QUESTIONS BOARD AND RISK COMMITTEES SHOULD ASK ABOUT CYBER SECURITY

Cyber security is everyone's responsibility. These questions are designed to give Boards and Risk Committees guidance on the type of information needed and actions required to take a risk management based approach to cyber security.

Governance and Culture

1. **Who is the most senior accountable officer for setting and monitoring the organisation's cyber and information security strategy?**
   Every organisation must appoint someone to develop and champion this strategy.

2. **Is the organisation's cyber culture regularly discussed by the Board?**
   Is every employee and stakeholder aware of, and 'on board' with the organisation's cyber culture?

3. **Are all senior executives engaged in the issues and risks?**
   Do they take steps to improve their organisation's cyber security culture, prevention and resilience?

4. **What is the cyber risk profile for the organisation?**
   Is the trend improving over time? Are incidents being reported appropriately to Cyber Security NSW and appropriate Commissioner(s)? Does bad news travel up to the Board? Are the recommendations from internal and external audits being implemented and reported against?

5. **Have you set a risk appetite for the organisation?**
   Do you understand potential impacts on others (below) and have you set appropriate risk tolerance statements for such events? Do you have resilience and recovery plans that address impacts according to this appetite?

6. **Have you considered cyber insurance?**
   Given the potential impacts of an incident on your organisation and on others (people and organisations), cyber insurance may be appropriate. However, having cyber insurance does not replace the need to answer and address the rest of these questions.

7. **Have you implemented the NSW Cyber Security Policy?**
   Do you know what are your "Crown Jewels"? These are your organisations highest risk assets or sets of information.

Information Security

1. **What is the full range of information you hold?**
   This includes information the organisation collects from others and generates itself. It will include the information that is 'core' to the organisation's mission as well as secondary data such as audit logs.

2. **Do you know the value of your information?**
   You must know the value of your information – not only, what it is worth to you and your customers, but also to those who may wish to steal it. If your information falls into the wrong hands, how will that impact its value to you?

3. **Where is your information stored?**
   Which systems and where are they located? If a service provider holds it for you, what are the terms of the contract? I.e. can they store it anywhere? Can they provide it to others? Are there any risks to the information being stored offshore?

4. **What is the impact to others (people and organisations) if your information is affected by an incident?**
   What is the impact to individuals if their information is exposed, corrupted or lost? Do you know how you will respond when people or organisations are impacted? Do recovery plans include restoring the impacts on others?

Service & System Security

1. **What services do you provide and to whom?**
   Do you know if your entire supply chain is secure? You need to understand the services across the full value chain – to your employees, customers or other service providers. You are only as strong as your weakest link – how secure are third party services that are part of your supply chain?

2. **What is the impact to others (people and organisations) if your services are affected by an incident?**
   What is the impact to customers if the services go offline? Are these critical infrastructure services? Do you know how you will respond when people or organisations are impacted? Do response plans address impacts on others?

Personnel Security

1. **Who has access to what information? Beware the 'trusted insider'.**
   Who has access to information – both from inside and outside your organisation – and is that level of access appropriate? What access rights or privileges do they have? Who may want to access it or corrupt it?

2. **Who is protecting your information and systems? How well are they doing it?**
   Are the minimum-security controls in place? Are there proper policies and procedures in place to secure your information? If service providers are protecting your information, do your contracts specifically account for your expectations for security? When something goes wrong are the right procedures in place and are they regularly exercised?

NSW GOVERNMENT

FURTHER RESOURCES

Who?	When/why?	How?
Agency CISO	For Information Security related incident reporting or advice, your first point of contact should always be your Agency's CISO.	Please consult your organisation's directory or contact your IT Service Desk
Cyber Security NSW	Your agency CISO works with Cyber Security NSW on high level cyber security strategy, policy and standards as well as whole of government incident reporting, coordination or advice.	community@cyber.nsw.gov.au
Australian Cyber Security Centre (ACSC)	Leads the Australian Government's efforts to improve cyber security. ACSC works with our business, government and Academic partners and experts in Australia and overseas to investigate and develop solutions to cyber security threats.	https://cyber.gov.au/acsc/report/ 1300 CYBER1 (1300 292 371)
eSafety	Leads and coordinates the online safety efforts of government, industry and the not- for-profit community in Australia. eSafety helps safeguard Australians at risk from online harms and promote safer, more positive online experiences.	https://www.esafety.gov.au/
Scamwatch	Scamwatch is run by the Australian Competition and Consumer Commission (ACCC). It provides information to consumers and small businesses about how to recognise, avoid and report scams.	https://www.scamwatch.gov.au/report-a-scam
IDSupport	IDSupport provides identity theft advice and support, including how to restore the security of your identity if your government proof of identity credentials are stolen or fraudulently obtained.	https://www.nsw.gov.au/idsupport-nsw Phone: 1800 001 040 Online form: https://www.nsw.gov.au/idsupport-nsw/contact-idsupport

NSW GOVERNMENT