Cyber in the Boardroom

Helping Boards Meet Their Responsibilities Regarding Cyber Security

Ton Diemont RE, ir. Thijs Timmerman CISM, Erik Schneider MBA MSc and Ruud Verbij MSc

An organization's board does not only have a key responsibility for securing information assets, but they are in the best position to effectively allocate and steer resources towards cyber security. We review a standard model for board responsibility and we describe our Cyber in the Boardroom methodology that addresses each facet of the model. Finally, we present research on the current state of reporting cyber resilience aspects in annual reports, one of the responsibilities of the board in our methodology.

T. Diemont RE
is a senior manager at KPMG.
diemont.ton@kpmg.nl

ir. T.R. Timmerman CISM
is a cyber risk manager at KPMG.
timmerman.thijs@kpmg.nl

E. Schneider MBA MSc
is a cyber risk senior consultant at KPMG.
schneider.erik@kpmg.nl

R.P. Verbij MSc
is a cyber risk senior consultant at KPMG.
verbij.ruud@kpmg.nl

Introduction

As the number, impact and media coverage of cyber security incidents have grown in recent years, investors, governments, and global regulators are increasingly challenging board members to demonstrate diligence in the area of cyber security. Regulators expect personal and sensitive information to be protected and systems to be resilient to both accidents and deliberate attacks; value chain partners expect a trustworthy and transparent approach to risks; and customers expect that services are available and that their data is protected when stored or processed by organizations.

Boards need to respond to the above pressures, but many board members have a poor understanding of cyber risk and are unsure how best to address these issues. Other members believe responsibility for cyber security rests

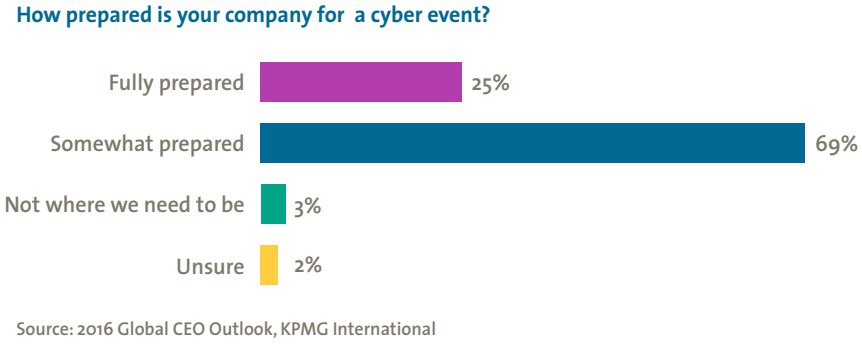

Figure 1. **CEO survey on company preparedness for cyber events.**

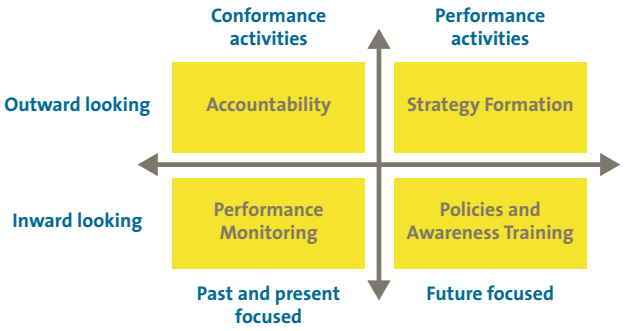

Figure 2. **Bob Tricker's model for corporate governance.**

with the IT or security department. Our work with organizations suggests that not only does the board have a key responsibility for securing information assets, but that they are in the best position to effectively allocate and steer resources towards cyber security. And improving cyber security effectiveness is needed, as indicated by a 2016 KPMG survey of CEOs regarding their organization's preparedness for cyber events (Figure 1).

In this article we review a standard model for board responsibility and then describe our Cyber in the Boardroom methodology that addresses each facet of the model. Finally, we present research on the current state of reporting cyber resilience aspects in annual reports, one of the responsibilities of the board in our methodology.

A Model for Board Responsibilities

To understand why corporate boards need to understand cyber security and how their needs are served by our methodology, we first need to create a model for board responsibilities. There are several such models but for this paper we focus on the one created by Bob Tricker, an influential researcher in the field of corporate governance. This model, created in 1994, is displayed in Figure 2.

As the figure shows, boards have duties to both internal and external parties. In addition, their activities are sometimes past/present focused and sometimes future focused. Let us take a closer look at each quadrant, starting with Strategy Formation and proceeding clockwise.

Strategy defines how the expectations of the external stakeholders will be met, and we noted in the introduction that several key stakeholders (investors, regulators, business partners and governments) are raising their expectations of the board with regard to cyber security. Furthermore, many business strategies are based on IT innovations, so a focus on cyber security should increase with equal measure.

Strategy needs to be supported by a set of policies that translate the high-level, long-term objectives of strategy into actionable plans. Awareness programs must also be established to steer the corporate culture in specific directions. Together, policies and awareness programs reduce risks and change employee behavior. Both are critical in the domain of cyber security.

Once implemented, policies and awareness programs need to be assessed to determine their effectiveness. This is the monitoring category. Key performance indicators (KPIs), key risk indicators (KRIs) and key goal indicators (KGIs) help the board understand trends in management effectiveness at delivering desired results. Good indicators show the benefits of investments and could indicate areas where more resources need to be allocated or changes need to be made.

A final responsibility of the board is being accountable to external parties through independent audits and published reports. These reports discuss not only financial data but also major risks and trends while the audit findings demonstrate compliance to regulatory standards (e.g. Payment Card Industry-Data Security Standard). A case study will be discussed later in this article.

How does cyber security fit into this governance model? Very easily. Our "Cyber in the Boardroom" methodology addresses each board responsibility in turn, incorporating the top-down approach on the performance side and the

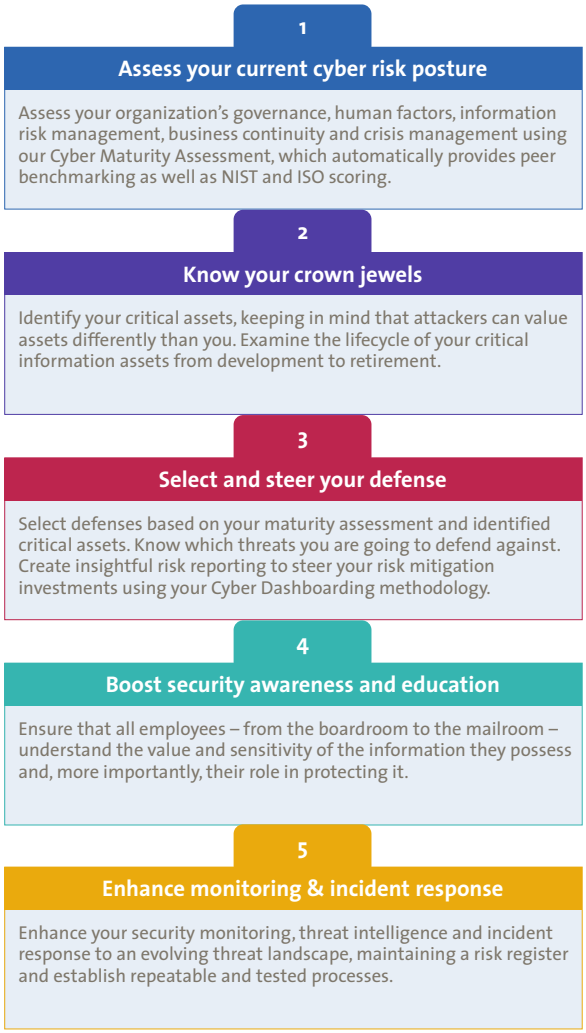

Figure 3. **Cyber in the Boardroom methodology.**

bottom-up approach on the conformance side. We now describe this approach in more detail.

A Methodology for Cyber in the Boardroom

The Cyber in the Boardroom methodology (see Figure 3) helps board members answer their most common questions: how to gain insight into their current risk posture, how to steer and assess the effectiveness of their cyber security program and how to develop key risk indicators. The steps are as follows.

1. Assessing the Organization's Current Cyber Risk Posture

An organization cannot move forward intelligently without knowing where it stands. Thus a first step in strategy formation is to gain insight into its current risk posture, which can be done by assessing governance models, human factors, information risk management, business continuity, crisis management, operations and technology, and legal and compliance profiles. KPMG's Cyber Maturity Assessment (CMA) methodology is a strong tool to assess these domains because it automatically provides benchmarking against industry peers using KPMG, NIST and/or ISO maturity scores.

2. Perform an Information Risk Assessment

The next two steps cover the information risk management (IRM) process that is described in greater detail in two previous articles (see [Herm13] and [Hars14]). In summary, identifying critical business processes and assets is a key step in effectively allocating limited resources to have the greatest business impact. The involvement of board members and senior business leaders in this process is necessary to ensure the highest business priorities are covered. Otherwise, lower management may exaggerate the importance of their division or service lines, which can lead to sub-optimal investments.

Risks are composed of event likelihoods and impact. In the cyber domain, likelihoods are often calculated by considering how threats can exploit specific vulnerabilities. Therefore, business must be aware of which threats will have the biggest impact if they materialize and which vulnerabilities are the most critical. The end result of this process is a top-level overview of the major risks from an information management perspective.

3. Select and Steer Your Defense

Once these top risks have been identified, business leaders must consider their appetite for risk and determine whether specific risks will be transferred, mitigated, avoided or accepted. The establishment of a cyber security steering committee, which consists of both business and support functions, e.g. IT Risk, Legal, Compliance, Internal Audit, can improve the execution and monitoring of these decisions. A complete overview of residual risks using a risk register is also recommended to ensure the business is not holding risks in excess of its defined risk appetite.

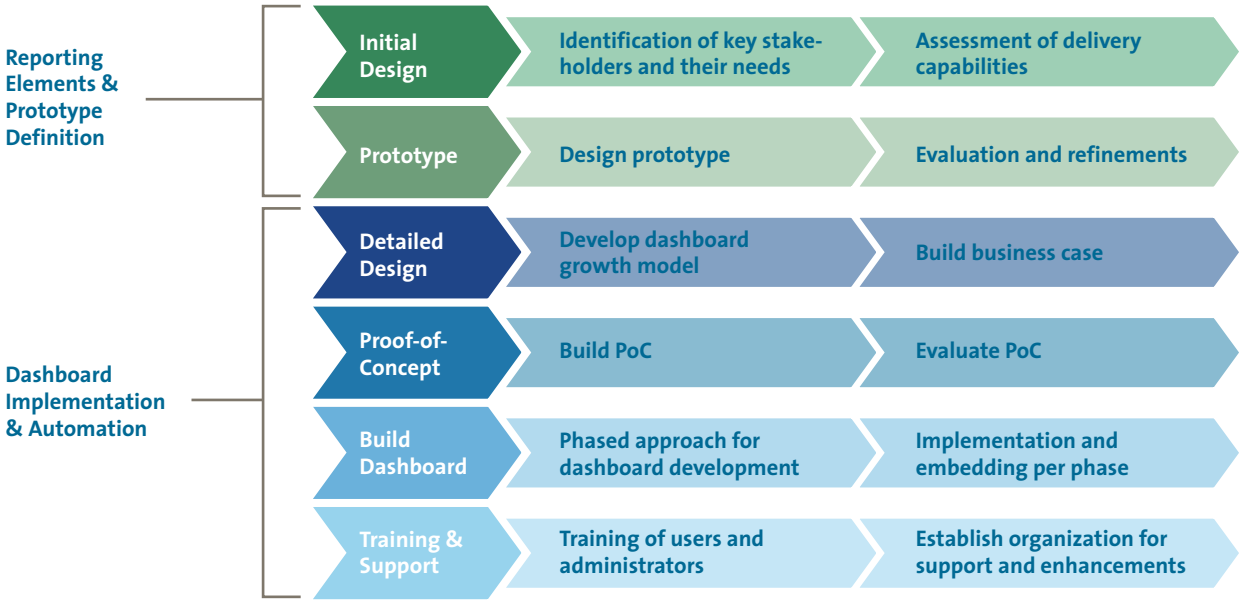

Figure 4. **Cyber dashboard development methodology.**

4. Develop Policies and Security Awareness Programs

Creating a cyber risk culture can pay large dividends over time and vastly improve the security of any organization. Two important ingredients to affect a change in culture and procedures are: *policies* and *security awareness programs*. Policies provide concrete directions on how to implement the risk strategies selected in the first three steps. They should be further refined into detailed procedures and guidelines for technical domains to ensure consistent application across regions and to improve resilience despite employee turnover. Security awareness programs attempt to change human behavior and should cover all internal parties, from board members to entry level joiners. Humans are often the weakest link in cyber or information security so creating awareness among employees regarding the value of the information assets and best practices to prevent or report security incidents can act as an insurance policy for the large investments made in customer procurement, IT assets and branding. Changing behavior is difficult and the threat landscape is ever changing so awareness programs must be regularly administered and frequently updated.

5. Enhance Monitoring

After establishing or approving the performance actions in the first four steps, the board must maintain insight and report to external stakeholders on the effectiveness of their information risk management. The selection of KPIs, KRIs and KGIs with the greatest impact is critical to attain informed oversight and to assess where additional resources need to be directed. Downward trending indicators may also suggest that the threat landscape has changed or security assets have become outdated. The reporting of threats, risks and compliance is not only a legal requirement but also provides input to the next iteration of strategy formation. We explore the current state of cyber and information security within annual reports in the last section of this article.

A well-designed cyber dashboard is key to providing a periodic, comprehensive and integrated picture that will address board questions or concerns. It should not only provide insight into the organization's current state of cyber resiliency but should also provide feedback on the effectiveness of security management and highlight the value of past investments. Although similar in concept, actual security dashboards are highly customized. Our team has created a methodology for dashboard development (Figure 4) that accounts for the target organization's specific information needs, its data sources and its avail-

able platforms. These requirements and capabilities are gathered via interviews and workshops with key stakeholders during the initial design phase. It is during this discovery stage that we encourage organizations to adopt a comprehensive view on cyber security and to consider KPIs, KRIs and KGIs that address non-technical security domains in addition to technical ones.

Our general framework for dashboard categories is presented in Figure 5. Let us look at example visuals for each element.

Threats

Threats represent potential forces that can negatively impact business operations if they materialize. We consider both external sources (e.g. hackers hired by organized crime) and internal sources (e.g. lack of a secure coding standard for application development) for threats. Figure 6 shows how threats may be presented on a "threat radar". The organization's ability to manage the threat is plotted against the threat's potential impact. In addition to the radar, the dashboard may also indicate the trend in the threat level since the previous reporting period and what projects, systems and/or actions the organization is using or taking to address the threats.

Risks

Risks combine high potential threats to known vulnerabilities within the organization and are specific enough for decisions to be made whether to accept, mitigate, transfer or avoid them. Risk maps are a common way to display risks and an example is shown in Figure 7. Here risks are plotted depending on their likelihood and impact. Colors are often used to highlight criticality and may define required actions (e.g. red actions must be mitigated or otherwise the business must sign a formal risk acceptance document). These colors are frequently aligned with defined risk acceptance statements or tolerances. Like threats, there is usually an accompanying table that shows the changes to the risk since the last period, the risk owner (person to act) and the next steps.

Compliance

Compliance informs the board about how well the organization is adhering to defined thresholds and controls. Security-related audit findings can be displayed but other representations, such as highlighting the organization's capability to detect, protect, respond and recover, can also be developed. Figure 8 shows just one example that highlights not only the number of findings but also the ability

Figure 5. **Cyber dashboard domains.**

of organizations to resolve the findings within specified timelines.

Incidents

Security incidents highlight the major security events during the last reporting period. These incidents can provide insight into risks and threats and the security function's ability to respond. Detection and response are critical components of the security process because achieving 100% prevention is nearly impossible. Dashboards usually use tables to review incidents and include information on data sensitivity, business impact and lessons learned. In addition, information on time to detect and time to resolve the incidents provide information on organizations resiliency.

Awareness and Culture

People are often the weakest link in a security system and can negate heavy investment in security hardware and software products. Therefore, investments in security awareness can represent a force multiplier in an organizations security plan. Speed dials (Figure 9) showing the coverage of security awareness programs, the percentage of staff who have failed to complete training within timelines and surveys/tests of security knowledge are frequent dashboard elements.

Projects

Projects highlight ongoing efforts to improve security and address security issues identified on the other dashboard categories. Tables of security-related projects indicate the

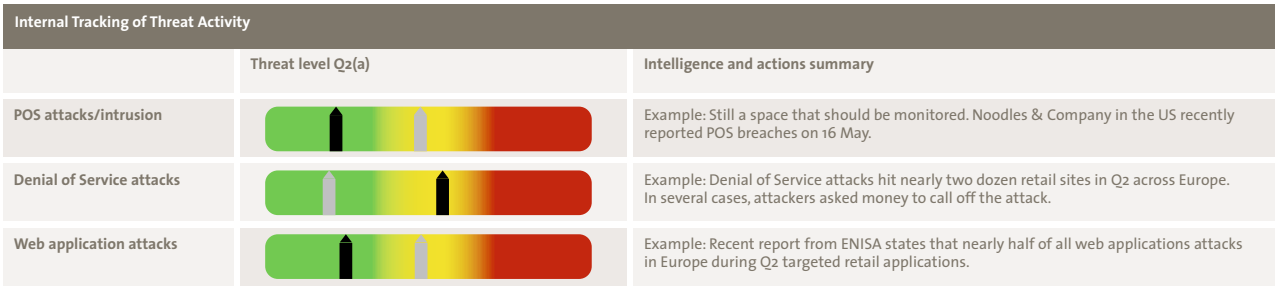

Figure 6. **Threat radar.**

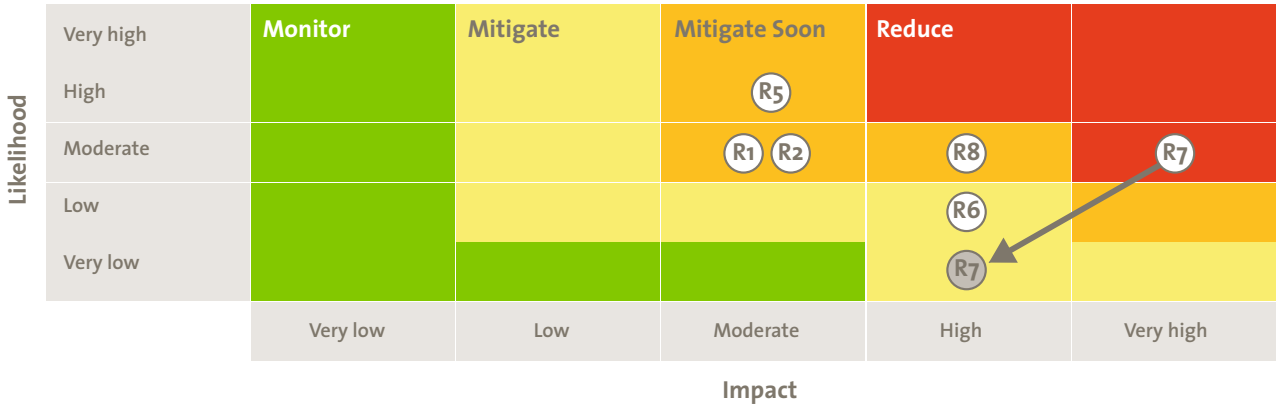

Figure 7. **Risk map.**

project owner, whether it is on schedule and risks to the projects, among other possible attributes.

Once we have a clear understanding of an organization's requirements and capabilities, we can begin selecting relevant key performance/risk indicators and start developing a dashboard prototype. This prototype is then presented for feedback and the development process progresses in an agile fashion with multiple rounds of feedback and improvement until an acceptable model is put into production.

The KPMG Approach Addressing Board Responsibilities

Let us revisit the model for board responsibility that we presented at the beginning (Bob Tricker's model in Figure 2) and see how KPMG's Cyber in the Boardroom approach helps boards meet these responsibilities regarding cyber security. We plotted the components of our approach in relation to the model in Figure 10.

As one can see, the first four steps help the board with performance activities while the cyber security dashboard assists with conformance duties. Determining the current risk posture and conducting a full information risk assessment are important aspects of cyber security strategy formation. Selecting and steering defensive measures, spans both strategy and policies – risk actions are more strategy activities while the duties of the information security steering committee relate to the policy side. The next step is directly addressing policies and awareness training, an inward looking performance activity of the board. Finally, a dashboard informs the board of all conformance related topics, both inward and outward looking.

We note that while the dashboard informs the board about risks and compliance issues, the board itself must update external stakeholders regarding these topics. One requirement for doing this is through annual financial reports. We now present our research on the extent to which cyber security is addressed in these reports, focusing on the AEX and Midcap-listed organizations (top 50 listed organizations in the Netherlands by capitalization weight).

Understanding the Current State of Affairs

An annual survey by KPMG on the reporting of cyber security risks in the annual reports of AEX and Mid-cap-listed organizations shows that the reporting of these risks is currently inadequate. Although more than 83% of annual reports mention cyber security, further investigation reveals that only 66% do so with any degree of depth in terms of threats, risks or measures taken.

In some sectors we see a strong focus on cyber security risks in annual reports, such as in the financial sector where the Dutch Central Bank, and in turn also the European Central Bank, have expressed strong expectations in this regard. The paragraph "A Sector View" provides more information about the differences per sector.

Too often "cyber" is left to individual departments within organizations (almost always the IT department), and often even the CIO can no longer "see the wood for the trees". This results in a diffuse approach and a lack of focus on the ultimate risk to the organization. We see this in the reporting to shareholders in the annual report as discussed previously. And while the topic is increasingly addressed in annual reports, there has been little progress in terms of the depth to which the topic is discussed; in fact, there has been a slight regression in this regard.

Let us look at other research insights. More than in previous years, responsibility for managing the risks of cyber security is laid at the door of the executive board. Figure 11 shows the number of annual reports which discussed the subject of cyber security and to what depth, as well as the percentage of annual reports that deemed the risk of cyber security to be a matter for the executive board.

A Sector View

Sectors differ in their dependence on IT, as can be seen in Figure 12. Organizations in diverse sectors also assign different values to the " " of the organization. It is therefore not surprising to see a big difference between the number of organizations within a sector addressing cyber security in their annual reports, how in-depth the coverage is and whether the issue is regarded as a responsibility of the board. For some sectors it could be true that more important risks exist than cyber security. However, some generic cyber security risks apply to every company, such as: integrity of financial data; continuity of the organization based on the IT environment; confidentiality of customer/

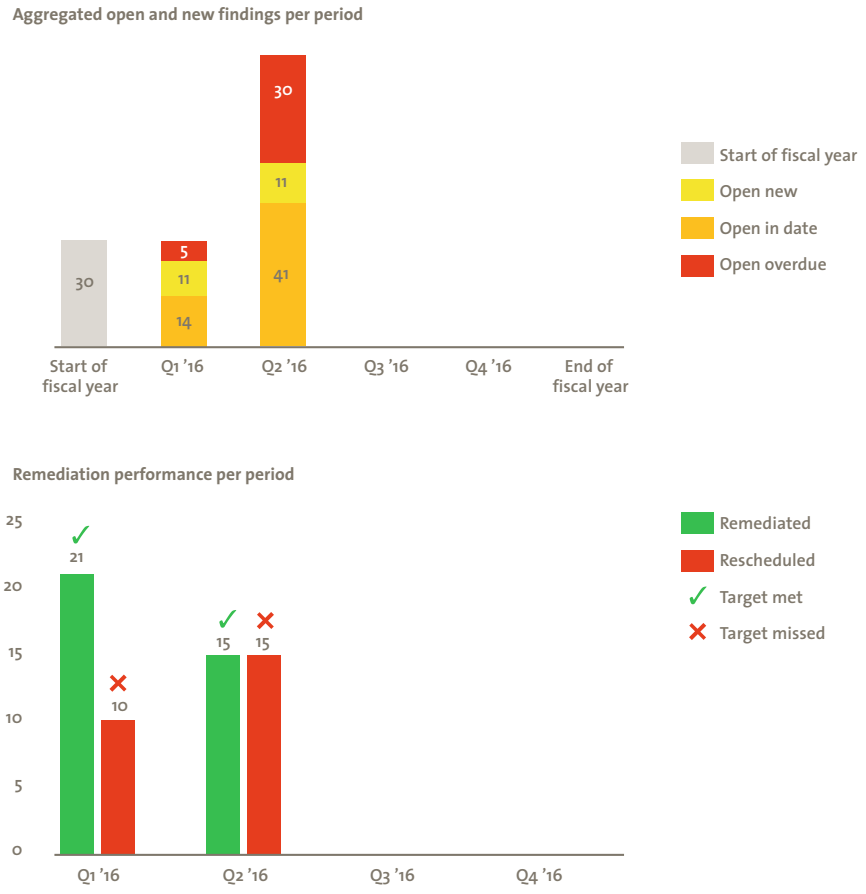

Figure 8. **Security related audit findings and remediation.**

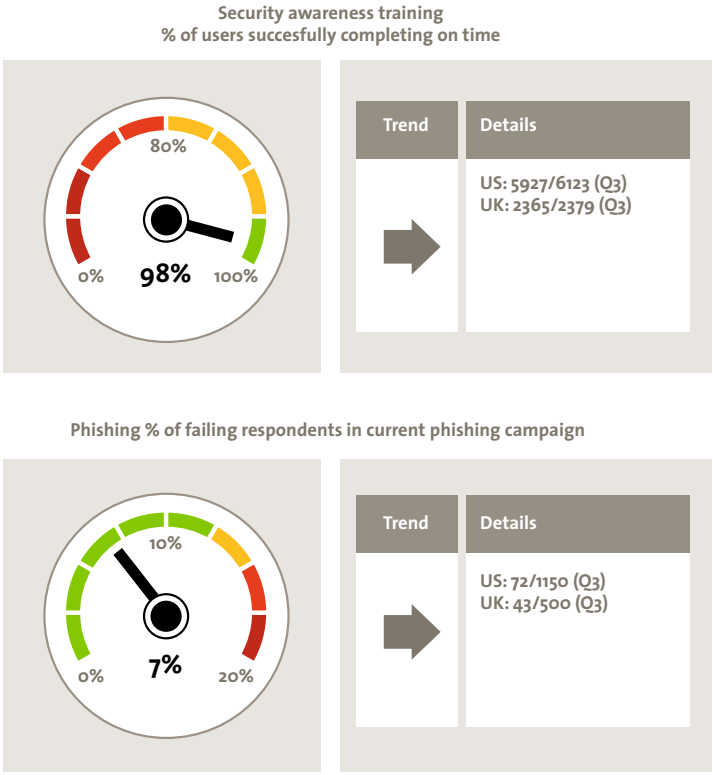

Figure 9. **Speed dials related to security awareness.**

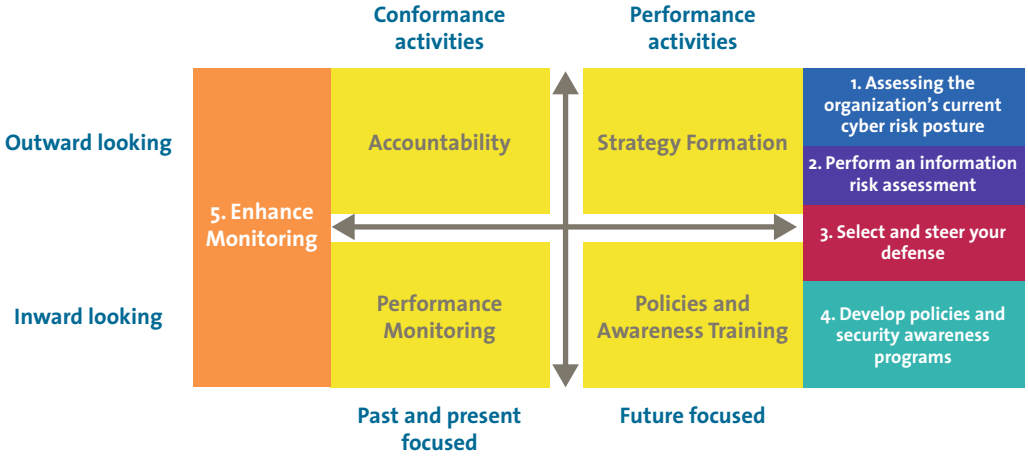

Figure 10. **Bob Tricker model incorporating KPMG's Cyber in the Boardroom approach.**

employee private data. Addressing these cyber security risks should be a minimum for annual reports.

It is plain to see that organizations in the technology and financial services industry have a strong focus on this topic and regard it as a responsibility of the executive board. A sector like real estate, on the other hand, is clearly less concerned about the subject. Opportunities for improvement are readily present.

Summary

We believe cyber security is an important topic at the board level. This can be understood by observing the increasing cyber security expectations external stakeholder are placing on the board and the board's responsibilities in meeting those expectations. Our "Cyber in the Boardroom" approach addresses these responsibilities by assessing an organization's current risk posture, identify-

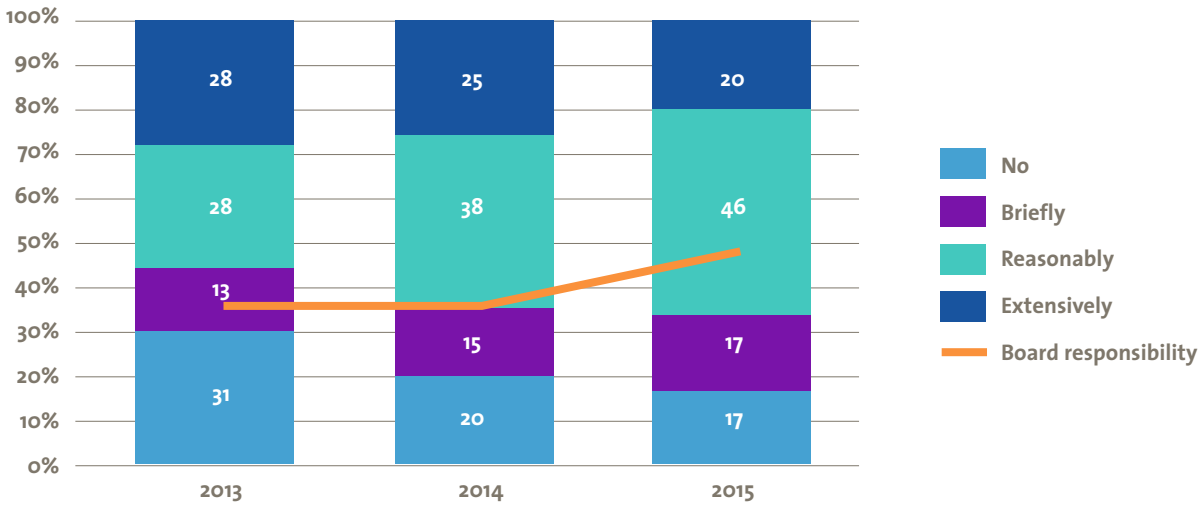

Figure 11. **Percentage of annual reports discussing cyber security.**

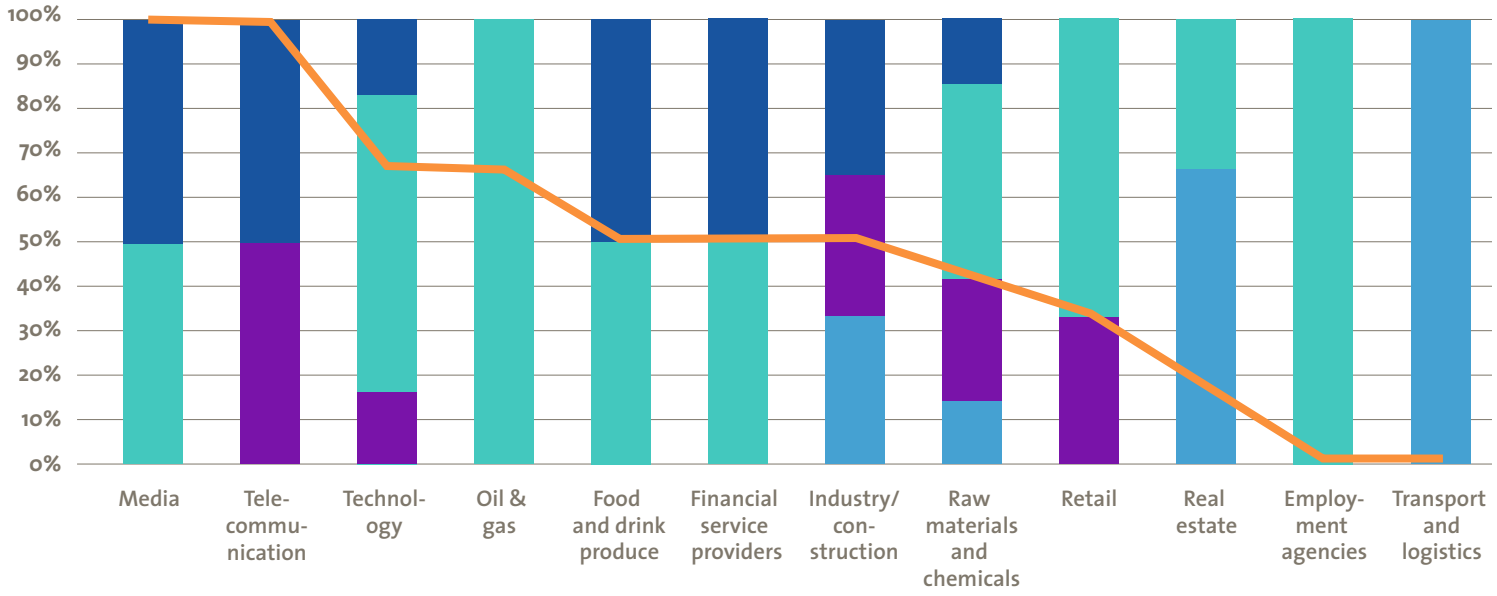

Figure 12. **Sector overview of annual reports discussing cyber security.**

ing its crown jewels, developing a strategy and directing internal stakeholders on how to achieve strategic goals with awareness education and policies. The final element, dashboards and reporting, measures management effectiveness in achieving stated objectives and provides information for reports back to external stakeholders.

Boards are experienced at identifying and addressing risks so they are more than capable of addressing cyber security risk as well. And to some extent they do. Our research demonstrates that boards are already reporting on cyber risks in annual reports but they can improve the depth of their analysis. We believe doing so will better inform external stakeholders and further improve the cyber risk management process, creating a safer environment to conduct business.

References

[Hars14] A. van der Harst, J. Hermans and P. de Meijer, *Realizing the 2020 Vision of Information Risk Management*, Compact 2014/1.

[Herm13] J. Hermans, A. van der Harst, P. de Meijer and S. Verkaart, *The 2020 Vision of Information Risk Management*, Compact 2013/1.

About the Authors

T. Diemont RE is a senior manager at KPMG. He advises and supports our clients within the Financial Services industry on Information Risk Management, security strategies, cyber security, cyber resilience, business continuity management and risk reporting (dashboards). He has more than 20 years of international and strong experience in the full range of Banking and IT, along with IT Risk, IT Security management, Security Architecture, IT Strategy, Operational Risk Management, Enterprise Risk Management, internal control, auditing and advisory at multiple complex and international organizations. He is used to operating at an Executive level (board, C-level, senior management) and dealing with other stakeholders such as Supervisory Board, Audit Committee, Regulators, Supervisors, Program Directors and Project Leaders.

Ir. T.R. Timmerman CISM is a cyber risk manager at KPMG. He helps organizations in designing and improving their information risk management strategy, as well as in designing insightful cyber risk reporting for board and supervisors. Being an interim CISO himself, he has sat on the other side of the table. In addition, he is actively involved in KPMG's innovation program where he cooperates with fast-growing start-ups in the information and intelligence area. He was responsible for the development of the KPMG Cyber Trends Index and the KPMG Cyber News and Trends app. He holds a master's degree in Industrial and Applied Mathematics.

E. Schneider MBA MSc is a cyber risk senior consultant at KPMG. He is focused on board level awareness, cyber risk quantification, security dashboards, threat intelligence and maturity assessments. He has a long background in equity investments and finance prior to his career in information security. Before joining KPMG, he researched network anomaly detection and best practices within the Cyber Crime Expertise and Response Team (CCERT) of a major Dutch bank. He holds an MSc in Security Technology and an MBA in General Management.

R.P. Verbij MSc is a cyber risk senior consultant at KPMG. He started his career at KPMG in 2013 as an intern, researching risk assessment methods for e-voting schemes. In 2014, he joined the Cyber Security team as a consultant with a focus on both the organizational and the technical part of IT security. He has gained experience in PKI and general IT audits using different control frameworks. He gives security advice on IT Security policies, was involved in security awareness and governance as well as with risk and compliance engagements and has gained significant experience on security reporting and being the security challenger of a large multi-million euro software project. He holds a master's degree in Computer Science.