Freshfields Bruckhaus Deringer

CYBER SECURITY CHECKLIST FOR BOARDS OF DIRECTORS

1. UNDERSTANDING CYBER SECURITY

Recognize that cyber security is a board room issue

Recognize that cyber security is an enterprise-wide – not just an IT – issue.

You have a duty to implement and monitor systems and controls related to cyber security

Allocate management responsibility for cyber risk and ensure that regular and adequate time is reserved on the board agenda to receive reports on cyber security issues

Consider appointing directors with specialist knowledge or forming a specialized committee focused on cyber security issues

Consider who your ideal crisis commander will be in the event of a breach, which may come down to professional duties, personality, and/or maintaining privilege. Identify what company assets might be vulnerable to a cyber security incident. Identify any third parties who might want to access the company's data improperly

Identify the potential impact of a cyber breach on the company, including on reputation and share price disclosure obligations, follow-on litigation, contractual liabilities, criminal/regulatory liability, and the business impact of a short or sustained disruption to key services

Recognize that there are a variety of regulatory regimes around the world and take a risk-driven approach to developing cyber security governance and compliance policies in key jurisdictions

2. PREVENTATIVE MEASURES/MINIMIZING THE RISK

Ensure that there are clear communication channels between the Chief Technology Officer or Chief Information Security Officer and the board

Implement a written information security policy (including HR/IT issues), with regular training for employees

Practice good cyber hygiene, by hardening baseline systems and protecting and maintaining those systems and company devices appropriately

Continuously monitor strategies and systems – do you have a clear and complete record of what types of data your organization holds (including third party data) and where? Is the data categorized clearly? Do you encrypt your data? Does any live in the Cloud? Is the data still needed? Who is responsible for these policies? Have you undertaken breach testing?

Ensure information and communications systems are configured securely and appropriately, and that networks are secure – consider whether your organization applies recognized information security standards (e.g. ISO 27001/27002 and/or the US NIST framework)

Manage the company's most important information appropriately – do you apply additional security measures (e.g. firewalls/restricted permissions, and non-technical e.g. employee vetting) for higher priority categories of data, such as business plans and customer information? Do you understand what you are legally obligated to protect?

Be aware and respond to employee risks posed by removable media and home and mobile working – does your computer use policy expressly permit your monitoring of employees? Do you limit the number of employees with access to sensitive data, and are they vetted? Do you have robust processes for reviewing and disabling employees' (and contractors') user accounts when they leave? Do you understand the privacy, civil liberties, and employment issues that may be in play?

Audit suppliers' cyber security policies/review supplier contracts to ensure that they are adequate – do they comply with industry standards and government guidance on information security? Do they otherwise generally protect confidential information? Is the supplier required to allow you to audit their policies/notify you of any breach? What is the liability cap/what are the exclusions for liability?

Be familiar with your key system/information security obligations under your contracts with customers and employees – what protections, including limits of liability, do you have for business interruption and/or data loss?

Consider whether a data breach could affect your key financing arrangements (reporting obligations) (for example, as a material adverse change)

Consider whether your annual reports, accounts, and regulatory disclosures include reporting on risk management regarding cyber security

Conduct adequate due diligence during M&A bids to ensure that you are fully aware of the cyber security history of the target company (its IT function, infrastructure, compliance, certifications, assets, technology) and are able to recognize and secure appropriate contractual protections for any potential liabilities and conduct necessary interviews, scans and penetration testing

3. PREPARING FOR A BREACH

Establish an appropriate and fluid incident response/crisis management plan – including, for example, procedures to contain and eradicate any breach, recover affected data, and identify responsible parties

Consider establishing an incident management team that reports to the board and is comprised of appropriate IT security, legal, compliance, physical security, HR, PR, and senior management resources and predetermine who will lead your crisis management team in the event of a breach. Identify appropriate external advisors (legal, IT, or otherwise) to assist with any necessary legal or technical (including forensic) assistance in the event of a breach

Take steps to ensure that appropriate document preservation systems are in place in the event of a cyber breach

Consider special protections for customers' personally identifiable information

Ensure that steps have been taken to ensure effective business continuity in the event of a breach

Ensure that there is an appropriate external communications strategy/a system to identify when external notification is necessary to regulatory authorities, customers, and other third parties, and to liaise with media

Share threat information (limited to technical details of the breach) after the event and as appropriate with other companies in the sector and across the economy

4. OTHER CONSIDERATIONS

Consider purchasing comprehensive cyber security insurance to cover hardware and data loss, business interruption, and costs relating to investigations and legal proceedings. Identify which risks to avoid, accept, mitigate or transfer through insurance as well as discrete plans associated with each approach

Be proactive, not reactive

*****

For further information, please contact:

Timothy P. Harkness,
Partner, New York
T +1 212 230 4610
E timothy.harkness@freshfields.com

Jane Jenkins,
Partner, London
T +44 20 78327280
E jane.jenkins@freshfields.com