physical access attempts.22 For a venture capital firm acquiring energy infrastructure, a red team assessment can be scoped to test whether an attacker could move from the corporate IT network to the OT network controlling the physical assets.25 It can uncover vulnerabilities that are missed by traditional assessments, such as unpatched legacy systems, weak passwords, and inadequate network segmentation that allow for lateral movement.26 The outcome is an objective, "battle-tested" measure of the target's defenses and a clear understanding of the real-world attack paths that could be used to cause significant damage.17

The value of combining these activities is that they work in a complementary fashion. While a due diligence checklist may reveal the existence of a documented incident response plan, a tabletop exercise would test whether the plan's components are known and understood by the people who need to execute them. A red team assessment would then test the underlying technical security of the systems the plan is meant to protect. This integrated approach prevents a false sense of security derived from static audits and provides a much clearer picture of the actual risks being acquired.

#### **2.3. Understanding Asset-Specific Threats and Vulnerabilities**

The acquisition of energy distribution assets, including power lines and smart meters, introduces distinct and specialized cybersecurity risks that must be understood in detail.

* **Operational Technology (OT) and SCADA Systems:** The acquired infrastructure will rely on OT, including Supervisory Control and Data Acquisition (SCADA) systems, to manage the flow of power.27 These systems were historically designed for isolated, dedicated networks.27 As they are increasingly connected to broader networks, they expose vulnerabilities such as inadequate authentication mechanisms, the use of proprietary protocols without encryption, and legacy software with unpatched flaws.26 The consequences of these vulnerabilities are severe and can include:
  + **Disconnecting Resources:** An attacker with full access to the network could send control commands to switches in substations, disconnecting power lines and causing immediate, widespread outages.28
  + **Injecting False Information:** An attacker could manipulate sensor readings sent to the control room, causing operators to take corrective actions for a non-existent problem that could lead to an overload and physical damage to infrastructure.28
  + **Denial-of-Service (DoS) Attacks:** An attacker could overload critical systems or their communication infrastructure, rendering them non-functional and disrupting crucial substation functions like protection and measurement.28
* **Smart Meters: The New Attack Surface:** The introduction of smart meters represents a major advancement in energy management, but each device also creates a new attack vector.31 These meters collect and transmit detailed information about energy use, making them an attractive target for cybercriminals.31 Key threats include data breaches, unauthorized access, denial-of-service attacks, and data manipulation.31 The vulnerabilities that enable these attacks often stem from weak authentication, outdated software, and undocumented communications.31 The lack of common standards can also hinder effective communication and security across a diverse network of devices and systems.31

### **III. The Australian Regulatory Framework: A Non-Negotiable Reality**

The Australian government has a clear and evolving regulatory framework for critical infrastructure security. A venture capital firm must recognize that upon acquisition, it is not merely acquiring an asset but also assuming a set of mandatory legal and operational obligations.5 This regulatory environment must be a core focus of due diligence, as non-compliance can result in significant legal and financial penalties.5

#### **3.1. The Security of Critical Infrastructure (SOCI) Act 2018**

The Security of Critical Infrastructure Act 2018 (SOCI Act) is the primary legislative framework designed to protect Australia's critical infrastructure assets and services from disruption.5 Successive amendments to the Act have expanded its scope and introduced new requirements, and grace periods for compliance have ended.5 The SOCI Act imposes mandatory

**Positive Security Obligations (PSOs)** on responsible entities in key sectors, including energy.5 These PSOs include:

* **Register of Critical Infrastructure Assets:** Responsible entities must provide ownership and operational information about their critical assets to the government.5
* **Mandatory Cyber Incident Reporting:** Entities must report cyber incidents to the Australian Cyber Security Centre (ACSC) via phone and a written report.5
* **Critical Infrastructure Risk Management Program (CIRMP):** Entities must implement a written program that outlines how they will identify, minimize, and mitigate hazards to their assets.5 The program must take an "all hazards" approach, considering risks across four vectors: physical security and natural hazards, personnel hazards, supply chain hazards, and cyber security.5

#### **3.2. Enhanced Cyber Security Obligations (ECSO) for Systems of National Significance (SoNS)**

A subset of critical infrastructure assets may be designated as a System of National Significance (SoNS) if their disruption would have severe, cascading consequences for Australia's social or economic stability.34 If the acquired assets are declared a SoNS, the firm would be subject to a set of more stringent

**Enhanced Cyber Security Obligations (ECSOs)** in addition to the PSOs.5 These obligations include:

* **Incident Response Plans:** Responsible entities must develop, maintain, and regularly review a plan to respond to cyber incidents.34
* **Cyber Security Exercises:** The government may require the entity to undertake cyber security exercises to test their incident response capabilities.18 These exercises, which can include discussion-based tabletop exercises or full operational simulations, are designed to reveal whether existing resources and processes are sufficient to safeguard the system from an attack.18
* **Vulnerability Assessments:** Mandatory vulnerability assessments must be performed to identify weaknesses in the system that need to be remediated.34
* **Provision of System Information:** Entities may be required to provide system information to the government to contribute to a near-real-time threat picture.34

#### **3.3. Leveraging the Australian Energy Sector Cybersecurity Framework (AESCSF)**

The Australian Energy Sector Cybersecurity Framework (AESCSF) is a set of guidelines developed by the Australian Energy Market Operator (AEMO), industry, and the government to help energy participants assess and improve their cyber maturity.37 While it is a voluntary framework, the AESCSF is closely aligned with other industry standards like the NIST Cybersecurity Framework and is recognized under the SOCI Act as a valid framework for meeting the CIRMP obligations.5 A target company's existing self-assessment against the AESCSF can therefore demonstrate a mature and compliant security posture, making it a more attractive acquisition target.27

The Australian government is actively reinforcing this regulatory landscape. Recent actions, such as the AEMC clarifying AEMO's cybersecurity role in the National Electricity Rules, demonstrate a clear and deliberate trend towards increasing government oversight and a systematic effort to enhance the security of the energy sector.39 This context highlights that a target company's readiness to meet these existing and future obligations is a key determinant of its long-term value and operational stability.

#### **Table 2: Summary of Australian Critical Infrastructure Obligations**

| Obligation | Requirement | Legal Basis | Implication for Business |
| --- | --- | --- | --- |
| **Positive Security Obligations (PSOs)** |  |  |  |
| Register of Assets | Register critical infrastructure assets and provide ownership/operational information. | SOCI Act 2018 | Mandatory, non-compliance can result in legal proceedings, significant penalties, and reputational damage.5 |
| Mandatory Cyber Incident Reporting | Report significant cyber incidents to the ACSC. | SOCI Act 2018 | Mandatory, non-compliance can result in legal proceedings, significant penalties, and reputational damage.5 |
| Risk Management Program (CIRMP) | Implement a program to identify, minimize, and mitigate all-hazards risks. | SOCI Act 2018 | Mandatory, non-compliance can result in legal proceedings, significant penalties, and reputational damage.5 |
| **Enhanced Cyber Security Obligations (ECSOs)** |  |  |  |
| Incident Response Plan | Develop, maintain, and review a plan to respond to cyber incidents. | SOCI Act 2018 (for SoNS) | May be mandated by the Minister for Home Affairs for Systems of National Significance.34 |
| Cyber Security Exercises | Undertake exercises to test response capabilities. | SOCI Act 2018 (for SoNS) | May be mandated by the Minister for Home Affairs, often on an annual basis.18 |
| Vulnerability Assessments | Perform assessments to identify system weaknesses. | SOCI Act 2018 (for SoNS) | May be mandated by the Minister for Home Affairs for Systems of National Significance.34 |

### **IV. Cyber Risk and Its Impact on Valuation and Deal Terms**

#### **4.1. From Footnote to Material Line Item**

Cyber risk is no longer a post-deal footnote but a material line item that directly affects M&A valuation.2 The value of an acquisition can decline significantly if undisclosed or unknown cybersecurity issues are discovered during due diligence.1 The cases of Verizon/Yahoo and Marriott/Starwood demonstrate that these issues can lead to substantial price adjustments and even jeopardize the transaction itself.1 Conversely, a company with a strong cybersecurity posture and a clean bill of health is a more attractive target, which can lead to a smoother and more secure transition while potentially achieving a maximum valuation during the sale process.1

#### **4.2. Quantifying the Cost of Remediation and Liabilities**

A key objective of cyber due diligence is to translate identified risks into a clear, costed roadmap of remediation items that can be financially quantified and used in valuation models.2 This process involves assessing the potential costs and liabilities associated with the target's security posture.

* **Direct Costs:** These are the immediate and quantifiable costs associated with addressing vulnerabilities. They include the costs of new tools, engaging external consultants, and retraining staff.42 According to a recent survey, the median recovery costs for the energy sector from a ransomware attack have quadrupled in a single year to $3 million, a figure four times higher than the global cross-sector median.44 This makes the financial liability of a poor security posture more significant than ever. The report also notes that 49% of ransomware attacks in the energy sector began with an exploited vulnerability, which can be identified during due diligence, and that a high rate of backup compromise (79%) and successful encryption (80%) was reported, leading to increasingly longer recovery times.44
* **Indirect Costs and Liabilities:** These costs, while harder to quantify, have a profound impact on value. They include fines for non-compliance with regulations like the SOCI Act, legal fees from potential class-action lawsuits, and the often-irreparable damage to a company's reputation and customer trust.16

The increasing frequency and financial impact of ransomware attacks in the energy sector, as evidenced by the quadrupling of recovery costs, directly amplify the significance of cybersecurity in deal valuation. As the potential cost of a cyber incident rises, the financial liability of inheriting a weak security posture becomes a more dominant factor. This dynamic creates a significant opportunity for a buyer to negotiate a more favorable price based on the quantifiable, and rising, remediation costs required to mitigate these liabilities.

#### **4.3. Using Findings to Inform Negotiation**

The knowledge gained from a thorough due diligence assessment can have a critical impact on the deal's terms and cost.6 The acquirer can use the findings as leverage to negotiate a price reduction that accounts for the cost of identified remediation projects and potential liabilities.2 Beyond a simple price adjustment, the acquirer can also use the findings to structure the deal in other ways. This may include establishing an escrow account to cover remediation costs or inserting specific cyber-related representations and warranties into the deal terms to hedge against residual risk.2 This process transforms technical findings into tangible business adjustments, allowing deal teams to negotiate with the same discipline they would apply to financial multiples.2

#### **Table 3: Valuing Cyber Risk: A Financial Impact Model**

| Risk Scenario | Due Diligence Finding | Potential Business Impact | Estimated Financial Cost |
| --- | --- | --- | --- |
| **Ransomware Attack** | Legacy OT systems with unpatched software 26 | Operational downtime, disruption of service, physical damage 28 | $3 million (median recovery cost) 44 |
| **Data Breach** | Weak authentication, lack of MFA on customer platforms 31 | Loss of customer trust, reputational damage, legal action 45 | Significant regulatory fines and legal fees 16 |
| **Regulatory Fine** | No Critical Infrastructure Risk Management Program (CIRMP) 5 | Non-compliance penalties, legal proceedings 5 | Substantial financial penalties and reputational damage 5 |

### **V. Post-Acquisition: Securing and Integrating the Investment**

The period immediately following an acquisition is a time of heightened vulnerability, as IT resources are often overstretched and systems are being integrated.1 The Australian threat report notes that a high percentage of attacks are initiated during business disruptions such as mergers, when IT teams are less likely to be operating at full capacity.47 A structured, security-first integration plan is therefore essential to protect the value of the investment.

#### **5.1. The First 100 Days: A Critical Integration Plan**

The initial phase of integration is critical for establishing a unified and secure operational environment.48 The plan should include the following key steps:

* **Establish a Dedicated Integration Management Office (IMO):** A cross-functional team, including leaders from IT, legal, HR, and security, should be assembled to oversee the integration process and assign clear responsibilities to all team members.49
* **Conduct Security Assessments and Inventory:** Before any network integration, a final security assessment of all systems should be performed, and a comprehensive, unified asset inventory should be created.13 The inventory should identify obsolete or outdated assets that must be retired or remediated.13
* **Implement Enhanced Monitoring:** Deploy enhanced security monitoring tools during the integration phase to detect potential security incidents that might be masked by the influx of activity.48
* **Harmonize Policies and Governance:** Review and align the information security and HR policies of both organizations and ensure all employees receive updated security training and policy acknowledgments.13

#### **5.2. Framework-Based Integration for Long-Term Resilience**

A framework-based approach provides a systematic and defensible method for achieving long-term cybersecurity resilience.

* **NIST Cybersecurity Framework (CSF):** The NIST CSF 2.0 provides a clear, outcome-based structure for managing and reducing cybersecurity risks.51 The framework's core functions—Govern, Identify, Protect, Detect, Respond, and Recover—provide a clear roadmap for post-acquisition security uplift.2 The new  
  Govern function, in particular, is highly relevant for the venture capital firm's board, as it emphasizes establishing and monitoring a cybersecurity risk management strategy that is aligned with business objectives.52
* **ISO 27001:** This international standard for an Information Security Management System (ISMS) provides a systematic approach to managing and protecting information assets.54 A target company with an existing ISO 27001 certification may have compatible information security practices, which can streamline the integration process and reduce the time and costs associated with consolidating IT systems and cultures.54

#### **5.3. Developing a Culture of Cyber Vigilance**

Technical controls alone are insufficient to mitigate risk. The human element remains a primary attack vector, with threats like phishing and social engineering being common entry points for critical infrastructure incidents.8 To combat this, the firm must invest in continuous cybersecurity training for all employees to reduce human error and susceptibility to attacks.13 This cultural shift, which includes a focus on robust password management and clear communication channels, is a critical, long-term value-creation activity that strengthens the entire organization's security posture.9

### **VI. Actionable Recommendations and Strategic Roadmap**

Based on the analysis of the Australian energy sector's threat landscape, the regulatory environment, and the financial implications of cyber risk, the following phased roadmap is recommended for the venture capital firm.

* **Phase I: Pre-Deal (Due Diligence & Valuation)**
  + **Recommendation 1: Conduct Multi-Layered Cyber Due Diligence.** Move beyond a basic checklist and engage specialist firms to conduct practical exercises. This includes both a tabletop exercise to test the target's incident response plans and a targeted red team assessment to test the attack paths between corporate IT and the OT environment. This provides a battle-tested and objective measure of the target's resilience.
  + **Recommendation 2: Understand and Model Regulatory Compliance.** Assess the target's readiness to comply with mandatory SOCI Act obligations, including its Critical Infrastructure Risk Management Program. Use the Australian Energy Sector Cybersecurity Framework (AESCSF) as a benchmark for maturity, and identify any gaps that would require remediation.
  + **Recommendation 3: Quantify Cyber Risk for Negotiation.** Use the findings from the due diligence activities and the identified costs of remediation to develop a formal, risk-adjusted valuation model. This can be used to negotiate a price adjustment, establish an escrow account for remediation, or insert protective clauses into the deal terms to safeguard against future liabilities.
* **Phase II: Post-Close (First 100 Days)**
  + **Recommendation 4: Execute a Security-First Integration Plan.** Immediately form an Integration Management Office (IMO) and implement a plan that prioritizes cybersecurity. This includes a final asset inventory, the immediate deployment of enhanced monitoring, and the rapid harmonization of security policies.
  + **Recommendation 5: Meet Immediate Regulatory Obligations.** Begin the process of meeting mandatory SOCI Act Positive Security Obligations, including registering critical assets and establishing a mandatory reporting process for cyber incidents with the ACSC.
* **Phase III: Long-Term (Value Creation)**
  + **Recommendation 6: Implement a Framework-Based Security Uplift.** Use a recognized framework like the NIST Cybersecurity Framework (CSF) 2.0 to guide the long-term security uplift of the new entity. This includes modernizing legacy systems, securing smart meters, and strengthening controls around identity and access management.
  + **Recommendation 7: Foster a Culture of Cyber Vigilance.** Invest in continuous and comprehensive cybersecurity training for all employees to address the human element of risk and reduce the likelihood of incidents caused by phishing or other forms of social engineering. This will build long-term resilience and protect the value of the acquired asset.

#### Works cited

1. The Role of Cybersecurity in Mergers and Acquisitions (M&A) | UpGuard, accessed August 14, 2025, <https://www.upguard.com/blog/the-role-of-cybersecurity-in-mergers-and-acquisitions>
2. How Cyber Due Diligence Can Impact an M&A Valuation, accessed August 14, 2025, <https://www.rexoncyber.com/blog/how-cyber-due-diligence-can-impact-an-ma-valuation>
3. Is Australia's energy sector at risk? | Eftsure AU, accessed August 14, 2025, <https://www.eftsure.com/en-au/blog/industry-news/is-australias-energy-sector-at-risk/>
4. Cybersecurity Concerns Rise for Australia's Infrastructure - Cyber Magazine, accessed August 14, 2025, <https://cybermagazine.com/articles/australia-11-of-cyber-incidents-hit-infrastructure>
5. SOCI Act: Protecting the Security of Critical Infrastructure - KPMG International, accessed August 14, 2025, <https://kpmg.com/au/en/insights/risk-regulation/critical-infrastructure-reforms.html>
6. Cybersecurity Due Diligence: A Practical Guide - Kroll, accessed August 14, 2025, <https://www.kroll.com/en/insights/publications/cyber/cybersecurity-due-diligence-a-practical-guide>
7. Why Cyber Due Diligence is Critical for M&A Success - River Security, accessed August 14, 2025, <https://riversecurity.eu/why-cyber-due-diligence-is-critical-for-ma-success/>
8. Annual Cyber Threat Report 2023-2024 | Cyber.gov.au, accessed August 14, 2025, <https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024>
9. Cybersecurity for Electricity Distribution [2025 Update] - Tripwire, accessed August 14, 2025, <https://www.tripwire.com/state-of-security/cybersecurity-electricity-distribution-2025-update>
10. Safeguarding critical infrastructure | Community support - Queensland Government, accessed August 14, 2025, <https://www.qld.gov.au/community/your-home-community/cyber-security/cyber-security-for-queenslanders/case-studies/safeguarding-critical-infrastructure>
11. Energy company AGL reports cyber incident | Insurance Business Australia, accessed August 14, 2025, <https://www.insurancebusinessmag.com/au/news/cyber/energy-company-agl-reports-cyber-incident-429425.aspx>
12. AGL Cyber Attack Incident Has Caused Customer Account Lockdown - 2Fa.tv, accessed August 14, 2025, <https://www.2fa.tv/2022/12/07/agl-cyber-attack-incident-has-caused-customer-account-lockdown/>
13. Mergers and Acquisitions Cybersecurity Checklist - FRSecure, accessed August 14, 2025, <https://frsecure.com/mergers-and-acquisitions-cybersecurity-checklist/>
14. 5 Steps for Evaluating Cybersecurity Before an Acquisition - Tanium, accessed August 14, 2025, <https://www.tanium.com/blog/5-steps-for-evaluating-cybersecurity-before-an-acquisition/>
15. 2025 Cybersecurity Guide to Due Diligence in M&A Transactions - Virtual Data Rooms, accessed August 14, 2025, <https://datarooms.org/vdr-blog/cybersecurity-due-diligence-in-mergers-and-acquisitions/>
16. The Importance of Cybersecurity in Mergers & Acquisitions - Allegrow, accessed August 14, 2025, <https://allegrow.com/cybersecurity-m-a/>
17. Start Your Ransomware Readiness Assessment | Bishop Fox, accessed August 14, 2025, <https://bishopfox.com/services/ransomware-readiness>
18. ECSO Guidance - Cyber Security Exercises, accessed August 14, 2025, <https://www.cisc.gov.au/resources-subsite/Documents/ecso-guidance-cyber-security-exercises.pdf>
19. Tabletop and Simulation exercises - Deloitte, accessed August 14, 2025, <https://www.deloitte.com/ce/en/services/consulting/perspectives/hr-tabletop-and-simulation-exercises.html>
20. How to Run a Ransomware Tabletop Exercise [+ Scenarios] - AlertMedia, accessed August 14, 2025, <https://www.alertmedia.com/blog/ransomware-tabletop-exercise/>
21. How to Run Incident Response Tabletop Exercises in 2025 - Sygnia, accessed August 14, 2025, <https://www.sygnia.co/blog/incident-response-tabletop-exercise/>
22. What Is Red Teaming and How Does It Work? | Black Duck, accessed August 14, 2025, <https://www.blackduck.com/glossary/what-is-red-teaming.html>
23. Red Team Services | Black Duck, accessed August 14, 2025, <https://www.blackduck.com/services/security-program/red-teaming.html>
24. Case Study: Red Team Assessment - Bridewell Consulting, accessed August 14, 2025, <https://www.bridewell.com/insights/case-studies/detail/case-study-red-team-assessment>
25. Red Teaming a Law Firm | Black Duck, accessed August 14, 2025, <https://www.blackduck.com/content/dam/black-duck/en-us/case-studies/red-teaming-a-law-firm.pdf>
26. 9 SCADA System Vulnerabilities and How to Secure Them, accessed August 14, 2025, <https://gca.isa.org/blog/9-scada-system-vulnerabilities-and-how-to-secure-them>
27. Consumer energy resources: Cyber security - KWM, accessed August 14, 2025, <https://www.kwm.com/au/en/insights/latest-thinking/consumer-energy-resources-cyber-security.html>
28. Cybersecurity in Power Grids: Challenges and Opportunities - PMC, accessed August 14, 2025, <https://pmc.ncbi.nlm.nih.gov/articles/PMC8473297/>
29. False data injection attack in smart grid: Attack model and reinforcement learning-based detection method - Frontiers, accessed August 14, 2025, <https://www.frontiersin.org/journals/energy-research/articles/10.3389/fenrg.2022.1104989/full>
30. Detecting False Data Injection Attacks in Smart Grids: A Semi-supervised Deep Learning Approach - DOE OSTI, accessed August 14, 2025, <https://www.osti.gov/servlets/purl/1812900>
31. Cybersecurity and Major Cyber Threats of Smart Meters: A Systematic Mapping Review, accessed August 14, 2025, <https://www.mdpi.com/1996-1073/18/6/1445>
32. Cybersecurity and Major Cyberthreats of Smart Meters: A Systematic Mapping Study - Preprints.org, accessed August 14, 2025, <https://www.preprints.org/frontend/manuscript/69ee8cc469fae138faddc9ec655e7eff/download_pub>
33. Cybersecurity in Smart Metering: Standards, Threats & Compliance - Kalkitech, accessed August 14, 2025, <https://kalkitech.com/cybersecurity-in-smart-metering-standards-threats-compliance/>
34. Security Of Critical Infrastructure | CyberCX, accessed August 14, 2025, <https://cybercx.com.au/security-of-critical-infrastructure-act/>
35. SOCI Act Explained: Compliance Rules & Requirements - UpGuard, accessed August 14, 2025, <https://www.upguard.com/blog/soci-act-2018>
36. CISC Factsheet - Systems of National Significance and Enhanced Cyber Security Obligations, accessed August 14, 2025, <https://www.cisc.gov.au/resources-subsite/Documents/cisc-factsheet-systems-of-national-significance-enhanced-cyber-security-obligations.pdf>
37. Australian Energy Sector Cybersecurity Framework (AESCSF ..., accessed August 14, 2025, <https://www.industrialdefender.com/resources/aescsf-mapping-guide-industrial-defender>
38. Australian AESCSF Authoritative Source - Archer Exchange, accessed August 14, 2025, <https://archerirm.exchange/en-US/apps/420625/australian-aescsf-authoritative-source/features>
39. Cyber security roles and responsibilities | AEMC, accessed August 14, 2025, <https://www.aemc.gov.au/rule-changes/cyber-security-roles-and-responsibilities>
40. Cyber Security Threats In Mergers & Acquisitions (M&A) - PwC UK, accessed August 14, 2025, <https://www.pwc.co.uk/services/technology/cyber-security-services/strategy-advisory/mergers-and-acquisitions.html>
41. Understanding cyber due diligence - PwC, accessed August 14, 2025, <https://www.pwc.com/us/en/services/consulting/deals/library/understanding-cyber-due-diligence.html>
42. Cybersecurity in Mergers & Acquisitions: The Overlooked Risk That Could Derail Your Deal, accessed August 14, 2025, <https://securityboulevard.com/2025/08/cybersecurity-in-mergers-acquisitions-the-overlooked-risk-that-could-derail-your-deal/>
43. The Real Cost of Cybersecurity Due Diligence: What You're Paying For and Why It Varies So Much - Atlant | Security, accessed August 14, 2025, <https://atlantsecurity.com/blog/cost-of-cybersecurity-due-diligence/>
44. The Median Recovery Costs for 2 Critical Infrastructure Sectors, Energy and Water, Quadruples to $3 Million in 1 Year, Sophos Survey Finds, accessed August 14, 2025, <https://www.sophos.com/en-us/press/press-releases/2024/07/median-recovery-costs-2-critical-infrastructure-sectors-energy-and>
45. Cyber Case Study: Colonial Pipeline Ransomware Attack | INSURICA, accessed August 14, 2025, <https://insurica.com/blog/colonial-pipeline-ransomware-attack/>
46. Cybersecurity Risk Due Diligence for M&As | Kovrr, accessed August 14, 2025, <https://www.kovrr.com/cyber-risk-due-diligence-ma>
47. ANZ firms face rising repeat ransomware attacks & executive threats - SecurityBrief Australia, accessed August 14, 2025, <https://securitybrief.com.au/story/anz-firms-face-rising-repeat-ransomware-attacks-executive-threats>
48. Post-Acquisition Integration & Compliance Strategies, accessed August 14, 2025, <https://msi-international.com/post-acquisition-integration-compliance-strategies/>
49. The Ultimate Post-Acquisition Integration Checklist - Allegrow, accessed August 14, 2025, <https://allegrow.com/post-acquisition-integration-checklist/>
50. Post-Merger Integration Explained: Key Stages, Focus Areas + Checklist, accessed August 14, 2025, <https://www.idealsvdr.com/blog/post-merger-integration-process-checklist/>
51. Cybersecurity framework - GSA, accessed August 14, 2025, <https://www.gsa.gov/technology/government-it-initiatives/cybersecurity/cybersecurity-framework>
52. The NIST Cybersecurity Framework (CSF) 2.0, accessed August 14, 2025, <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>
53. NIST Cybersecurity Framework and NIST Cybersecurity Framework 2.0 - SailPoint, accessed August 14, 2025, <https://www.sailpoint.com/identity-library/nist-cybersecurity-framework>
54. What are the implications of ISO/IEC 27001 on mergers and acquisitions, particularly in due diligence processes? - Flevy.com, accessed August 14, 2025, <https://flevy.com/topic/iec-27001/question/impact-iso-iec-27001-manda-due-diligence-processes>