A JOURNAL ON CORPORATE GOVERNANCE & LEADERSHIP

issue 11

CYBER RISK AND THE BOARD — HOW DIRECTORS CAN STAY AHEAD

Fadi Mutlak
Partner, Deloitte

The digital economy is in full-flight: Disruptive technologies have created unprecedented opportunities for businesses. But it is those same opportunities, that also pose a threat.

The world economic forum, in their recently published Global Risks Report 2018, identify cyberattacks as the top technological risk alongside, environmental, societal, economic and geo-political;[1]

And while many organizations now recognize that cyber risk is a top business risk, despite the heightened attention the number of cyber incidents and their associated costs continues to rise.

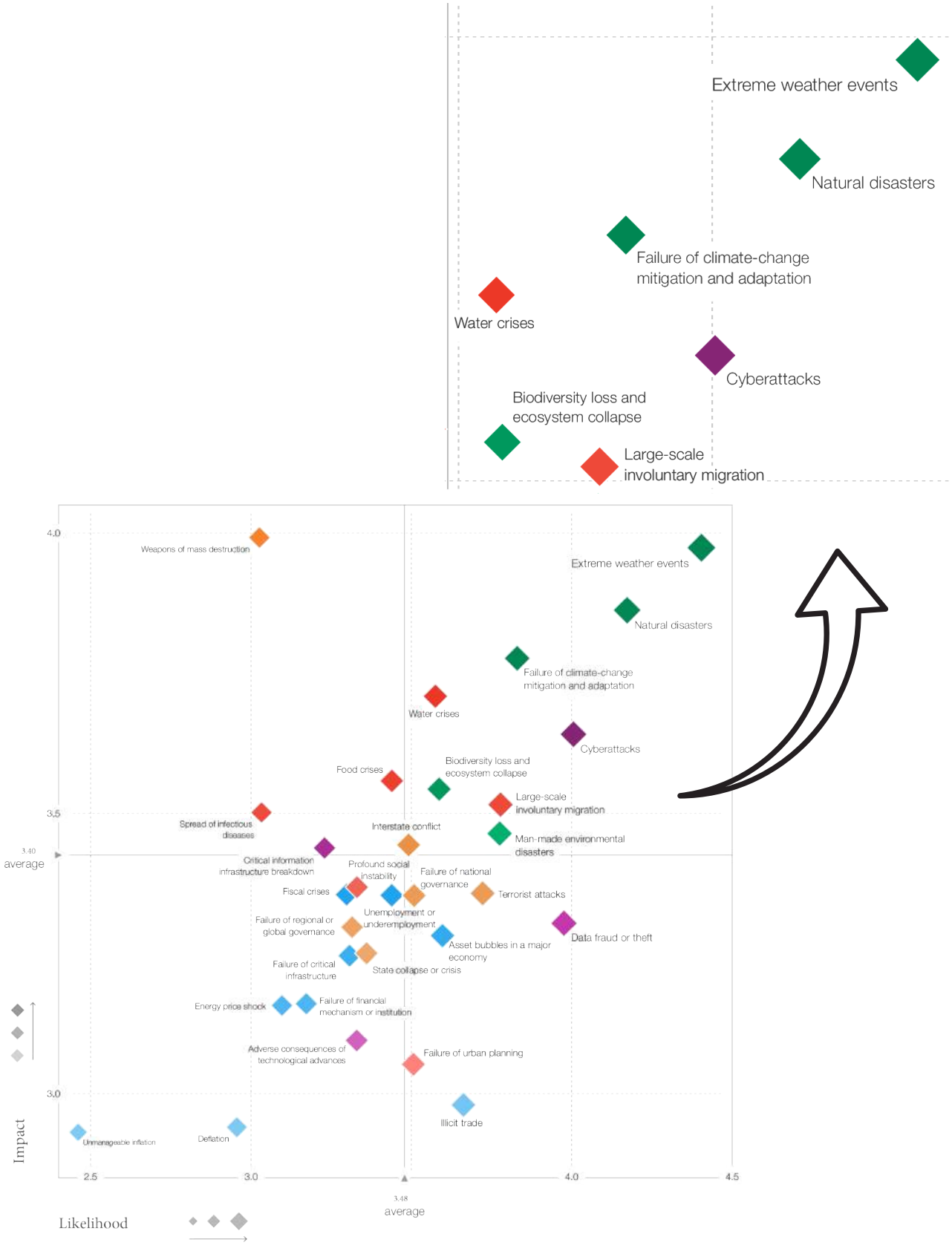
In that regard, 2017 was a particularly challenging year: with a series of attacks that Mcafee estimates cost the global economy as much as $600 billion in 2017[2]. Some of those most damaging attacks included[3] ;

[1] http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

[2] https://www.mcafee.com/us/solutions/lp/economics-cybercrime.html

[3] http://money.cnn.com/2017/12/18/technology/biggest-cyberattacks-of-the-year/index.html

Figure 1: The Global Risk Landscape 2018



• **April 2017**, an anonymous group called the Shadow Brokers leaked a suite of hacking tools widely believed to belong to a government security agency. The tools allowed hackers to compromise a variety of Windows servers and Windows operating systems, including Windows 7 and Windows 8.

• **May 2017**, WannaCry, which spanned more than 150 countries, leveraged some of the leaked NSA tools. In May, the ransomware targeted businesses running outdated Windows software and locked down computer systems. The hackers behind WannaCry demanded money to unlock files. More than 300,000 machines were hit across numerous industries, including health care and car companies.

• **June 2017**, the computer virus NotPetya targeted Ukrainian businesses using compromised tax software. The malware spread to major global businesses. This virus also spread by leveraging a vulnerability leaked by the Shadow Brokers. In September, FedEx attributed a $300 million loss to the attack. The company's subsidiary TNT Express had to suspend business.

• **July 2017**, a large credit bureau was penetrated by cybercriminals in July and stole the personal data of 145 million people. It was considered among the worst breaches of all time because of the amount of sensitive information exposed, including Social Security numbers.

The Middle East has been no exception, to these highly sophisticated attacks, including:

• **Jan 2017**, Saudi state-run TV reported that 15 government agencies and organizations had been hit with Shamoon 2 wiping data and taking control of the computer's boot record, which prevented the PC from being turned back on.[4]

• **August 2017**, Malicious software attacked a safety system at a petrochemicals company, in what was the first-ever example of malware targeting the computer systems designed to prevent a disaster at an industrial facility.[5]

However, despite the increased recognition that cyber risk is a top business risk and a 7.8% year-over-year increase in average spend on cyber security[6], why are organizations still struggling to manage cyber risk?

Cyber Security Governance

An effective cyber security program should be overseen by the board of directors as part of its oversight of the organization's risk management activities. As with other risk programs, the board should set its expectations and accountability for management and ensure there are adequate resources, funding and focus for its cyber security activities.

A recent survey conducted by Deloitte's Center for Board Effectiveness and the Society for Corporate Governance (Society) examines the[7] current practices of boards related to cyber security and also offers some insight into the current challenges related to cyber security governance:

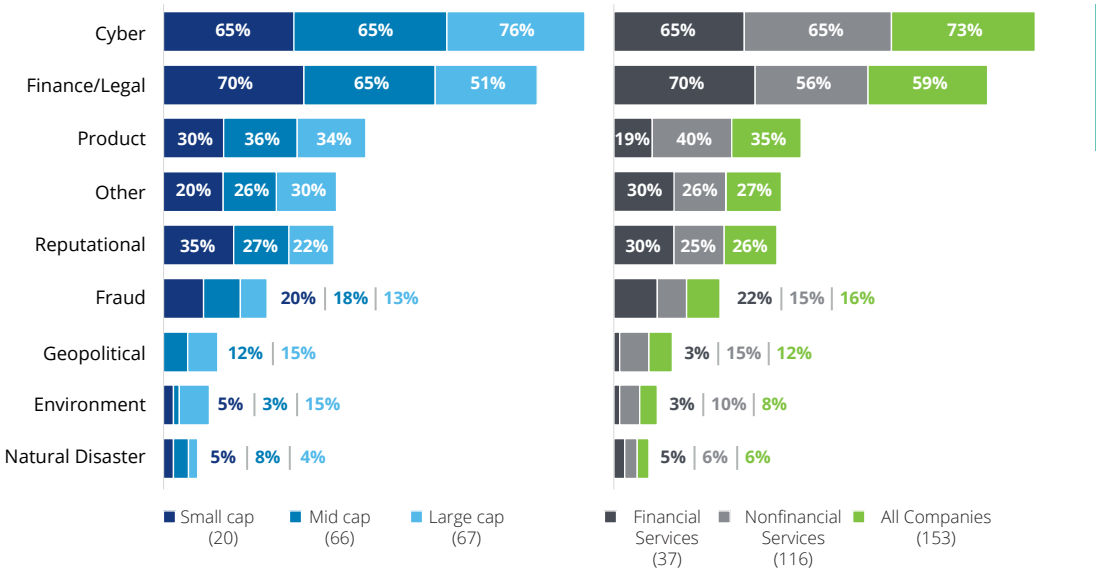
4 https://www.csoonline.com/article/3161146/security/saudi-arabia-again-hit-with-disk-wiping-malware-shamoon-2.html

5 http://foreignpolicy.com/2017/12/21/cyber-attack-targets-safety-system-at-saudi-aramco/

6 Gartner: Forecast: Information Security, Worldwide, 2015-2021, 2Q17 Update

7 https://www2.deloitte.com/content/dam/Deloitte/us/Documents/center-for-board-effectiveness/us-cbe-2016-board-practices-report-a-transparent-look-at-the-work-of-the-board.pdf

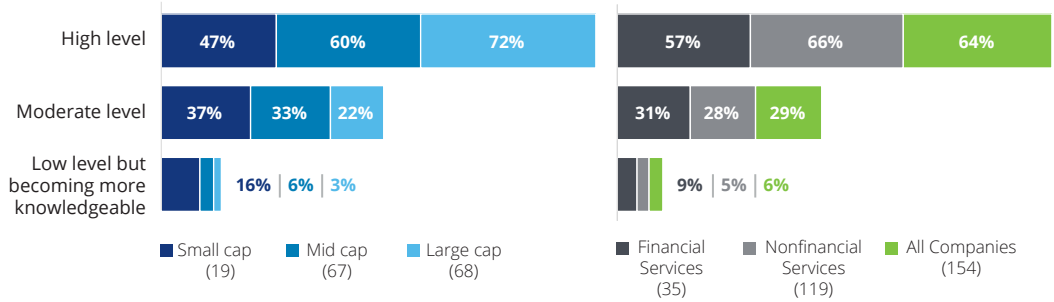
Rank the top three risks that your board is focused on.



Respondents answering "Don't know/Not applicable" were as follows: 15% small cap, 6% mid cap, 13% large cap, 14% FSI, 9% non-FSI, and 10% all companies.

A majority of boards' directors at large cap organizations have indicated that cyber risk is the top risk that as a board, are focusing on.

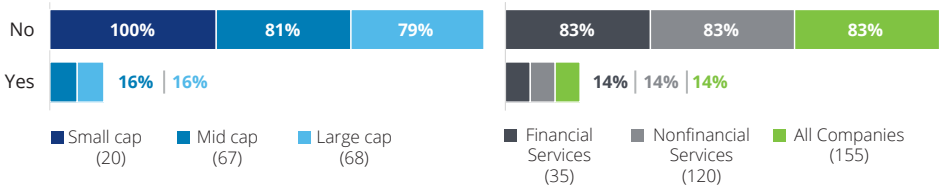
What level of awareness specific to your company does the board have on cyber security?



Respondents answering "Don't know/Not applicable" were as follows: 1% mid cap, 3% large cap, 3% FSI, 2% non-FSI, and 2% all companies.

64% of boards have a high level of awareness of cyber security, and 29% have a moderate level of awareness confirming the notion that the level of cyber security awareness at the board level is high.

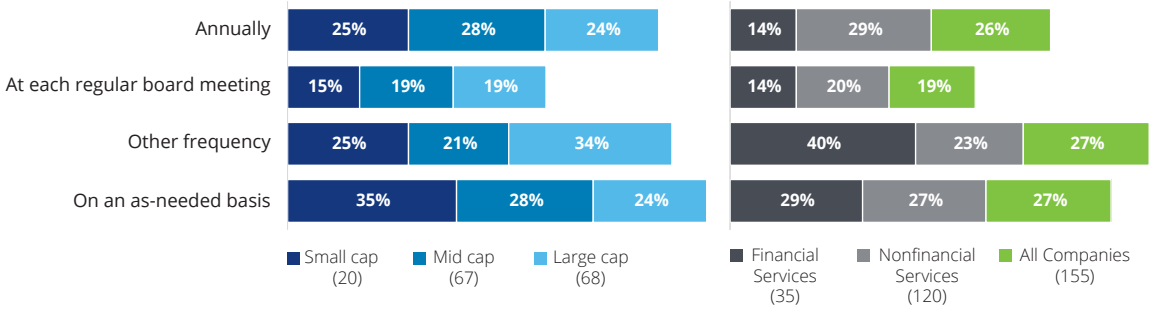
Have you added a director with cyber experience to your board in the past two years?



Respondents answering "Don't know/Not applicable" were as follows: 3% mid cap, 4% large cap, 3% FSI, 3% non-FSI, and 3% all companies.

Despite 14% of boards having added a board member with cyber experience in the past two years a resounding majority of boards still sit without one and while awareness is a vital first step of strong corporate governance, safeguarding an organization's crown jewels requires accountability and timely action. Could the absence of a board member with specialist technology or cyber background be one of the factors contributing to why cyber security programs are failing?

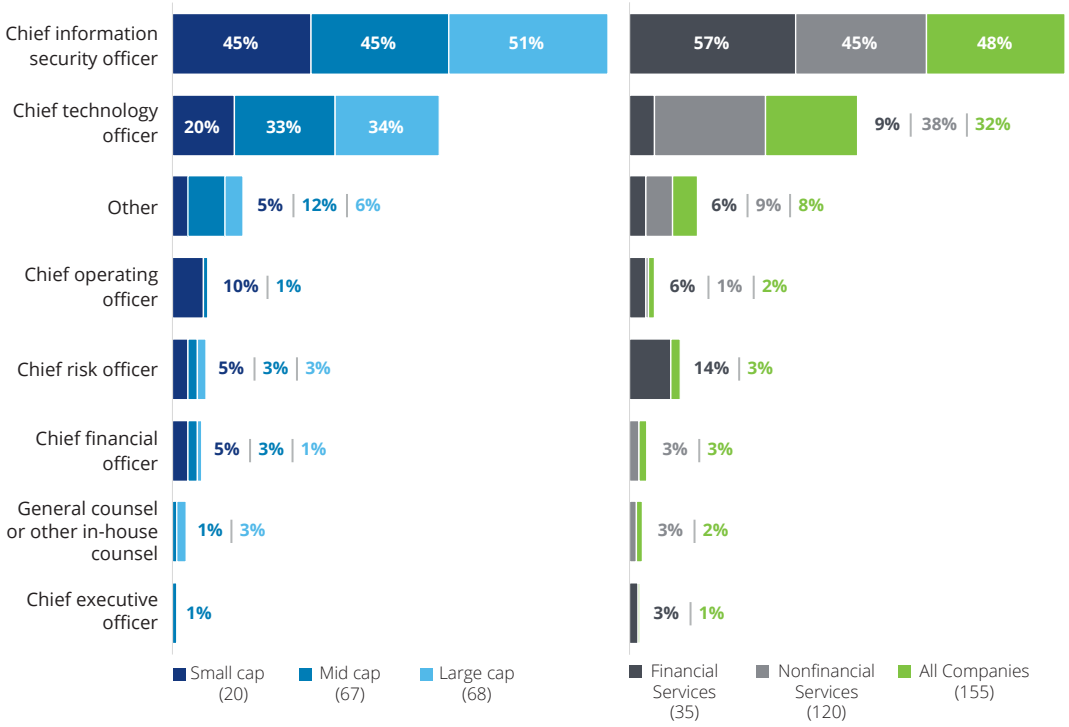
How often does the board receive reports on cybersecurity?



No one selected "Never". Respondents answering "Don't know/Not applicable" were as follows: 3% mid cap, 3% FSI, 1% non-FSI, and 1% all companies.

The cyber threat landscape is ever changing and voluminous. With only 20% of boards receiving updates at each regular board meeting, are board of directors being sufficiently kept up to date on the current state of the organization's cyber security capabilities? And subsequently can actions be taken quickly enough in order to manage that risk within acceptable levels?

Who is responsible for reporting on cybersecurity to the board?



Respondents answering "Don't know/Not applicable" were as follows: 10% small cap, 1% large cap, 6% FSI, 1% non-FSI, and 2% all companies.

With only 51% of large cap organizations having a dedicated executive for cyber security (Chief Information Security Officer) it would appear that many organizations have failed to establish sufficient accountability at the executive level in order to drive the cyber security programs required to manage cyber risk.

As with all things governance "tone-from-the-top" is key, cyber security governance is no different. What the above survey seems to indicate, is that while a majority of boards of directors recognize that cyber risk is the top risk their organizations face, and that there is a high level of general awareness of what cyber risk represents, there is still a divide when it comes to translating that awareness into organizational specific understanding and subsequent action.

Organizations that govern and manage cyber security well have a few common characteristics:

• Management has ownership, responsibility and accountability for assessing, controlling and mitigating risks.

• Management incorporates risk-informed decision making into day-to-day operations, and fully integrates risk management into operational processes

• The board, walks a fine line, playing an active role in oversight, but not extending itself into the day-to-day management of the business is fully aware of internal and external threats, and proactively provides direction and guidance to the management allowing for agile response to changes in threat.

Managing cyber risk and Role of the Board

The growing magnitude of cyber risk and the corresponding potential losses are forcing the board directors to consider devoting increased

attention and resources to respond to cyber threats.

To improve their preparedness to tackle cyber risks, Boards of Directors can focus on the following leading practices[8]:

1. Become aware of cyber threats: Whether or not there is a dedicated risk committee on the Board, it is important to have directors with knowledge and skills pertaining to security, IT governance and cyber fraud. Periodic training and workshops can be organized for directors to come up to speed with the developments in the world of cyber risk.

2. Coordinate cyber threat initiatives: In its capacity of overseeing risk management activities and monitoring the management's policies and procedures, the Board plays a strategic role in coordinating cyber risk initiatives and policies, and confirming their efficacy. These responsibilities include setting expectations and accountability for the management, as well as assessing the adequacy of resources, funding and focus for cyber security activities. The Board can leverage the audit committee chair as an effective liaison with other groups, in enforcing and communicating expectations on security and fraud risk mitigation.

3. Appoint a senior management person to develop a cyber-threat response plan: It is recommended that the Board appoint an executive, focused on information security, so that there is a clear voice directing cyber threat prevention, remediation and recovery plans, related educational activities, and the development of frameworks for effective reporting.

4. Leverage external specialists to review cyber-threat response plans: External specialists can often be a valuable source of information on cyber security issues for evaluating and strengthening security controls and implementing programs for cyber risk management. Specialists can also provide recommendations on key performance indicators that can be used to evaluate and monitor cyber threats.

5. Evaluate the effectiveness of the cyber security program: Boards and C-suites must ensure that the cybersecurity program is reviewed for effectiveness and that any identified gaps are appropriately managed in line with risk appetite. The board, or a committee of the board, should be engaged on a regular basis to review and discuss the implementation of the organization's cybersecurity framework and implementation plan, including the adequacy of existing mitigating controls. Oversight activities include regular cybersecurity budget evaluation, service outsourcing, incident reports, assessment results, and policy reviews/approvals.

6. Prepare for the inevitable: The board should hold management accountable for implementing a cyber crisis management plan and for building cyber resilience capabilities that address the unique risks to the organization. The plan should be regularly measured for effectiveness and should continually evolve over time. Cyberattacks are constantly evolving, and the board should confirm the organization can evolve as well. Finally, the board should ensure the organization's cyber incident response is tested and shown to be effective in a simulated attack. Results of simulations should be used to correct weaknesses in security, vigilance, and resilience.

[8] https://www2.deloitte.com/content/dam/Deloitte/in/Documents/finance/in-fa-cyber-threat-noexp.pdf