Top 10 Take-Aways To Get #NDBReady

Enabling Opportunity, Realising Potential

Appoint someone at exec / board level to be responsible for cyber security who will have the authority and know-how to address the risks and demonstrate leadership during times of crisis.

Include cyber security on every board agenda or senior exec meeting, reporting on: risk to the business, nature of sensitive data and mitigation progress at a minimum.

Treat cyber security as a company-wide business risk and assess as you would with other key business risks such as major safety issues, environmental disasters and accounting scandals.

Ensure that the company understands the rapidly developing legal landscape that applies to cyber risk in particular; begin preparing NDB now.

Get specialist expertise to advise and inform execs / board, whether from internal teams or external advisors.

Set a programme of work to manage cyber risk, allowing a realistic time and budget.

Encourage discussion about cyber risk management**,** risk appetite, risk avoidance, risk mitigation and cyber security insurance.

Assume you have already been breached but you might not yet know about it. Take action to reassure yourself no such attack has taken place, but plan on the assumption that they have.

Educate your employees regularly and start build cyber security education, training and best practice into your organisation's culture.

Ask who use, access, repair, or maintain your data or systems about your organisation's data compliance rules and requirements.

PTO for Maxsum's Get #NDBReady Checklist →

Maxsum Solutions Pty. Ltd.
A.C.N. 102 287 212 A.B.N. 67 102 287 212
Mel +61 (0)3 9098 0000 Bgo: +61 (0)3 4433 9200
E: info@maxsum.com I: www.maxsum.com

Get "Notifiable Data Breach Scheme" Ready

Enabling Opportunity, Realising Potential

Governance Checklist

Item	Yes/No	Action/ Comments
***Executive Buy-In*:** Is the cyber threat landscape and NDB being discussed at board/exec level routinely?		
***Corporate Culture*:** How does security fit into your corporate culture? (Disgruntled employees are a major source of breaches.)		
Education: Do you provide organised and regular education and updates to staff on cyber threats, security, and compliance?		
***Policies & Procedures*:** Do you have policies in place that support Cloud, BYOD, and (mobile) App use? Examples include: • *Cloud Governance Strategy* • *Acceptable Use Policy* • *Data Classification Scheme* • *Data Loss Prevention Policy* • *Incident Response Plan*		
Expertise: Do you have security, legal and business technology experts providing regular advice to your board/execs?		
***Insurance*:** Do you have any or adequate cyber-insurance?		

Business Technology Checklist

Backup & Systems Replication: • Do you perform a full backup of ALL existing systems? • Is backup monitored and tested? • Do you replicate all server and software systems?		
***Document Security*:** • Have you enabled two-factor authentication? • Have you mandated the encryption of particular data and documents?		
***Digital Rights Management*:** Do you use access control technologies that restrict and control the use, modification and distribution of hardware, software and content?		
***Mobile Device Management*:** Do you have systems and technology in place for the remote lock&wipe of company mobile computing devices?		
***End-Point Protection*:** Do you have robust, best-in-class security solutions and endpoint protection in place?		
***Shadow IT*:** Have you audited unsanctioned device, cloud and app use in your organisation and performed a risk analysis?		
***Business Intelligence Tools*:** Do you use business intelligence tools and dash boarding as a risk management tool to assess and report on your Security, Availability and Recoverability risks?		
***Disaster Response & Recovery Planning*:** Do you have incident response plans in place for data breaches, as well as natural disasters, theft and loss, critical employee loss, etc.? • Do your plans detail exactly who, what, where, when and how your organisation will respond, report and recover? • Do you conduct incident response and cybersecurity drills?		

Maxsum Solutions Pty. Ltd.
A.C.N. 102 287 212 A.B.N. 67 102 287 212
Mel +61 (0)3 9098 0000 Bgo: +61 (0)3 4433 9200
E: info@maxsum.com I: www.maxsum.com