EST 2016

BLACKSMITHS

FORGING INTELLIGENT SECURITY

Cyber Security Questions

At a recent presentation to BCKR by Blacksmiths Group, we provided a list of questions about security controls that Non-Executive Directors (NEDs) may find useful to ask in their future roles. These are reproduced below, with some explanatory notes.

Question 1: **How many serious security incidents were there in the last year and what was learned from them?**

Who to ask: The CEO or Board colleagues. The Board Secretary should be able to pull out the relevant papers, depending on what the answer is!

What to look for: Security incidents should be recorded and classified according to their severity. You should expect to see management information (MI) about numbers, trends and patterns of incidents on a fairly regular basis, but individual high impact incidents should be brought directly to the attention of the Board. The key role of the Board is to ensure that security incidents are reviewed, and that lessons are genuinely learned rather than just identified. In practice, this means ensuring that decisions are taken about actions required to avoid the occurrence of a similar event in the future. When you have been involved in managing a security incident, you should make a point of asking three months later what conclusions were drawn, and what actions have been taken.

Question 2: Is security mentioned in the company values?

Who to ask: Company values should be available online, but the Board Secretary should be able to supply the associated strategy documents.

What to look for: Company values should ideally include a statement on the importance of working safely and securely, as this provides a valuable hook for other security messaging. You should ask whether there is a company security strategy available to all employees, and whether it is introduced by the CEO. You should look for signs of visible commitment to security from Board members. This is important because it sets a strong example to all staff when the leadership is seen to walk the talk. If there is a rule about wearing passes, check whether the CEO is wearing one!

Question 3: How does the corporate risk process work and does security appear on the Board risk register?

Who to ask: The CEO or Board colleagues or, if there is one, the Chief Risk Officer. The Board Secretary should be able to provide the relevant documents.

What to look for: Your organisation may well have a Chief Risk Officer. Risk processes can be complex and cover all sorts of areas, from poor sales to inadequate resource and capability. But is there a process that relates to security? Do you know how it feeds up from the operational level and who reviews it? Critically, can the Board rely on it to tell them when they need to take action?

Question 4: What is the Board's risk appetite?

Who to ask: The CEO and Board colleagues. The Board Secretary should be able to provide the relevant papers.

What to look for: Encourage the Board to identify clearly what its critical assets are, and what threatens those assets most. Find out what threat information the Board receives. Does it include information from inside as well as outside the organisation, such as responses to phishing exercises or organisational stress levels? Has the Board examined the impact and likelihood of the company's key security risks materialising? Has it given a clear steer to the organisation about its risk appetite, based on a sound understanding of the controls available to it? Is its communication on risk appetite sufficiently clear to enable delivery teams to make decisions about deploying and investing in controls? How often and in what circumstances is the Board's risk appetite reviewed?

Question 5: Who is accountable for security risks?

Who to ask: The CEO

What to look for: Try to establish who in the leadership team is answerable if there is a security incident. Who is accountable to that person for physical, personnel and cyber security risk? You should be looking for named directors here. If everyone accountable has 'security' in their title, the company probably has a problem. The HR Director is generally best placed to own insider risk and the Chief Information Officer to own cyber risk. Physical risk will usually be owned by Estates or Facilities Management.

Question 6: What information assurance management system is used, and can I see the last review report?

Who to ask: The Chief Information Officer

What to look for: The company is likely to be using an information security standard such as ISO27001 or NIST. If there is no such framework in place, it is a cause for concern. Even if there is, look at the last return and make sure you understand what lies behind the scoring and whether it chimes with your own experience of the organisation. In companies where information assurance processes are undertaken with little or no involvement from leadership, they are liable to become a tick box exercise. Some leaders have been known to express the view that 'as long as I have a defensible position (a certificate) I can't be blamed if something happens'. This is both reckless and unrealistic.

Question 7: Can I see the information asset register?

Who to ask: The Chief Information Officer

What to look for: This can feel like boring administration work, but it is vital. The Board should be accountable for the existence and quality of the Information Asset Register. If there is no up to date record of what information is held, why and how long for, and if there is no statement of how critical the information is and who owns it, then the rules for protecting that information cannot be relied upon. The absence of a proper information records is a strong indicator that the company is at risk of breaching GDPR rules on personal data.

Question 8: Can I see a comprehensive record of our supply chain?

Who to ask: The Chief Commercial Officer, or Finance Director if there isn't one

What to look for: Depending on the company, supply chains can be huge and complex. A proper record is important for understanding business dependencies and resilience, but in a security context it is important to establish clearly which external parties have access to your assets. As a follow up, you should seek assurance that these parties are properly assessed and held accountable for their own security.

Questions 9: How much was spent on security as a percentage of turnover last year?

Who to ask: The Finance Director

What to look for: You should ask how the company spend on security compares with others in the sector. It is an encouraging sign if security spend is being tracked; it is common to find it getting lost in Facilities Management or IT spend. Find out how the figures are reached and what they include. And bear in mind that not all controls which are important to security have a 'security' label. For example, strong welfare support and clear rules about information management are equally important.

Question 10: When were security controls last reviewed by the Audit Committee?

Who to ask: The Chair of the Audit Committee and the Chief Information Officer

What to look for: You should check whether security appears as a regular item on the Audit Committee workplan. What was concluded at the last review, and how many recommendations remain unresolved? Independent assurance is really important. There are a range of ways of testing whether controls are fit for purpose. You can hire companies like Blacksmiths, and we have developed a systematic method for doing this. Alternatively, there are companies who specialise in trying to breach company defences (so-called red-teaming or penetration testing), something which Blacksmiths also offers. The Data Protection Officer is required to independently assure personal data, but not all your critical information may fall into that category. It is important therefore that independent assurance is conducted across all aspects of information management and security.

Contact Details

malcolm@blacksmithsgroup.com

susanna@blacksmithsgroup.com

josh@blacksmithsgroup.com

60 St. George’s Place, Formal House, Cheltenham GL50 3PN, United Kingdom
info@blacksmithsgroup.com | +44 20 3880 2282 | www.blacksmithsgroup.com
Registered No: 09875845 | VAT No: 231039057