HERBERT SMITH FREEHILLS

CYBER SECURITY IS A TEAM SPORT

Global
Legal Briefings

Tackling the ever-changing cyber security threat in an agile and proactive way requires influential members from the whole business to work together. Here is a selection of key questions by which you can assess your business's cyber-readiness.

BOARD AND C-SUITE

- What are our key information assets including IP and who is responsible to protect them?
- Do we know the reputational and financial impacts of a cyber security attack?
- Am I personally at risk?
- Can solutions be found that marry a desire for security with competiveness?
- How does our crisis response plan take information assets into account?
- How can we move from reacting to anticipating the threat?
- Are we considering cyber security when making investment decisions during mergers and acquisitions?
- Are we exposed further up or down the supply chain?
- How regularly do we review the cyber threat and update response plans?
- Have we created a culture where employees can raise issues before it is too late, and that those issues will be escalated appropriately within the business?

CIO AND IT PROFESSIONALS

- What systems do we need to operate?
- Which of those systems have the most business critical or sensitive information?
- What would motivate a cyber-attacker specifically to attack our business? Do we know who and why?
- How regularly do we review and test processes in line with the ever-changing technology and security climate?
- What is cyber security best practice for my industry and are we keeping pace of changing regulation?
- Are there any trends that make our information vulnerable at certain times?
- What cyber attacks has our business suffered so far?
- How affective has our response been to date?
- Are training programmes in place to address data protection and cyber risks faced by our employees?
- Who is represented in our incident response team? (Legal, HR, PR, IT, Risk, etc)
- Who is empowered to act and make the decisions needed in the event of a crisis; what's the chain of command?
- Do we have a review mechanism in place to determine the cause of the incident and learn from the experience?

GENERAL COUNSEL AND LEGAL PROFESSIONALS

- Do we know our regulatory and compliance obligations as they pertain to cyber security?
- Have these been adequately communicated to the other relevant stakeholders in the business?
- Do we have reporting processes in place to make appropriate regulatory notifications

and reports in the event of a cyber security incident?

- Who regularly tests our incident response plans and should a representative from legal be involved?
- How do we keep up to date and implement cyber security policies across multiple jurisdictions?
- Do we have appropriate policies and procedures in place for our employees describing acceptable and secure use of the organisation's information assets and systems?
- Are our policies and procedures formally acknowledged in employment terms and conditions?
- Are our stakeholders clear on how to interact with the media in the event of a crisis?
- What should happen if we suffer a breach through our supply chain?
- Have we adequately reviewed our inbound and outbound contracts in the context of cyber security risk?
- Are we adequately involved in assessing cyber security risk associated with any mergers, acquisitions or outsourcing arrangements?
- Do we have appropriate insurance in place to cover loss as a result of a cyber incident?
- How do we feedback the conclusions from an investigation into our policies and procedures and ensure that employees are given appropriate notice and training on them?

LEGAL NOTICE