Cyber security questions to ask in your business

Cyber security questions to ask in your business

When did you last think & do something about your cybersecurity & cyber risk? What would happen if you got hacked, lost your key data or were held to ransom over stolen data? All good questions & ones that we hope that we never have to ask.

The key question around data for boards, directors, managers & business owners is:

What are the critical assets we need to protect?

The reality is that cyber criminals attack organisations of every size, seeking anything that may have value, which may include:

- Employee login details
- Staff & customer data
- Payment information (hackers may change payment data in order to divert funds to themselves)
- Strategic documents, business plans, tender information
- Lists of employees & other stakeholders

So what are you doing about it?

Consider five core principles:

1. Take a holistic approach
   a. Cyber security is treated as an enterprise risk management issue, not an IT issue

2. Understand the legislative environment
   a. Understand the legal implications of cyber risk as they apply to the organisation, as well as any privacy breach notification requirements

3. Have cybersecurity on the board agenda
   a. Management to report to the board around risks & mitigation of those risks

4. Establish a framework
   a. Set expectations that management will establish an enterprise cybersecurity management framework

5. Categorise the risks
   a. The board & management to understand what the critical cyber assets are, what level of risk is accepted, what risks are covered & not covered by insurance & any specific plans that are required

Cyber risk review questions

Question	Answer
What is the critical IT infrastructure we need to protect (internal/external) & how are we doing that?	
What are our company's most mission-critical data assets (the crown jewels), where do they reside and who can access them?	
What assurance can you give the Board that we have managed risks to privacy & security	
Has the Board been told about cyber-attacks that have occurred in the past and how severe they were? How would we know we were hacked?	
What are the organisation's cyber security risks (internal and external) and how are we managing them?	
What is management's response plan regarding cyber-attacks? What disclosure obligations exist for our organisation (internal & external)?	
Are these plans and obligations regularly tested and checked for effectiveness?	
Have we conducted a penetration test, external assessment or cybersecurity audit? What were the results and what have we changed, improved since then? Where are the priorities?	
Do we have access to cyber expertise?	
Is management reporting regularly with quality information and engaging in robust discussions about cybersecurity?	
Is management aware of the threats and who may see our organisation as a target, as well as their methods and motivations?	

Are we adhering to our internal policies (if there are any)	

Do we adhere to these four controls:

1. Restricting user installation of applications (called white listing)
2. Ensuring the operating system is patched with current updates (especially security updates)
3. Ensuring software applications have current updates
4. Restricting administrative privileges

For more information visit:

- Institute of Directors cyber risk practice guide
  https://www.iod.org.nz/resources-and-insights/guides-and-resources/cyber-risk-practice-guide/#

- Privacy Commissioner information regarding privacy breaches
  https://www.privacy.org.nz/responsibilities/privacy-breaches/

- CertNZ
  https://www.cert.govt.nz/individuals/guides/get-started-cyber-security/

- PlanA Consulting
  www.planaconsulting.co.nz