
Australian Local Government Association
Technical Leadership Summit 2025
Cr. Jeff Whitton FAICD, CDPSE

Cr. Jeff Whitton FAICD, CDPSE

Certified Subject Matter Expert

- Cyber Threat Intelligence Analysis
- Cyber Security Incident Response, Investigation & Forensics
- Cyber Security Defence & Operations
- Disaster Response & Recovery

0419 5888 15 - jeff.whitton@jargrove.com.au

- 40 years in the Telco, IT & Cyber Security, OSI Full Stack Subject Matter Expert
- 30 years in Board Rooms
- Fellow Australian Institute of Company Directors
- Ambassador, NSW Cyber Security Hub, NSW Investment
- Current NSW Local Government Councillor 20 years
- Certified Data Privacy Solutions Engineer
- Board Advisor, Critical Infrastructure - ISAC, Australia
- Australian Defence Certified Chief Security Officer
- Global Advisor BITO and Australian Chair, BITO -Australia.
- CEO 27 years, Digital Tech & Cyber Security company ,Australia, NZ, Singapore.
- Cyber Security & GRC advisor, University Infrastructure Committee of the Board of Trustees Western Sydney University
- Advisory Board Member for the School of Computing and Engineering, Macquarie University
- Chairman of the NFP Disability Employment Services provider in Australia, OCTEC Limited.
- Co-Founding Director, of Australian Indigenous Cyber Security Company
- Executive Committee Member, Australian Information Security Association, NSW Branch.
- Founding Non-Executive Director, NFP Marathon Health.
- Professional Member, Information Systems Audit and Control Association

Digital Forensics and **Incident Response** (DFIR) Plan is the cornerstone of a cybersecurity strategy shaping entire security posture and guiding ALL cyber strategic direction.

Developing an Incident Response (IR) plan using industry best practices, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, involves a comprehensive process that enhances our organization's resilience against cyber threats

"Who on the board understands our Cuber Securitu risk?"

"And the responsibilitu for mitigating the risk. is the boards!"

cyber.gov.au

Yes, local government entities in Australia are subject to specific compliance and reporting obligations concerning cybersecurity breaches. These obligations primarily stem from the Privacy Act 1988 and its subsequent amendments, notably the Notifiable Data Breaches (NDB) scheme introduced in 2018.

Application to Local Government: Local government agencies are generally considered "agencies" under the Privacy Act and are thus obligated to comply with its provisions, including the NDB scheme. This means that if a local council experiences a data breach involving personal information likely to cause serious harm, it must promptly notify both the affected individuals and the OAIC.

"Who on the board understands our Cuber Securitu risk?"

"And the responsibilitu for mitigating the risk. is the boards!"

cyber.gov.au

Are Councillors Responsible for Protecting Data?

Yes, but indirectly.

Councillors typically **do not** manage cybersecurity themselves, but they are responsible for ensuring their council has appropriate policies and protections.

If a council **fails to protect sensitive information** (e.g., ratepayer data, employee records), there could be **legal consequences** for the council, and councillors could face **political or governance consequences.**

If a councillor **mishandles personal data**, they may **personally breach** privacy laws, particularly if they access or disclose information improperly.

"Who on the board understands our Cuber Securitu risk?"

"And the responsibilitu for mitigating the risk. is the boards!"

cyber.gov.au

Are Councillors Responsible for Protecting Data?

Key Takeaways:

- Councillors do not have the same corporate governance obligations as company directors under ASIC regulations.
- However, they have public sector governance responsibilities and must ensure their council has appropriate cybersecurity policies.
- Councils must comply with privacy laws, and councillors could be held accountable for data mishandling.

"Who on the board understands our Cuber Securitu risk?"

"And the responsibilitu for mitigating the risk. is the boards!"

cyber.gov.au

Digital Forensics and **Incident Response** (DFIR) Plan is the cornerstone of a cybersecurity strategy shaping entire security posture and guiding ALL cyber strategic direction.

Developing an Incident Response (IR) plan using industry best practices, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, involves a comprehensive process that enhances our organization's resilience against cyber threats

"Who on the board understands our Cuber Securitu risk?"

"And the responsibilitu for mitigating the risk. is the boards!"

cyber.gov.au

The process of constructing our IR plan encompasses several critical components:

Comprehensive Asset and Risk Management: Developing the IR plan necessitates the creation of a dynamic asset register and risk register. This process identifies vulnerabilities and, crucially, pinpoints our organization's "crown jewels"—the most vital assets requiring robust protection. Such clarity enables the Board or Council to distinguish between vulnerabilities that can be promptly addressed and those that must be accepted as acceptable risks until budgetary provisions allow for remediation.

Decision-Making Framework: A well-structured IR plan provides clear guidelines for responding to security breaches, addressing critical decisions such as whether to pay a ransom and delineating the responsibilities of decision-makers. This ensures that, during an incident, actions are taken swiftly and in alignment with organizational policies and ethical considerations.

Development and Testing of Playbooks: The IR plan facilitates the creation of detailed playbooks for various incident scenarios. Regular testing of these playbooks through simulated attacks ensures that our response strategies remain effective and that our team is prepared to handle real-world incidents efficiently.

"Who on the board understands our Cuber Securitu risk?"

"And the responsibilitu for mitigating the risk. is the boards!"

cyber.gov.au

Jeff Whitton FAICD CDPSE

The process of constructing our IR plan encompasses several critical components:

Inclusive of Supply Chain Partners: DFIR plan extends beyond internal protocols to encompass our supply chain partners, ensuring a unified and comprehensive approach to cybersecurity. This holistic inclusion guarantees that all stakeholders are aligned and prepared to respond cohesively to potential threats.

Independent Evaluation: Recognizing the importance of impartiality, the development, testing, and implementation of our DFIR plan are conducted by neutral third parties, not by existing supply chain Managed Service Providers (MSPs) or Managed Security Service Providers (MSSPs). This approach ensures unbiased assessments and the integrity of our cybersecurity measures

Board/Council Ratification and Ownership: The active involvement and ratification of the IR plan by the Board or Council are imperative. This top-level endorsement ensures organizational commitment and preparedness. In the event of a cyber breach, adherence to the ratified and tested IR plan is crucial, as there may be pressures to deviate or take shortcuts. Firm commitment to the established plan safeguards the organization’s integrity and response effectiveness.

"Who on the board understands our Cuber Securitu risk?"

"And the responsibilitu for mitigating the risk. is the boards!"

cyber.gov.au

The process of constructing our IR plan encompasses several critical components:

Integration with Digital Forensic Methodologies: IR plan is intricately linked to our Digital Forensic Plan, aligning with strict methodologies akin to crime scene investigations. This integration ensures that evidence is meticulously preserved, facilitating thorough investigations and legal compliance.

By embedding these elements into our DFIR plan, we establish a robust framework that not only fortifies our cybersecurity posture but also ensures a structured, impartial, and legally sound response to any cyber incidents.

"Who on the board understands our Cuber Securitu risk?"

"And the responsibilitu for mitigating the risk. is the boards!"

cyber.gov.au

https://www.aicd.com.au/content/dam/aicd/pdf/tools-resources/director-tools/board/cyber-security-governance-principles-web3.pdf

"Who on the board understands our Cuber Securitu risk?"

"And the responsibilitu for mitigating the risk is the boards!"

Australian Government
Office of the Australian Information Commissioner

Data breach preparation and response

A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)

oaic.gov.au

https://www.oaic.gov.au/__data/assets/pdf_file/0017/1691/data-breach-preparation-and-response.pdf

"Who on the board understands our Cuber Securitu risk?"

"And the responsibilitu for mitigating the risk is the boards!"

Jeff Whitton FAICD

97% of Cyber Attacks focus on humans, not machines.

List of Cyber Breaches 2025

"Who on the board understands our Cuber Securitu risk?"

"And. the responsibilitu for mitigating the risk is the boards!"

Jeff Whitton FAICD

List of Regulators

Cyber Security NSW

Audit Office of NSW

The Office Australian Information Commissioner

Apra

Cyber and Infrastructure Security Center

Australian Cyber Security Center

Australian Defence

"Who on the board understands our Cuber Securitu risk?"

"And. the responsibilitu for mitigating the risk is the boards!"

PREPARE YOUR STAFF

Train your employees regularly on:

- Best cyber security practices.
- What to do in case of a cyber incident or attack.

Encourage your employees to visit cyber.gov.au/learn to complete the e-learning modules and quizzes.