Cyber resilience good practices

The following good practices enable organisations to operate highly adaptive and responsive cyber resilience processes. We encourage all organisations to discuss, share and consider their application to improve their cyber resilience preparedness.

Cybersecurity strategy and governance

The good practices we observed in relation to cybersecurity strategy and governance were characterised by board 'ownership', and responsive and agile governance models.

Good practice 1: Board engagement

Periodic review

Boards take ownership of cyber strategy and ensure it is reviewed on a periodic basis to assess progress against success measures outlined in the strategy. Measures include time to detection, speed of response and recovery process.

Cyber resilience as a management tool

The management of cyber resilience is viewed by the board as a critical management tool for understanding risk status and making important investment decisions on cyber risk. It is seen as a tool for 'enabling' (not limiting) the organisation —by anticipating scenarios and building protection against them to take advantage of market opportunities.

Cyber resilience fluency

Board members are becoming increasingly educated in the language of cyber resilience and the potential threats to organisations, and are more readily able to ask risk and audit committees the relevant questions. This reflects an active understanding of the cyber threat landscape and the planning and testing of response scenarios. See the appendix for a set of questions for board members to consider when evaluating cyber resilience within their organisations.

Assurance processes

Assurance processes are focused on end-to-end business processes. This is undertaken with a view to confirming that critical business operations, technology applications and infrastructure, and the supporting data, are tested as a whole rather than independently of business processes and technology functions. This will ensure that critical business processes can be re-activated if and when an incident occurs.

Good practice 2: Governance

Responsive governance

Organisations are tailoring traditional governance processes, to ensure 'responsive governance'. In a rapidly changing cyber risk environment, the policies and procedures of today are not necessarily valid for long periods of time, and may not remain valid between typical annual review cycles.

This approach considers how adjustments can be driven by events and incidents, rather than by keeping to a fixed review period which might ignore the need for change that arises in between set periodic review points.

Alignment with the organisations overall governance framework

Cybersecurity governance is clearly and visibly aligned to other organisation-wide governance processes and procedures. This means that documented strategies, principles, policies, rules and procedures are in line with the overall governance framework.

Cyber risk management and threat assessment

Good practice in the area of cyber risk management and threat assessment is led by intelligence gathering through the use of third-party experts, and driven by routine threat assessments, including of relevant third parties

Good practice 3: Cyber risk management

Cyber risk management is increasingly becoming intelligence-led and moving to near real-time processes through automation and use of risk management tools that can integrate many sources of risk, including those from collaboration and information-sharing sources such as peers in the industry, police and government agencies.

'Fusion' centres

Some organisations have taken the step of establishing specialist functional groups within their organisations to monitor and address risks in real time, often known as 'fusion' centres.

Third-party risk management

As outsourcing and cloud-based services become more prevalent, the reliance on third-party service providers and partners has become essential to the provision of products and services for many organisations.

Good practice 4: Third-party risk management

Organisations have developed risk-based assessment methods and tools to ensure that third-party suppliers and partners are regularly assessed to guarantee compliance with required security standards. Some organisations are also using external service providers to carry out periodic assessments of partners and vendors.

Collaboration and information sharing

Collaboration is often characterised by confidential information-sharing arrangements with other financial institutions, security agencies and law enforcement. Information sharing is fundamental for organisations that are intelligence-led and aids in understanding attackers and potential threats, including terrorist organisations, political activists, organised crime and nation-state-sponsored attackers. This process also helps organisations to understand attackers' motives—whether it be information, funds or general disruption.

Good practice 5: Collaboration and information sharing

To gather intelligence, organisations are often engaging specialist third-party organisations to undertake security monitoring and assessments. By employing the services of specialist individuals and companies operating in foreign jurisdictions, organisations are able to gather threat intelligence.

Organisations also have confidential information-sharing arrangements in place with other financial institutions, security agencies and law enforcement.

Asset management

Effective management of organisational assets is characterised by centralised management systems for critical internal and external assets (e.g. software and data), and configuration management that ensures visibility of critical assets.

Good practice 6: Asset management

Centralised asset management system

Asset inventories for hardware, software and data, both internal and external to organisations, are managed through a centralised asset management system.

Configuration management

Configuration management is important for ensuring there is visibility of critical assets across the organisation, and for managing software versions and security patches.

Cyber awareness and training

There is clear recognition that effective cyber resilience requires a strong 'cultural' focus driven by the board and reflected in organisation-wide programs for staff awareness, education and random testing, including of third parties.

Good practice 7: Cyber awareness and training

Training

Development of organisation-wide programs and strategies to ensure staff awareness and education—including for contractors and partners—which is effectively managed and monitored against success criteria.

Continuous development

Strategies based on a program of continuous development of knowledge and awareness—so that, through active vigilance, staff become an effective defence against malicious cyber activities by preventing incidents arising from attempted phishing attacks and other forms of social engineering.

Random staff testing

Random testing of staff enables the organisation to measure the effectiveness of cyber-awareness programs (e.g. a test email containing malware is sent to a staff member or group to test their response) and to take appropriate measures based on the response (i.e. staff may be required to undertake further training if they do not manage the situation in accordance with their training).

Protective measures and controls

Proactive measures and controls for cyber risks are characterised by implementation of the Australian Signals Directorate's (ASD) Strategies to mitigate targeted cyber intrusions (or equivalent), as well as a range of additional controls (e.g. encryption for 'data in transit' based on a risk assessment of the asset in question).

Good practice 8: Protective measures and controls

Organisations have already implemented, or have made it a priority to implement the ASD's 'essential eight' Strategies to mitigate targeted cyber incidents. This is accompanied by the 'essential eight maturity model' which enables organisations to self-assess their relative maturity against the essential eight recommendations.

Additionally, the more progressive organisations have also sought to apply:

- security as integral to the systems development lifecycle, sometimes known as the Security Development Lifecycle (SDL);
- encryption for stored data and 'data in transit' based on a risk assessment of the assets in question;
- filtering and monitoring of outbound email messages to ensure that data is not transmitted outside of the organisation's network in error or through intent; and
- highly restricted access to use of USB ports on computer equipment to minimise risks of data leakage or introductions of unauthorised software or files.

Detection systems and processes

There has been a lot of development in the approaches taken by 'good-practice' organisations in the area of cyber detection systems and processes. Good practices are characterised by the use of enterprise-wide continuous monitoring systems and the use of data analytics to integrate sources of threats in real time.

Good practice 9: Detection systems and processes

Continuous monitoring systems

Continuous monitoring systems, often organisation-wide, are implemented to monitor events on the organisations network and systems using Security Information and Event Management (SIEM) technologies. SIEM technologies enable the detection and alert of anomalous user behaviours such as access to applications or files, as well as abnormal movement of information across the networks measured against a baseline reference of 'normal' activity.

Data analytics

Use of data analytics to enable organisations to integrate sources of threats and associated risks into a single view of the threat landscape in real time. Threats detected by the organisation, in addition to information collected through collaboration and information-sharing channels, are analysed to move response capability towards predicting malicious cyber activities.

'Red teaming'

Employing technical specialists to work on breaking into an organisation's networks.

Response and recovery planning

Response planning for cyber risks is different from standard business continuity planning because the scenarios are not as predictable, in part due to:

- the range of threat sources (e.g. insider threats, which contribute to over 30% of identified incidents – see also, Australian Cyber Security Centre Threat Report 2017; and
- the speed at which the sophistication levels of attacks are changing.

Good practices we observed included routine and detailed scenario planning, war gaming, proactive reporting to the board and well-developed communication plans.

Good practice 10: Response planning

Organisations are adopting some of the following practices:

- Scenario planning: To predict the types of incidents that may occur based on their specific risk profile, and implementing and exercising response processes.
- War gaming: Some organisations are using war gaming techniques to better understand and plan their defence against malicious cyber activities.
- Proactive reporting to the board: Reporting of changing threats and the counter measures that are in place.

Good practice 11: Recovery planning

In the event of a data breach, organisations have actively determined when and how to notify customers—and there is a well-defined communication plan in place for managing stakeholders and public relations.

Last updated: 30/03/2021 09:26