Australian Institute of Company Directors

CYBER SECURITY COOPERATIVE RESEARCH CENTRE

Ashurst

Snapshot of Governing Through a Cyber Crisis

CYBER INCIDENT RESPONSE AND RECOVERY FOR AUSTRALIAN DIRECTORS

March 2024

Role of the board during a cyber crisis

Boards need to be confident that their organisation is ready for cyber incidents. Thorough and comprehensive planning for significant cyber incidents is key.

Boards should be prepared to become actively involved in a cyber crisis, have oversight of, and support, management's key decisions and responses.

From the outset, boards need to contemplate the long tail of potential post-incident risks, including regulatory, operational and reputational.

Readiness

KEY POINTS

Effective cyber crisis response starts with a current and comprehensive cyber incident response plan that is regularly tested and updated.

Clearly defined roles and responsibilities, including the role of the board and any board committees, are key to effective decision-making during a cyber crisis.

A thorough communications strategy is central to how an organisation manages external and internal stakeholders during a cyber crisis.

A rigorous cyber incident response training and testing program that simulates crisis conditions is a key preparedness tool for the board and management.

KEY QUESTIONS

1. Are roles and responsibilities comprehensively documented, including the role of the Chair and specific directors in the event of a significant incident?
2. Are the processes for key decision-making and external support detailed in the response plan?
3. Do we have a comprehensive approach and plan to communicating with internal and external stakeholders, including responsibilities for notifying and engaging with regulators and approving market disclosures?
4. Do we understand how insurance would operate in the event of an incident and the support the insurer can/cannot provide?
5. Do we regularly scenario test or conduct a simulation on our response plan? How often do we review the response plan and update it to ensure it reflects organisational changes and the current threat environment?

RED FLAGS

1. The board and senior management have not undertaken regular scenario testing or incident simulations to test the cyber incident response plan.
2. The organisation indicated there are no gaps in current cyber readiness.
3. Likely scenarios and consequences are undocumented with lessons from simulations not being captured or actioned.
4. It is not clear how communications with key stakeholders, including customers, will be managed in the event of a critical incident.
5. It is not clear who the organisation will engage to provide support during a critical cyber incident.

Response

KEY POINTS

The dynamic and fluid nature of a cyber crisis means the board should provide agile and timely support and oversight of management decision-making.

For larger organisations, consider establishing a Cyber Incident Sub-Committee of the board that can provide effective and agile governance during the response phase of a cyber crisis.

Consistent, timely, accurate and transparent communications with key stakeholders, such as customers and employees, is critical and plays an important role in mitigating reputational damage.

Expert external advice plays a critical role in supporting boards to effectively oversee decision-making during the response phase.

Have oversight of regulators reporting obligations, and ongoing liaison with regulatory, the ACSC and the National Cyber Coordinator.

For larger organisations, consider establishing a remediation and post-incident review team in parallel to the response team.

KEY QUESTIONS

1. Do we need to establish a sub-committee of the board to oversee management's actions during the response phase and speed-up decision-making?
2. Do we understand our legal and contractual obligations to make notifications (to whom, when and of what)? Do we have a set of priorities for the most-urgent to least-urgent notifications?
3. Who has primary responsibility for making those notifications? Has legal advice been sought on those notifications and their content?
4. Are we satisfied that the resources available to the management team to respond to the incident are appropriate given the scale and complexity of the organisation and the nature of the incident?
5. What key third-party providers are we relying on to provide support during the response phase? What is the nature of this support?

RED FLAGS

1. A significant delay in discovering the incident and understanding the impact on systems, data and key stakeholders, including employees and customers.
2. Confusing or contradictory information reported to the board and/or communicated to employees, customers and key regulators and government agencies.
3. Key elements of the cyber incident response plan not being followed; for instance, a lack of information sharing between teams, or a lack of focus on customers.
4. Failing to utilise the expertise of external advisers and cyber security professionals, including in relation to approaches to crisis management and communications, regulatory notifications and forensics.

Recovery

KEY POINTS

Oversee steps to secure systems and data are appropriate, including the implementation of any immediate or short-term investment in cyber security.

Understand the impact of the cyber crisis on employee well-being and take steps to support employees impacted by the cyber crisis.

The board should oversee a comprehensive post-incident review, which includes utilising external advice, where appropriate.

KEY QUESTIONS

1. Are there immediate security measures that can be implemented?
2. Has the board sought independent advice on the actions taken and the current level of security?
3. Does the board understand the potential risk of harm that impacted individuals face because of data loss? What steps have been taken to adequately mitigate this risk, and what additional steps can be taken?
4. Is the cost, pace and scale of recovery commensurate with the expectations of your customers, government, regulators, and other key stakeholders?
5. Does the board have oversight of ongoing regulators' investigations and requests for information?

RED FLAGS

1. A limited investigation that focuses on fixing immediate issues without identifying the underlying root causes and vulnerabilities.
2. Limited transparency to key stakeholders on the nature of the incident and how it is being remediated.
3. Accountability not apportioned fairly – failures being blamed on one or two individuals.
4. Not documenting and disseminating the lessons learned from the incident across the organisation, including how to approach crisis management.
5. No plan for supporting staff and recognising their contribution.

Remediation

KEY POINTS

Require remediation plans that are customer focused, well resourced and swiftly implemented.

Oversee continuing effective communication and support for employees, customers and third parties who may have been impacted or potentially harmed by the incident.

Oversee remediation, compensation and complaints-handling processes to customers where appropriate.

Responsibly share knowledge and insights gained from the crisis with other organisations.

KEY QUESTIONS

1. Does the board have oversight of likely potential claims which may arise out of the particular incident? Has a strategy been developed to handle each type of claim?
2. Are there sufficient resources and funds available to remediate at the appropriate scale and pace?
3. Has the board reviewed and approved updates to the cyber risk framework, risk appetite statements and incident response plans? Is there a continuation of the simulation and testing program scheduled?
4. Does the board have appropriate oversight over the key customer and employee issues that may require remediation?
5. How would our planned approach to remediation be viewed externally?
6. Has the board agreed, with appropriate legal advice, what lessons can be openly shared with key stakeholders?

RED FLAGS

1. Limited or no genuine attempt to recognise the impact on individual customers and provide them with appropriate support.
2. Management downplaying the severity of the incident or resisting further focus on improving cyber security.
3. No clear strategy or plan for rebuilding the organisation's reputation.
4. Limited information from management about the legal risks and external investigations resulting from the incident.

Practical guidance for SME and NFP directors

The Australian Cyber Security Centre has extensive resources to support smaller organisations available here[1].

Readiness

- Document core elements of a response plan, including:
  - Who will be responsible in leading the response to a cyber crisis?
  - What are the key systems essential to the operations of the SME and NFP?
  - Do we hold highly sensitive or critical data, for example an NFP holding the personal information of clients/beneficiaries?
  - Where are our backups located and are they secure?
  - What will be our approach to communications, including responsibilities for communications and regulatory reporting?
  - What external sources of assistance and expertise can we call on?

Response

- Seek assistance from trusted sources.
- Report the incident to the ACSC.
- Inform key stakeholders including employees, customers, and partners in a transparent, accurate and timely manner.
- Restore systems, critical operations and data from backups where possible. Prioritise recovering essential functions.
- Reset all passwords for affected accounts, including employee, customer, service and administrator accounts.
- Implement strong password policies with multi-factor authentication.

Recovery

- Where possible invest in cyber security enhancements, such as storing key data and systems with reputable cloud providers or migrating key functions to SaaS providers.
- Support impacted employees and volunteers.
- Train employees and volunteers on cyber security awareness and practical controls, including cyber hygiene and awareness of scams.

Remediation

- Where possible provide assistance to impacted individuals, including financial support to replace documents.
- Utilise templates, social media, FAQs on a website, or a dedicated customer telephone line to assist in triaging and responding to customer issues and complaints.
- Continue to communicate honestly, clearly and empathetically with impacted stakeholders.
- Demonstrate cyber enhancements to key stakeholders.
- Consider the range of appropriate remediation options that might be available to those impacted.

[1] https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/smallbusiness