Safeguarding the Grid:

# Cyber Threats in Energy Infrastructure

The Transformation Group

Talenza | Tranzformd.

# Key Themes of the Report

- Supply Chain Security
- Securing Operational Technology
- Balancing Innovation and Risk
- Proactive Planning and Assessment
- Securing the Transition to Smart Grids and Cleaner Futures
- Finding, Retaining, and Training Talent

Cyber-attacks on energy, transportation, and telecommunications are on the rise, with a 30% increase in just one year, according to a report from KnowBe4. As these sectors become more reliant on digital technologies, new vulnerabilities emerge, making them prime targets for cyber threats.

The KnowBe4 report highlights the serious risks these attacks pose to national security, with geopolitical adversaries increasingly using them as digital weapons.

In Australia, the SoCI Act (Security of Critical Infrastructure Act 2018) aims to protect critical infrastructure, ensuring the resilience of essential systems and services. To meet these standards, major cyber security initiatives have been implemented across sectors like energy.

**But what does this mean for businesses in 2025 and beyond? How will cyber security regulations shape future operations and priorities?**

## Looking at the Landscape

Over the last decade, Australian and international energy companies have been targeted by cyber security incidents. Here's a rundown:

2019

**SolarWinds:** Russian hackers targeted the software supply chain of SolarWinds' Orion platform, affecting over 18,000 customers, including energy companies.

2020

**CS Energy:** Millions of Australian homes were potentially moments away from losing power after CS Energy was hit by a ransomware attack believed to have been executed by a group of Chinese hackers.

2021

**Colonial Pipeline:** A ransomware attack by DarkSide group targeted the largest fuel pipeline in the US, causing significant disruptions. It was the largest cyber-attack on critical infrastructure in the United States that had been publicly disclosed.

2022

**EnergyAustralia:** 323 Australian residential and small business customers were affected by unauthorised access to the EnergyAustralia online platform, exposing personal details and billing information.

**Icon Energy:** A sophisticated ransomware attack encrypted critical systems of this Australian energy retailer.

2023

**3CX:** A supply chain attack on software company 3CX compromised two energy firms and two financial traders as part of their 600,000 global customers. The malware deployed a multi-stage backdoor enabled attackers to steal corporate login credentials from the employee's device, as well as loading on device startup, which gave attackers remote access to all compromised connected devices.

2024

**Sumo Energy and Telecomunnications:** The Australian energy and telecommunications provider experienced a data breach affecting approximately 40,000 customers. The compromised data included full names, email addresses, phone numbers, billing addresses, and account details.

# Supply Chain Security

More than one-third of procurement energy professionals suspect undisclosed breaches among their suppliers and across their supply chain globally according to the latest Energy Cyber Priority report from DNV Cyber.

Energy and utilities companies are implementing a range of strategies to secure their supply chains and mitigate cyber security risks associated with suppliers, vendors, and partners. At the same time, the Australian Government is looking at ways to build resilience into the national energy supply chain.

> Mature businesses are viewing cyber risks from a different lens – if we reduce our cyber risk we can win more business OR avoid actual costs from a breach."

**Riki Blok, Practice Manager, Cyber.**

## Key Trends to Watch

| | |
|---|---|
| **Supply Chain Visibility** | End-to-end transparency, digital tracking (AI, IoT, blockchain), regulatory-driven traceability. |
| **Supplier Security** | Heightened focus on third-party risk, AI for threat detection, collaborative cyber security efforts. |
| **Procurement** | AI-driven automation, resilience/diversification, ESG integration, data-centric decision-making. |

# Securing Operational Technology

Securing Operational Technology (OT) hardware and software systems ensures that energy companies and Government departments can monitor, control, and optimise the physical processes in energy generation, transmission, distribution, and storage, regardless of circumstances.

71% of energy professionals acknowledge that their organisations are more vulnerable to OT cyber events than ever before, with 57% saying that their OT defences lag their IT defences in a DNV Cyber report.

## What About Australia's OT?

Endeavour Energy achieved ISO 27001:2022 certification for its Information Security Management System (ISMS), covering 20 physical locations including 16 critical substations and control rooms. This certification ensures secure, reliable services across Endeavour Energy's critical infrastructure, including data centres, training rooms, and secondary systems. The project involved integrating both Operational Technology (OT) and Information Technology (IT) systems to bolster cyber resilience.

According to an Endeavour Energy press release, the implementation of the project alongside a consultancy took 18 months.

Ausgrid has planned an Operational Technology Security Program which aligns with industry best practices and complies with regulatory obligations, including SoCI and the Electricity Supply Act 1995 (NSW).

The program focusses on key areas such as Control System Isolation and Segregation, Control System Distribution Network Management System Improvements, Control System Security Architecture, and Security Information and Event Management (SIEM) to improve risk management by addressing emerging threat actors targeting OT environments. The Ausgrid report stated that projects will run from 2025-2029 and be prioritised on an annual basis.

This program reflects Ausgrid's commitment to strengthening its OT security posture in response to the dynamic cyber threat environment.

### Skills, Technologies and Technical Concepts

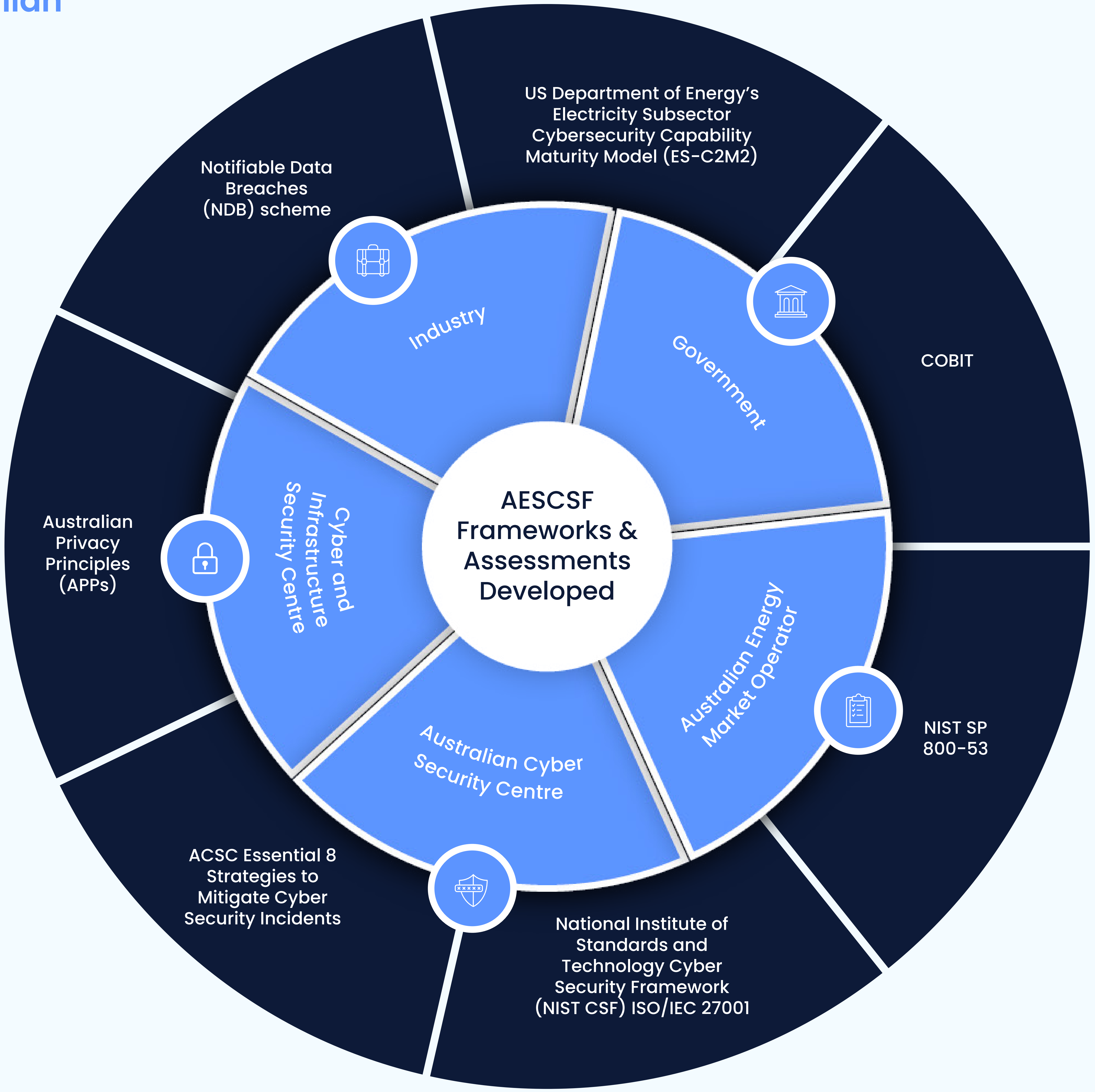
- Information Security Management
- OT/IT integration
- Risk assessment
- Security control implementation
- Advanced grid management technologies
- Security Information and Event Management (SIEM)
- Control System Distribution Network Management System
- SCADA systems
- ISMS covering both IT and OT
- OT security architecture
- Network segmentation

# Proactive Planning and Assessment

## Preparing for new and emerging cyber threats

Digital technologies are essential to drive and enable the energy transition, but introducing new tech potentially broadens exposure to cyber risk.

## Developing Australian Frameworks and Assessments



AESCSF Frameworks & Assessments Developed
Industry
Government
Australian Energy Market Operator
Australian Cyber Security Centre
Cyber and Infrastructure Security Centre
Notifiable Data Breaches (NDB) scheme
US Department of Energy’s Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)
COBIT
NIST SP 800-53
National Institute of Standards and Technology Cyber Security Framework (NIST CSF) ISO/IEC 27001
ACSC Essential 8 Strategies to Mitigate Cyber Security Incidents
Australian Privacy Principles (APPs)

# Key Trends in Cyber Security Innovation

## Practices to Build Cyber Safe Innovation

### Security from the Start

- New applications and digital services integrate security requirements from day one and beyond, "secure-by-design" principles lead the way and continuously protect bespoke applications.
- Cloud solutions are adopted with strict vendor security and data privacy controls.

### Risk-Based Approach

- Businesses prioritise threats with regular risk assessments and incident response exercises.
- AI-powered threat detection helps monitor and mitigate risks in real-time.
- Data-driven insights ensure cyber security efforts focus on the biggest risks.

### Building a Security-Minded Culture

- Cyber security training and awareness programs keep employees informed and act as your first line of defence.
- A shared responsibility approach makes security part of everyday work. Use gamification to make it fun and memorable, embedding security into work culture!
- Approach incidents with a positive and calm mindset. People need to be positive about raising incidents and not be scared of repercussions.

### Holistic Cyber Security Frameworks

- Companies align cyber security with business goals, ensuring security supports, rather than stifles, innovation.
- Continuous monitoring and updates keep defences strong.

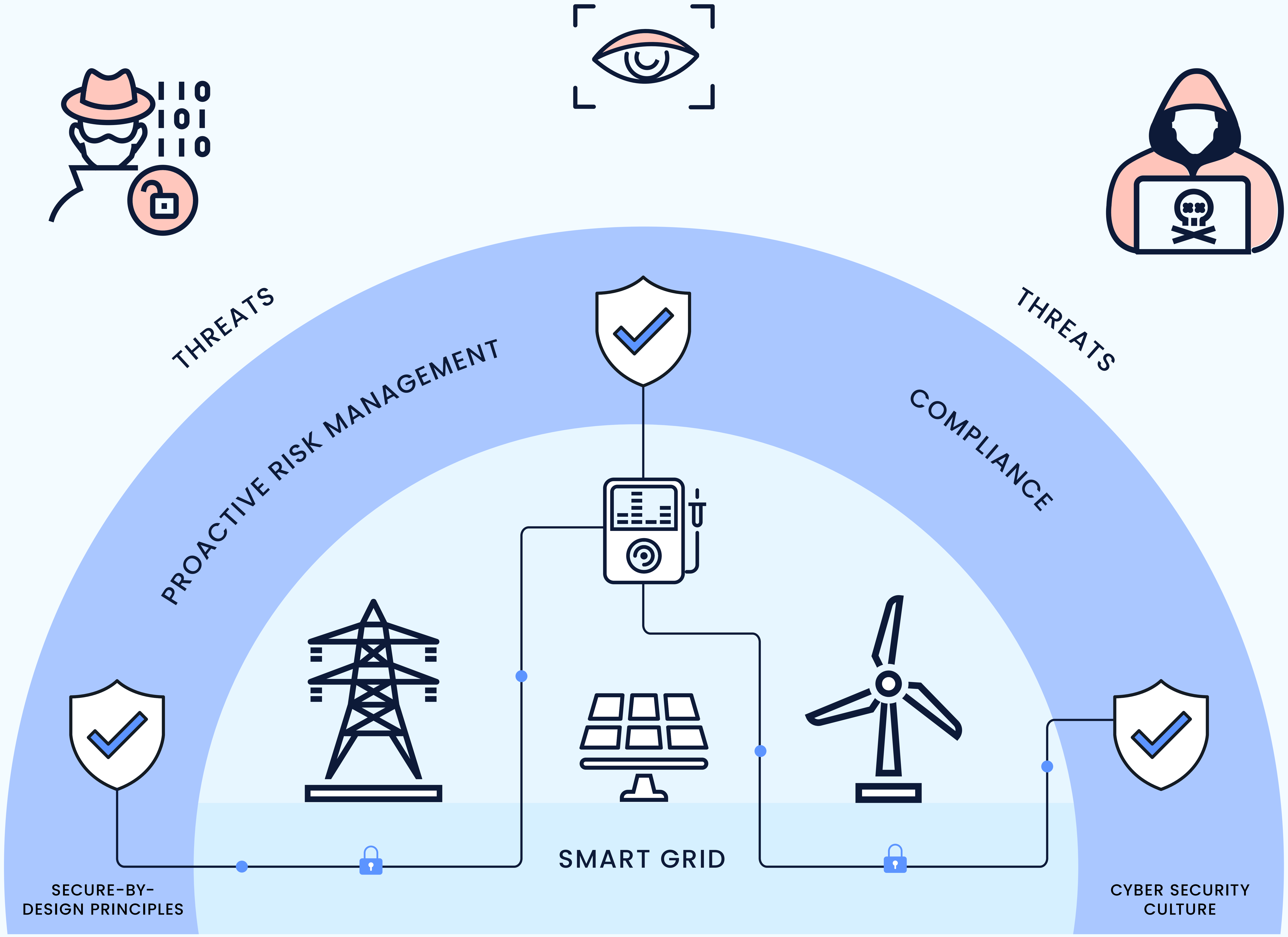
### Experimenting with IT Innovation

- Small-scale trials in isolated environments allow safe testing of new tech.
- Gradual scaling ensures security and privacy are maintained.

**By implementing these strategies, companies can navigate the complex landscape of digital innovation while maintaining robust cyber security measures. This balanced approach allows organisations to harness the power of new technologies while safeguarding against emerging cyber threats.**

# Securing the Transition to Smart Grids and Cleaner Futures

As we transition to smart grids and cleaner energy, digital technologies bring new risks. Staying secure means going beyond compliance, embedding secure-by-design principles, proactive risk management, and a strong cyber security culture.



Talenza

# Tips for Industry and Employers to Build Out the Cyber Workforce

The Tech Council of Australia has identified 5 key principles that it can use with Industry and Government to bring people into the workforce and deliver the skills for the future:

- ✔ Deliver a new modern Australian Digital Apprenticeship, to better meet the future needs of tech jobs.
- ✔ Define skills standards and pathways into tech jobs.
- ✔ Better identify and recognise innovative training solutions.
- ✔ Improve support for women to transition into tech jobs.
- ✔ Conduct ongoing data analysis and tech workforce planning in conjunction with Jobs and Skills Australia.

Alongside this, the TCA have recently launched the Consumer Energy Tech Alliance – CETA. Collaboration between both branches of the Tech Council would benefit the industry and talent, providing necessary training and industry awareness within tech pathways.

**The ASD has established a digital career pathway map and learning and development pathways. These can be found linked here**

> "The Australian Energy Sector Cyber Security Framework (AESCSF) has provided an excellent opportunity for Asset Operators to build a common language and guidance for Cyber Security for energy asset operators."

**Bruce Large, Director & Principal Cyber Security Architect at BLARGE.**

# Conclusion

Cyber security in critical infrastructure remains a top priority as the landscape of threats continues to evolve. However, the perspectives and priorities of various stakeholders, including Boards, CEOs, CISOs, and teams, can vary significantly in terms of day-to-day execution and strategic focus. It is crucial for organisations to remain proactive in adapting to these challenges while aligning their talent strategies with the ever-changing demands of cyber security.

By focusing on recruitment and talent development, organisations can build resilient, adaptable teams capable of safeguarding critical infrastructure. Leveraging skills-based hiring, providing career development opportunities, and fostering an inclusive, flexible work environment are key strategies that can support long-term success in this high-stakes field.

## Talenza Key Talent Takeaways:

- ✔ Look to use the shift in skills-based hiring to access candidates who understand wider the business impacts and objectives of Cyber, and advocate for it as a growth lever.
- ✔ Advance your talent strategy by developing career pathways and learning opportunities that foster retention, adaptability, and a pipeline of skilled professionals ready to meet evolving cyber security challenges.
- ✔ Use gender neutral language in job ads and conduct periodic review of your recruitment advertising language to ensure fair access for all.
- ✔ Consider flexible working or job-sharing agreements to allow more people to participate in cyber security.
- ✔ Embrace tech innovation. The rise of green energy and smart grids presents both new opportunities and risks, so recruit talent capable of navigating the balance between innovation and security. This provides exciting, new, and challenging work for talent.
- ✔ Create a culture of agility and adaptability to balance the psychosocial risks of ever-changing threats and new challenges. Supplement this with wellbeing and other meaningful benefits to retain top talent and top performance.

## Tranzformd. Key Takeaways:

Digital transformation is no longer just a buzz-phrase; it is a critical enabler of business success and resilience. As organisations embrace new technologies and innovative solutions, the need for a cohesive strategy that aligns cyber security and data strategy with broader business objectives becomes more urgent. Companies must foster a culture of innovation, adaptability, and continuous learning to navigate this ever-evolving digital landscape.

- ✔ Run data maturity assessments to really know and understand your data landscape
- ✔ Review your data retention and storage policies in line with new legislation
- ✔ Know the legal landscape
- ✔ Test and improve your incident response plan
- ✔ Invest in proactive cyber and data plans to create a competitive advantage, gain customer trust and market share

# Authors & Contributors

**Riki Blok**

Practice Lead, Security

**Chelsey Costello**

Practice Lead, Security

**Bruce Large**

Principal Cyber Security Architect

**Charlie Hales**

Director of Consulting

**Laurie Weeks**

Account Director

# Sources and Data Points

1. www.imperva.com/cyber-threat-index/
2. advantechww.com/the-guide-to-digital-transformation-strategies-in-energy-industry-in-2025/
3. discoveryalert.com.au/news-article/mining-sustainability-transformation-2025-tried-tested/
4. www.securityinfowatch.com/cybersecurity/press-release/55262561/energy-companies-boost-investment-in-cyber-arms-race-to-manage-industrys-greatest-risk
5. www.processunity.com/iconic-data-breaches-in-energy-industry/
6. www.cyberdaily.au/security/8372-hundreds-of-energy-australia-customers-at-risk-following-security-breach
7. www.corbado.com/blog/data-breaches-australia
8. kbi.media/australian-energy-sector-grappling-with-rising-ransomware-threat/
9. www.eurelectric.org/in-detail/cybersecurity-in-the-power-sector/
10. industrialcyber.co/critical-infrastructure/critical-infrastructure-faces-30-percent-surge-in-cyber-attacks-knowbe4-report-highlights/
11. www.dnv.com/cyber/insights/news/energy-companies-boosting-investment-in-cybersecurity-arms-race-to-manage-the-greatest-risk-to-the-industry-today/
12. www.endeavourenergy.com.au/news/media-releases/australian-first-paving-the-way-for-a-cyber-secure-energy-future
13. www.aer.gov.au/system/files/Ausgrid%20-%20Att.%205.8.d%20-%20Operational%20technology%20security%20program%20-%2031%20Jan%202023%20-%20Public.pdf
14. www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=economics%2Foilrefineries%2Freport%2Fchapter4.htm
15. aemo.com.au/initiatives/major-programs/cyber-security
16. www.actu.org.au/wp-content/uploads/2023/07/energy-security-2021.pdf
17. www.ussc.edu.au/should-australia-make-solar-panels-supply-chain-security-through-global-engagement
18. www.industry.gov.au/trade/office-supply-chain-resilience
19. www.cisc.gov.au/resources-subsite/Documents/raa-energy.pdf
20. www.oaic.gov.au/engage-with-us/research-and-training-resources/research/australian-community-attitudes-to-privacy-survey/australian-community-attitudes-to-privacy-survey-2023
21. LinkedIn Talent Insights
22. www.awsn.org.au/news-item/18305/awsns-women-in-security-mentoring-program-wins-global-award-for-diversity-in-cybersecurity
23. techcouncil.com.au/wp-content/uploads/2022/08/2022-Getting-to-1.2-million-report.pdf
24. techcouncil.com.au/newsroom/tca-launches-the-consumer-energy-tech-alliance/
25. behaviouraleconomics.pmc.gov.au/sites/default/files/projects/attracting-diverse-cyber-security-workforce.pdf