Australian Government
Department of Defence
Intelligence and Security

CYBER SECURITY OPERATIONS CENTRE

PROTECT

(UPDATED) AUGUST 2012

Questions senior management need to be asking about cyber security

1. An information security breach can have a direct impact on your organisation. Cyber threats to your organisation are becoming increasingly sophisticated and targeted. The information held on your networks can be pieced together by intruders for their economic or political gain.

2. Are you confident that your networks are not currently compromised? Is the security culture of your organisation a strength or a weakness? Here are six questions you could discuss with your ICT Security Team to review your organisation's information security.

What would a serious cyber incident cost our organisation?

3. ***Good information security is like an insurance policy.*** Good security can avoid direct costs of clean-up, but also indirect costs such as downtime, lost productivity and loss of reputation and confidence in your organisation. If records such as customer records, financial data and intellectual property were stolen, could you quickly and accurately determine what was lost? What if you had to take a system offline to conduct a forensic or legal investigation?

Who would benefit from having access to our information?

4. ***Your data is valuable.*** There are many state and non-state actors who would benefit from having access to your agency's information. Identify critical information, the confidentiality, integrity and the availability of which is essential to the function of your organisation. It is important to consider the aggregated value of your information, not only the value of individual records. Every organisation faces different threats and security risks, and needs to deal with them in different ways.

What makes us secure against threats?

5. ***Security is an ongoing process, not a product.*** As cyber intrusions become more sophisticated and targeted, so do information security techniques and processes. To secure your organisation against threats, make sure appropriate security governance, clearly defined policy, user education and third party assessments are in place, as they are all vital parts of information security. There is no silver bullet for information security and security products alone are not a solution.

Is the behaviour of my staff enabling a strong security culture?

6. ***Staff education is key.*** It only takes one malicious email attachment to be opened or one malicious website to be accessed to potentially compromise your whole business. Effectively trained staff enable a strong security culture. Responsibility for information is shared amongst all members of your organisation, so all staff should be aware of the threat to reduce the security risk of valued information being stolen.

Are we ready to respond to a cyber security incident?

7. ***Will a compromise affect your continuity?*** Sadly, many organisations generally do not take information security seriously until they have been compromised. Your systems could be taken off line by an attack, for example through a denial of service attack, affecting the availability and resilience of your networks. Having access to current threat information, including the likelihood and consequences, will enable informed risk assessments.

8. Most organisations conduct fire drills – perhaps it's also time to think about testing your resilience against a serious cyber security incident.

Has your organisation applied the top four mitigation strategies?

9. ***Help is at hand.*** DSD has published *Strategies to Mitigate Targeted Cyber Intrusions* to help you dramatically improve the 'defence-in-depth' of the information entrusted to you. If your CIO was to apply just the first four mitigation strategies, it would prevent at least 85% of the cyber intrusions to which DSD responds.

Contact details

Australian government customers with questions regarding this advice should contact the DSD Advice and Assistance Line on 1300 CYBER1 (1300 292 371) or dsd.assist@defence.gov.au.

Australian businesses or other private sector organisations seeking further information should contact CERT Australia at info@cert.gov.au or by calling 1300 172 499.