# Toolkit A

## Possible points to include in Board Review & Self-Assessment regarding "Cyber Literacy" and Cybersecurity Culture[76]

Even prior to a Board meeting, directors may do well to self-assess if they have considered various aspects of cybersecurity beyond the technical and operational aspects. In particular, boards should be thinking of cybersecurity in business terms, and considering if they are preparing their organisation on a strategic level. Among the questions, directors may want to ask are the following:

1. Does the CEO encourage open access between and among the Board, external sources, and management about emerging cyber threats?
2. Are we considering the cybersecurity aspects of our major business decisions, such as M&A, partnerships, new product launches, etc., in a timely fashion?
3. Do we know the maturity scale of our cyber risk programme?
4. Are we spending appropriately on cybersecurity tools and training? Do we know if our spending is cost effective? Are we actually improving security or just completing compliance requirements?
5. Who is managing our cybersecurity? Do we have the right talent and clear lines of accountability/communication for cybersecurity?
6. Have we considered how we would manage our communications in the case of a cyber event, including communicating with the public, our shareholders, our regulators, our rating agencies? Do we have segmented strategies for each of these audiences?
7. Does our organisation participate in any of the public or private sector ecosystem-wide cybersecurity and information-sharing organisations?
8. Is the organisation adequately monitoring current and potential cybersecurity-related legislation and regulation?[77]
9. Does the company have adequate insurance, including Directors and Officers, that covers cyber events? What exactly is covered?[78] Are there benefits beyond risk transfer to carrying cyber insurance?[79]

This toolkit will help directors identify what questions to ask senior management and also provides a numerical scale to assess the board's culture[80]. See also PwC publication on "How can Boards better oversee Cyber risk" which includes an appendix with relevant questions for the Board to ask[81]

Directors wishing to incorporate a cybersecurity component into their board's self-assessment can use the questions in the table below as a starting point.

---

[76] National Association of Corporate Directors, 2018-2019 NACD Public Company Governance Survey, p. 17. The *NACD 2018-2019 Public Company Governance Survey* found that, "More than half of directors, 52 percent, are now confident that they personally have the understanding to provide effective cyber risk oversight, and 58 percent "believe their boards collectively know enough about cyber risk to provide effective oversight."

[77] Ibid.

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

[79] Ibid.

[80] Report of the NACD Blue Ribbon Commission on Board Evaluations: Improving Director Effectiveness (Washington, DC; NACD, 2010), p.7. NACD has defined boardroom culture as "the shared values that underlie and drive board communications, interactions, and decision making. It is the essence of how things really get done."

[81] www.pwc.com/us/en/services/governance-insights-center/library/risk-oversight-series/overseeing-cyber-risk.html

| Use the numerical scale to indicate where the Board's culture generally falls on the spectrum shown below. <----------> | | | Action Item |
|---|---|---|---|
| We classify cyber risk as an IT or technology risk | 1 2 3 4 5<br>☐ ☐ ☐ ☐ ☐ | We classify risk as an enterprise wide risk | |
| Our cybersecurity discussions with management focus primarily on reviews of past events (e.g. historical breach data) | 1 2 3 4 5<br>☐ ☐ ☐ ☐ ☐ | Cybersecurity is incorporated into forward-looking discussions with management (e.g. new product/service development, M&A/joint ventures, market entry) | |
| Our Board relies on management to assess critical assets, major threats, and overall risk assessment | 1 2 3 4 5<br>☐ ☐ ☐ ☐ ☐ | Our Board has participated in a strategic risk assessment critical assets, major threats, and overall risk assessment, in order to promote an enterprise – wide risk management strategy | |
| The board receives information about cybersecurity exclusively from management | 1 2 3 4 5<br>☐ ☐ ☐ ☐ ☐ | The board receives first-hand information about cybersecurity from non-management sources | |
| Information about emerging cyber threats or potential issues is filtered through the CEO | 1 2 3 4 5<br>☐ ☐ ☐ ☐ ☐ | The CEO encourages open access and communications between and among the board, external sources and management about emerging cyber threats | |
| Our Board does not expect management to uniquely assess and manage cyber risks. | 1 2 3 4 5<br>☐ ☐ ☐ ☐ ☐ | Our Board expects management to provide it with a clear analysis of what our cyber risks are, which to accept, what we can mitigate, and what we can transfer consistent with our business goals | |
| Our Board is not supported by a Committee with sufficient knowledge of cyber risk management | 1 2 3 4 5<br>☐ ☐ ☐ ☐ ☐ | Our Board is sufficiently supported by a Committee with sufficient knowledge of cyber risk management | |

## Questions Directors Can Ask to Assess the Board's Cyber Literacy

1. What do we consider our most valuable assets? How does our IT system interact with those assets? What would it take to feel confident that those assets were protected?

2. Are we considering the cybersecurity aspects of our major business decisions, such as M&A, partnerships, new product launches, etc., in a timely fashion?

3. Who is in charge? Do we have the right talent and clear lines of accountability/responsibility for cybersecurity?

4. Does our organisation participate in any of the public or private sector ecosystem-wide cybersecurity and information-sharing organisations?

5. Is the organisation adequately monitoring current and potential cybersecurity-related legislation and regulation? Does the company have insurance that covers cyber events, and what exactly is covered? Is there Director and Officer exposure if we don't carry adequate insurance? What are the benefits beyond risk transfer of carrying cyber insurance?

## Case Studies

### Lax Security Culture Allowed North Korean Hackers to Penetrate a Multinational Corporation and Entertainment Industry Leader

In 2014, a multinational entertainment industry corporation reported a "brazen attack" on the company. Hackers penetrated the company's information systems, stole data, and leaked sensitive information online, including copies of unreleased films and embarrassing emails. The attackers also used malware to erase assets within the company's information systems. The U.S. government blamed the North Korean government for the attack.

At the time, former employees stated that the company's lax security practices contributed to the attack. One former employee called the company's information security team "a complete joke." The employee added: "We'd report security violations to them and our repeated reports were ignored." Another former employee explained. "The real problem lies in the fact that there was no real investment in or real understanding of what information security is."

### The U.K. National Health Service and the WannaCry Attack

On 12 May 2017, hundreds of thousands of computers around the world were victimized by the WannaCry Ransomware Attack. In the United Kingdom, the National Health Service (NHS) suffered significant disruptions—including 19,000 health appointments canceled. The attack cost the NHS an estimated £92 million; 139 of the appointments involved potential cancer referrals.
These disruptions and losses would have been avoidable, if the NHS had a stronger cybersecurity culture as an organization. Investigators later determined that the NHS was using old operating systems, including Windows XP, with known vulnerabilities.

The National Audit Office (NAO) evaluated the incident and reported that the Department of Health was warned about the risk of a cyber attack on the NHS a year earlier. "The WannaCry cyber attack had potentially serious implications for the NHS and its ability to provide care to patients," NAO head Amyyas Morse commented. "It was a relatively unsophisticated attack and could have been prevented by the NHS following basic IT security best practices."

The National Audit Office concluded: the Department and NHS national bodies need to, "ensure that organisations, boards, and their staffs are taking the cyber threat seriously, understand the direct risks to front-line services, and are working proactively to maximize their resilience and minimize impacts on patient care."

*Sources*: Matthew Field, "WannaCry cyber attack cost the NHS £92m as 19,000 appointments canceled," *The Telegraph*, 11 October 2018; National Audit Office, "Investigation: WannaCry cyber attack and the NHS," October 17, 2017.

## Case Study: International Banking System Exhibits Strong Leadership in Response to Breach

In 2016, an Asian bank experienced a major cyber attack, resulting in millions of dollars being transferred through the international SWIFT banking network. Although the SWIFT network was not compromised through this breach, SWIFT leadership proactively took action to preserve its reputation and delivered a message to all its clients that weaknesses in their systems would no longer be tolerated. SWIFT also created the Customer Security Programme following this incident. This programme led to the establishment of a customer security control framework providing a variety of mandatory and suggested criteria for SWIFT clients. This framework established a security baseline for all of the 11,000 banking institutions that use SWIFT. As a result of this programme, by 2018, 94% of SWIFT clients had attested to their compliance with the framework.

Source: www.centralbanking.com/fintech/4397726/cyber-security-provider-swift