42

CYBERSECURITY

Anjola Adeniyi

No matter where you are located in the world or what type of organisation you serve, cybersecurity is an increasingly complex area, and organisations need either to employ staff who have adequate skills and knowledge or, recognising that there is a global shortage of such skills, ensure that security staff acquire and maintain appropriate skills.

An organisation's board is responsible (and accountable to all its stakeholders) for the framework of standards, processes, and activities that, together, secure the organisation against cyber risk. All boards should be aware of the cyberthreat landscape and should understand what advanced persistent threats are.

Organisations need to develop cyber resilience, via a continuum of tested processes that enable an appropriate response to incidents of all sizes, including those which escalate and threaten the survival of the organisation itself.

The sections below cover the key topics and related questions to ask that are pertinent for directors to be mindful of.

Critical data and assets

Cyberattacks have the potential to be as destructive as major natural disasters. The board needs to have clarity on which of the organisation's data and assets are strategically critical. All assets don't deserve or need the same level of protection. While it would be good to be able to protect everything within security environments, often the truth is that resources needed to do so are out of reach for many companies – and strategic assets absolutely require the most attention.

- Has management defined and located its “crown jewels,” that is, critical assets (data and technology systems) which it needs to protect from a cyberattack?
- Where possible can you put a financial value on the data?
- Where do the crown jewels reside, and are they in more than one location? This can be relevant when considering who has access.
- Who has access to the crown jewels, and how are they accessed?
- What controls are in place for protecting the crown jewels, and how do we know they're effective?

Third-party relationships

Cybersecurity vulnerabilities within your third-party suppliers, and vendors, can put your organisation at risk. According to specialist research by the Ponemon Institute,¹ “37% of respondents do not believe their primary third-party vendor would notify them if it experienced a data breach involving sensitive and confidential information. Worse, 73% of respondents do not believe an Nth party vendor would notify them if they had a data breach.”

It is still common for organisations to have weak third-party cybersecurity management, with a low budget allocation.

- Does the organisation have appropriate policies, and processes in place for managing cybersecurity risks with partners and third-party suppliers?

1 Data Risk in the Third-Party Ecosystem by Ponemon Institute, 2016.

- Does the organisation ensure its partners and suppliers have appropriate policies, and processes across their partners and suppliers?

The board should ensure that third parties have similar arrangements with any downstream organisations being worked with. Data controllers must choose a data processor that provides sufficient guarantees about its security measures. The processor should undertake the same security measures that you would have to take if you were doing the processing yourself. Data controllers may have to audit and inspect the processor, either yourself or an authorised third party.

Awareness and training

The organisation should have a security awareness training programme, and all employees should take the training and test regularly. The training and awareness programme should be relevant to an individual's role such that those with higher-risk roles are given training and awareness at the appropriate level. Some individuals will handle customer data, another may handle sensitive commercial data, and finance functions may be vulnerable to social engineering and fraud, while others may just require general security awareness.

- Does the organisation educate its employees on their role in relation to cybersecurity?

Breach response

The organisation should plan, prepare, and rehearse for a successful cyberattack/data breach. Sample scenarios can be: what do you do if competitors access your IP/trade secrets/critical data? How do you reassure customers if their data is stolen? Everyone, including board members, should understand their roles and responsibilities in a response scenario, expectations from the regulators, law enforcement, customers, and other stakeholders.

It is very common for boards and executives to feel blindsided when a data breach occurs. Keeping abreast of all major cybersecurity incidents and data breach attempts can go a long way and as well as being aware of your

top cybersecurity risks. The definition of major will depend on the industry, and the organisation.

- Does the organisation have a robust incident response programme/ crisis management programme?
- Does the board keep track of its data breach attempts – successful/ unsuccessful?

Budget

- What percentage of the total revenue is the cybersecurity budget, and how does that compare to other companies – by industry, geography, size?
- What percentage of the IT budget is the cybersecurity budget, and how does that compare to other companies – by industry, geography, size?
- What other departments maintain a security budget, and how does that compare to other companies – by industry, geography, size?
- What's the percentage of security budget in those departments, and how does that compare to other companies – by industry, geography, size?

Security strategy

The board should set the parameters for selecting a security framework, and the framework should reflect how those parameters evolve. Below are some of the widely accepted industry frameworks:

- ISO27001 – focuses on legal, physical, and technical controls, and is often requested by customers who already use ISO in other aspects of their business.
- COBIT – a framework emphasising information governance and enterprise risk management.
- NIST – for US government agencies; however, it is used by the private sector and is probably the most mature security framework currently available.
- HIPAA – for the health-care industry
- PCI DSS – for payment data

The organisation may be going through digital transformation, expanding into new markets, or approaching a merger and acquisition. The security strategy should support your business initiatives, and their associated risks should be part of your security strategy.

- Does the organisation use a security framework?
- Does the cybersecurity strategy link with the business objectives?
- Does the organisation's cybersecurity programme account for internal and external threats?
- Does the organisation have a system in place for insider threats?
- Does the board discuss with the chief information security officer (CISO) their key cybersecurity issues, roadmap/strategy, current projects, budget?
- Does the board review the independently produced annual cybersecurity assessment?

Annual financial audits add credibility, promote transparency, and accuracy to the reported financial position and performance of a business. In the same sense, it is considered good practice to have regular independent cybersecurity assessment of an organisation. The annual cybersecurity assessment should cover all cybersecurity domains, identify vulnerabilities in the organisation's cybersecurity programme and, depending on the organisation, it should be from an independent source.

The board must require management to provide an independently produced annual cybersecurity assessment report, in a language accessible to the board. The cybersecurity assessment should evaluate: the security teams, IT and cyber governance, reporting relationships, security controls, security awareness training, and comparisons with the industry and organisations of similar sizes in other industries.

- Does the organisation understand the data privacy laws in all its geographies?

These laws can vary from one geography/jurisdiction to another, with details on the definition of a data breach, and reporting requirements also varying. General Data Protection Regulation requires companies and organisations to report a cyber breach or incident within 72 hours, and notify individuals and data protection authorities.

- How often does the board meet with the CISO?

The board should meet with the CISO, at least annually. Such meetings are an opportunity to understand key issues from the CISO's perspective – security issues, budget, political agendas, as well as discuss the security strategy. The board should set annual improvement expectations on various parameters, including incident response time and levels of compliance with the cybersecurity framework.

- Does the organisation have an established relationship with the appropriate authorities on cybersecurity?

The board should ensure that management has established relationships with the appropriate local and national authorities who are responsible for cybersecurity. Such bodies may include:

- National Cyber Security Centre
- Information Commissioner's Office
- Government Communications Headquarters
- Action Fraud
- National Crime Agency
- Scotland Yard
- Ministry of Defence
- Federal Bureau of Investigation
- Interpol

In some organisations a CISO may report through the chief information officer (CIO), which may create a conflict of interest where the CIO may be interested in operational performance or cost-cutting. Also, having the CISO reporting via the Legal, chief risk officer (CRO), or chief financial officer (CFO) may divorce the CISO from the IT areas. In an ideal scenario, the CISO should have independence with access to the board. It's important the CISO works with the CRO, CIO, chief operating officer (COO), chief privacy officer, chief digital officer, head of businesses and various functional leads. The CISO's reporting line should be considered on the industry and the organisation's dependency on technology. Typically, the higher one is in an organisational hierarchy, the greater influence one has on implementing policies and culture change.

Is the CISO reporting at the appropriate level within the organisation, and how does this compare with the industry and the organisation's dependency on technology – via the CIO, general counsel, COO, CRO, CFO, chief executive officer?

Risk

- Does the board meet with the CRO, at least annually, to discuss how the cyber risks are treated? As part of the day-to-day running of the organisation, management may accept risks which the board may be unaware of.
- Does the board verify the cyber insurance coverage is sufficient to address potential cyber risks?

The board must ensure the cyber insurance policy is sufficient to address the potential cyber risks, by asking management to understand the potential impact of a data breach. The global average cost of a data breach per record is \$144, the UK Average is \$123, and the UK average cost per data breach incident is \$3.10M.²

- Is the board aware of the organisation's top five risks in relation to cybersecurity?

The board should require management to provide information on the threats, actors, and their possible methods as well as the major breaches that have happened in the market/industry, and how their defences compare.

- How do you compare with your industry peers?
- Does the board monitor annually whether the enterprise risks relating to cybersecurity are improving or not? The board must monitor enterprise risks related to cybersecurity if they are improving or not from year to year and set expectations for them.

2 According to *Cost of a Data Breach* report by Ponemon Institute 2017.

Skills and leadership

Board directors are required to apply the constructive challenge to cybersecurity matters as they do to board discussions on strategy and performance. The board may want to consider additional directors who can bring in cybersecurity skills where needed. The current skills gap in cybersecurity may hinder this, and there are schools of thought against directors with a single functional skillset. Where possible, a board may benefit from a cybersecurity leader who has strong business acumen and can fulfil the role of a non-executive director whilst having a strong cybersecurity skill level. Other options include having access to independent cybersecurity consultants, and director-level training on cybersecurity.

- Does the board have members with a technology or cybersecurity skill?