Toolkit B

Questions for the Board to Ask Management About Cybersecurity

Of all the cybersecurity risk issues for an organisation to worry about, perhaps the greatest challenge is mitigating the insider threat. The cyber insider threat encompasses employers, contractors, vendors, and others who have legitimate access to the network, systems, and/or data of the organisation to some degree. Verizon's Data Breach Report identified five types of cyber insider threats[82]:

- **Careless Workers:** Employees or partners who non-maliciously misappropriate resources, break acceptable use policies, mishandle data, install unauthorized applications or use unapproved workarounds.
- **Inside Agents:** Insiders recruited, solicited, or bribed by external parties to exfiltrate data.
- **Disgruntled Employees:** Insiders recruited, solicited, or bribed by external parties to exfiltrate data.
- **Malicious Insiders:** Actors with access to corporate assets who use existing privileges to access information for personal gain.
- **Feckless Third Parties:** Business partners who compromise security through negligence, misuse, or malicious access to or use of an asset.

Case Study:
Insurance Company Insider Steals Customer Data

In 2017, an employee of a private global health insurance company accessed the firm's customer database to steal the personal data of more than 500,000 people. The information included customers' names, birthdays, email addresses and nationalities. The company insider later tried to sell the information on the dark web.

The U.K. Information Commissioner's Office fined the company £175,000 for failing to implement adequate security measures to protect customers' information. "[The company] failed to recognize that people's personal data was at risk and failed to take reasonable steps to secure it," said ICO Director of Investigations Steve Eckersley.

[82] Verizon Insider Threat Report, "Out of sight should never be out of mind," undated but released in 2019, p. 5

This toolkit will help boards of directors ask senior management the right questions to ensure that these wide-ranging cyber insider threats are being properly mitigated.

Questions Boards Should Ask Senior Management on Insider Threats

Strategy and Comprehensive Risk Assessment

1. What are the frameworks we align to, and has the organisation completed a gap analysis?
2. Do we have a systematic framework or ISO in place to address cybersecurity and to assure adequate cybersecurity risk management?
3. What are our critical business services and processes? How do they map to legal entities, regulators' perspectives, IT departments, and suppliers?
4. What is important to protect, and how many times have we seen these assets compromised?
5. Do we have appropriately differentiated strategies for general cybersecurity and for protecting our mission-critical assets?
6. Have we prioritised the company's cybersecurity risks, and identified the strategy to manage these risks?
    a. Do we have a list of most critical IT systems and an inventory of all IT systems?
    b. Have we identified our more likely adversaries and cyber threats, both internally and externally?
    c. Have we considered all aspects of connectivity with the external environment?
7. In management's opinion, what are the most serious vulnerabilities related to cybersecurity (including within our IT and technology systems, personnel, or processes)?
8. Have we considered obtaining an independent, third-party assessment of our cybersecurity risk management programme?

Risk Strategy and Business Evolution

1. What kind of business strategy decisions have an impact on cyber risk?
2. What is our insurance coverage for cyber? Is it adequate and what kind do we have? Why do we have that sort of insurance?
3. What is our strategy to address cloud, BYOD, and supply-chain threats?
4. How are we addressing the security vulnerabilities presented by an increasingly mobile workforce?
5. Are we growing organically or buying companies? Are they mature companies or start-ups? Where are we geographically?

Organisation

1. Do we have an enterprise-wide, independently budgeted **cyber-risk management team**? Is the budget adequate? How is it integrated with the overall enterprise risk management process?
2. How is the cyber-risk management team composed? Have all appropriate functions been considered? For example
   i. Steering committee composed of a range of management members with
   ii. Information security function
   iii. Physical security function
   iv. Information technology
   v. Legal
   vi. Compliance
   vii. Operations
   viii. Shared services
   ix. Business units

To initiate a dialogue about cyber risk governance in your organization, consider the following:

- Leverage opportunities to gain bottom up support/cooperation from 1st and 2nd lines of defence
- A strong champion is critical- it could be the CISO, CSO, CRO or another influential leader
- It also helps to have a top down support /mandate from the Board/top management
- Start small- invite other leaders to existing steering committee/governance/key project meetings and look for ways to help each other meet objectives

Source: Ferma- At the Junction of Corporate Governane & Cybersecurity 2019

3. How effective is the cyber risk management team, including the information-security team, in collaborating between departments and corporate functions on cybersecurity-related matters? For example, as regards:

   - Business development regarding due diligence on acquisition targets and partnership agreements;
   - Internal audit regarding the evaluation and testing of control systems and policies;
   - Human resources on employee training and access protocols;
   - Purchasing and supply chain regarding cybersecurity protocols with vendors, customers, and suppliers; and/or
   - Legal regarding compliance with regulatory and reporting standards related to cybersecurity as well as data privacy?

4. Does the cyber risk management team have the necessary skills? Do they receive continuing professional education?
5. What role does each member of the cyber risk management play in the organisation's enterprise risk management (ERM) structure and in the implementation of ERM processes?
6. How is the risk ownership decided?
7. What support does the cyber risk management team receive from the CEO, CIO, and senior management team?
8. How is the organisation's cybersecurity budget determined? Comparing this figure with industry spending trends is probably the best way to gain context over the adequacy of funding. What is its size (e.g., percentage of total IT/Technology spending), and how does this figure compare with leading practice in our industry and generally? What role does the security team play in cybersecurity budget allocation and investment decisions? Which security tools or other investments were below the "cut" line in the budget?

With particular regard to the information security function:

9. What is the information security function's scope of authority in terms of resources, decisions, rights, budget, staffing and access to information? How does this compare to leading practice in our industry and generally?[83]
10. What is the information security function's administrative reporting relationship (e.g., CIO, CISO, CTO, COO, Head of Corporate Security, other)? Does it differ from the functional reporting relationship?
11. What protocols are in place to ensure that the information security function has an independent channel to escalate issues and to provide prompt and full disclosure of cybersecurity deficiencies?[84]
12. What role, if any, does the cyber risk management team and the information security function play beyond setting and enforcing cybersecurity policies and related control systems?
    - For example, does the information security team provide input on the development process for new products, services, and systems or on the design of partnership and alliance agreements, etc., such that cybersecurity is "built in" rather than "added on" after the fact?
13. What are the arrangements in place to be able to scale up the information security function, in case of a crisis? Do we have the right relationships with suitable third parties?
14. How is the information security team's performance evaluated? Who performs these evaluations, and what metrics are used?
15. How does the information security team develop and maintain knowledge of the organisation's strategic objectives, business model, and operating activities?
    - For example, in companies that are actively pursuing a "big-data" strategy to improve customer and product analytics, to what extent does the security team understand the strategy and contribute to its secure execution?
16. Where do management and our cyber risk management team teams disagree on cybersecurity?

Prevention measures and Operations

1. How do our operational controls, including access restrictions, encryption, data backups, monitoring of network traffic, etc., help protect against insider threats?
2. How have we adapted our personnel policies, such as background checks, new employee orientation, training related to department/role changes, employee exits, and the like, to incorporate cybersecurity?
3. Do we have an insider-incident activity plan that spells out how and when to contact counsel, law enforcement and/or other authorities, and explore legal remedies?
4. Do we have forensic investigation capabilities?
5. What are the leading practices for combating insider threats, and how do ours differ?

[83] See, for example, Marc van Zadelhoff, Kristin Lovejoy, and David Jarvis, *Fortifying for the Future: Insights from the 2014 IBM Chief Information Security Officer Assessment* (Armonk, NY: IBM Center for Applied Insights, 2014).

[84] A 2014 study of global information security issues found that organizations with CISOs reporting outside the CIO's office have less downtime and lower financial losses related to cybersecurity incidents as compared with those who report directly to the CIO. See Bob Bragdon, "Maybe it really does matter who the CISO reports to," *The Business Side of Security* (blog), June 20, 2014.

6. How do key functions (IT, HR, Legal, and Compliance) work together and with business units to establish a culture of cyber-risk awareness and personal responsibility for cybersecurity? Considerations include the following:
    a. Written policies which cover data, systems, and mobile devices should be required and should cover all employees.
    b. Establishment of a safe environment for reporting cyber incidents (including self-reporting of accidental issues).
    c. Regular training on how to implement company cybersecurity policies and recognise threats.
7. What are we trying to prevent by protecting against insider threats?

Prevention measures - Supply-Chain/Third-Party Risks

1. What do we currently do and what will need to be done to fully include cybersecurity in our current supply-chain risk management?
2. How much do we know about our supply chain regarding cyber-risk exposure and controls? What due diligence processes do we use to evaluate the adequacy of our suppliers' cybersecurity practices (both during the on-boarding process and during the lifetime of each contract)? Which departments/business units are involved? Are there appropriate contingency arrangements in place in the event of a major problem with critical third-party suppliers?
3. Does the business carry out appropriate strategic monitoring of third-party suppliers?
4. What providers do we use for the cloud? Which critical business functions have we outsourced to third parties, such as cloud security?
5. How do we balance the financial opportunities (lower costs, higher efficiency, etc.) created by greater supply-chain flexibility with potentially higher cyber risks?
6. How are cybersecurity requirements built into vendor agreements? How are they monitored, and are we doing our due diligence to enforce contracts? Contracts can be written to include minimum cybersecurity requirements, including for example:
    a. Written cybersecurity policies.
    b. Personnel policies, such as background checks, training, etc.
    c. Access controls.
    d. Encryption, backup, and recovery policies.
    e. Detailed requirements regarding data held by the third party.
        i. Retention and deletion requirements for data held.
        ii. Clear inventories of types of data held.
        iii. Clarity on what is stored, moved, processed, etc.
    f. Secondary access to data.
    g. Countries where data will be stored.
    h. Notification of data breaches or other cyber incidents.
    i. Communication plans for incident reporting and response.
    j. Incident-response plans.
    k. Audits of cybersecurity practices and/or regular certifications of compliance.
7. Do we allow our suppliers to subcontract the delivery of any part of the contract? If so, what level of control/scrutiny do we exercise over the subcontracting arrangements? How do we monitor changes to subcontracting arrangements through the lifetime of the contract?

8. Do we have technology in place to profile suppliers and partners from the cybersecurity point of view to identify potential vulnerabilities and actively manage third party risk?
9. Are we indemnified against security incidents in our supply chain? What is the financial strength of the indemnification?
10. How difficult/costly will it be to establish and maintain a viable cyber-vulnerability and penetration-testing system for our supply chain?
11. How difficult/costly will it be to enhance monitoring of access points in the supplier networks?
12. Do our vendor agreements bring incremental legal risks or generate additional compliance requirements (e.g., GDPR, etc.)?

Response capability-Planning for a Potential Incident, Crisis Management and Response

1. Are we members of information sharing communities? If so, what are the lessons learned from our peers who have experienced breaches
2. How capable is management in "threat intelligence" by always updating its full knowledge of threats and adversaries, given the wide range of sources:
    - Phishing
    - Malware
    - External cyberattacks to disrupt, to expropriate funds, to steal IP
    - Internal attacks to disrupt, to expropriate funds, to steal IP
    - Fraud
    - Spam
    - Natural disasters
    - Espionage
3. When was the last time we conducted a penetration test or an independent external assessment of our cyber defences? What were the key findings, and how are we addressing them? What is our maturity level?
4. Were we told of cyber-attacks that have already occurred and how severe they were?
5. What is our ability to protect, detect and respond to incidents? How does it compare with others in our sector?
6. In the context of our business, has a material cybersecurity breach been defined to ensure proper escalation?
7. At what point is the board informed of an incident? What are the criteria for reporting?
8. What is known about the intent and capability of the attacker? What do we know about how the attacker might use the data?
9. Does our organisation have an appropriate methodology in place for assessing the risk in case of an incident and determining whether any notifications are legally required?
10. Are we clear as to who must be notified and when? What are the timetables and strategy considerations for reporting incidents to customers? Regulators/relevant government entities? Law Enforcement? Vendors/partners? Internally? Peers? Investors? What timetables are mandated by laws and regulations and what is at the company's discretion?
11. How will management respond to a cyberattack? Does the company have a validated incident-response plan?[85] Are we adequately exercising our cyber-preparedness and response plan?

[85] Ibid.

12. Do we have a crisis management plan in place? For significant breaches, how good is our communication plan (both internally and externally) as information is obtained regarding the nature and type of breach, the data impacted, and the ramifications to the company and the response plan?[86]
13. What are we doing to avoid making the problem worse for our organisation? How do we ensure we have appropriate legal advice in the incident and crisis management teams? Are the legal teams integrated in the incident and crisis plans?
14. What external communication strategies have been developed to manage reputational risk during the incident?

Recovery capability- After a Cybersecurity Incident

1. How did we learn about the incident? Were we notified by a third party, or was the incident discovered internally?
2. What do we believe was the motive for the incident? What was the impact, and how do we measure it? Have any of our operations been compromised?
3. Is our cyber-incident/crisis response plan in action, and is it working as planned?
4. What is the response team doing to ensure that the incident is under control and that the attacker no longer has access to our internal network?
5. What were the weaknesses in our system that allowed the incident to occur and why had they not been identified or remediated?
6. Has the security team checked for associated vulnerabilities across all company systems/networks, not just the affected systems or services? Have they checked what happened against the controls framework and made the necessary changes to both security controls and business controls?
7. What steps can we take to make sure this type of event does not happen again? How do we ensure that lessons are learned and remediation actions tracked?
8. What can we do to mitigate any losses caused by the incident?
9. Does the incident alter the risk tolerance of the business? Has this been discussed and have any changes been captured?
10. What external communication strategies have been developed to manage reputational risk after the incident?

Monitoring

1. What cybersecurity performance measures and milestones have been established for the organisation as a whole?
2. If we answer to regulatory authorities, can we be subject to a regulatory audit?
3. Does our external auditor indicate we have cybersecurity-related deficiencies in the company's internal controls over financial reporting? If so, what are they, and what are we doing to remedy these deficiencies

Adapted from NACD, et al., *Cybersecurity: Boardroom Implications* (Washington, DC: NACD, 2014) (an NACD white paper).

[86] StaySafeOnline.org, the National Cyber Security Alliance, and Business Executives for National Security, "Board Oversight."