Is your board aware how well-protected their crown jewels are?

Covid-19

The first place to address cybersecurity risk

March 2020

Cyber in the Boardroom

Countering the current Covid-19 pandemic requires board-level leadership, insight and the right prioritization in decision-making.

Why should cyber security be addressed in the boardroom?

Investors, governments, and global regulators are increasingly challenging board members to actively demonstrate diligence in the area of cyber security. Regulators expect personal 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. Meanwhile, customers expect that services are available and data is protected when stored or processed by leading organizations.

From threat to opportunity

In these times, customer transactions and business processes are digitalized at light speed, in order to adapt to the situation. This yield business opportunities both during and after the pandemic period. Senior management can capitalize on these opportunities while limiting unanticipated risks by establishing effective cyber risk management from the top. This includes having a comprehensive overview of your business environment, potential targets and threat actors, current state of protection and legal and regulatory requirements.
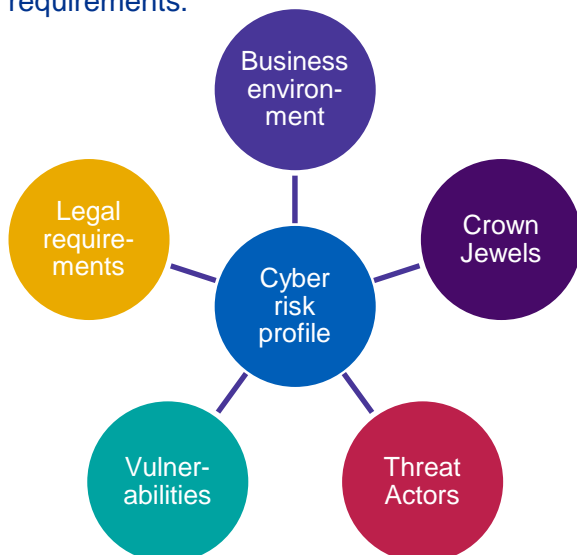
Common challenges

Based on our recent reach out to boards, these are the three most common questions at the executive management and board members ask today during Covid-19:

What are the cybersecurity threats and risks during Covid-19 and how do they affect my organization?

Is my organization's cyber security organization ready to meet the challenges related to the Covid-19 cyber threat landscape?

What key risk indicators should I be reviewing at executive and board levels to closely monitor my cyber risk management?

Obtaining insights

Recent KPMG research demonstrated that a limited number of the top 50 listed companies address their approach towards cyber security in their most prominent publication.

While cybersecurity is still a relatively new topic, board members must show their diligence and are expected to report based on trustworthy risk data and insights.

Traditional IT-based cyber security transforms into business-driven opportunity management within the comfortable bounds of mitigating controls. Clear insights in top risks, current threat levels and effectiveness of defenses gives business and Boardroom the comfort they need. Ensure you provide a real-time overview of cyber threats and trends to your organization via cyber dashboards and utilize your KRI's KPI's, maturity assessments and SOC intel.
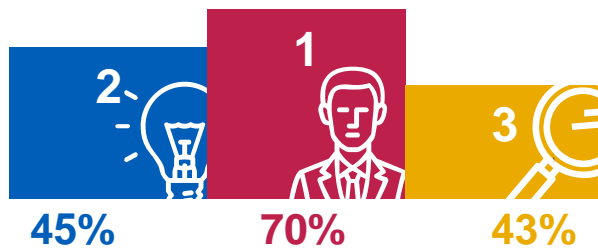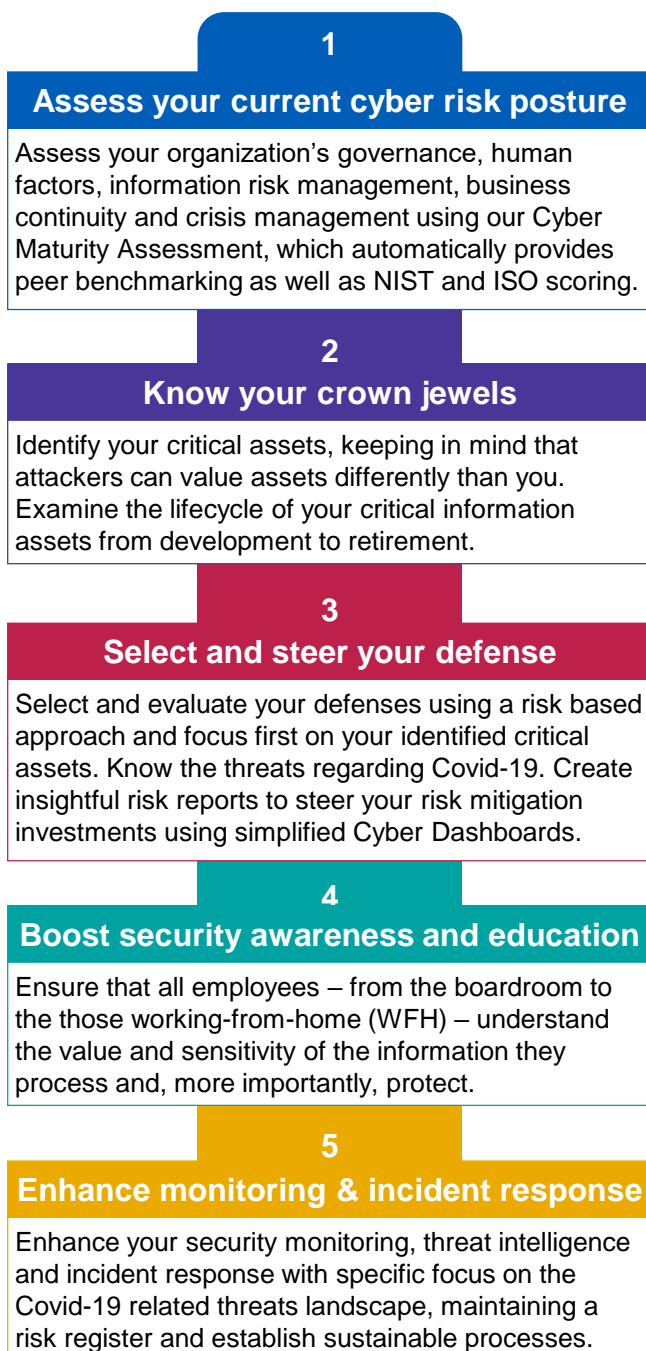
45%
The level of cybersecurity awareness in the organization is the number two success factor.

70%
The most important success factor regarding cybersecurity and risk management is senior management support.

43%
Having insights into the key information assets and information risks to your cybersecurity priorities and investments is the number three success factor.

The KPMG Cyber in the boardroom approach – during Covid-19

We help senior management and executive boards to understand cyber risk using their language and to improve strategic decision making by using aggregated cyber data.

1
Assess your current cyber risk posture

Assess your organization's governance, human factors, information risk management, business continuity and crisis management using our Cyber Maturity Assessment, which automatically provides peer benchmarking as well as NIST and ISO scoring.

2
Know your crown jewels

Identify your critical assets, keeping in mind that attackers can value assets differently than you. Examine the lifecycle of your critical information assets from development to retirement.

3
Select and steer your defense

Select and evaluate your defenses using a risk based approach and focus first on your identified critical assets. Know the threats regarding Covid-19. Create insightful risk reports to steer your risk mitigation investments using simplified Cyber Dashboards.

4
Boost security awareness and education

Ensure that all employees – from the boardroom to the those working-from-home (WFH) – understand the value and sensitivity of the information they process and, more importantly, protect.

5
Enhance monitoring & incident response

Enhance your security monitoring, threat intelligence and incident response with specific focus on the Covid-19 related threats landscape, maintaining a risk register and establish sustainable processes.

Why KPMG?

Cyber in the Boardroom is one component of KPMG's Global Cyber Security Services. Our vision is to make cyber security an integral part of your business through:

+ **Experience**
We understand your business and know all about cyber security. We have supported many organizations in various industry sectors in developing insights into cyber threats, trends and incidents, have identified key information assets and have created insights that strategic stakeholders are looking for.

+ **Integrated Approach**
We bring together specialists in information protection, risk management, organizational design, behavioral change and intelligence management. These combined skills are utilized to tailor a solution relevant to your risk appetite and the cyber threats your organization faces.

+ **World Leader**
KPMG has recently been rated as the global leader in cyber security services globally by Forrester Wave – the most widely recognized analyst report in the cyber security consulting market. Our clients recognize us as an easy to work with boardroom advisor and innovative cyber security ecosystem partner.

Cyber in the Boardroom

Contact us

For more information on the Cyber in the Boardroom during Covid-19 or our other KPMG's Cybersecurity services, please contact us or visit us at:

https://home.kpmg/sa/en/home/services/advisory/technology/cybersecurity.html

Ton Diemont
Director and Head of Cybersecurity
KPMG in Saudi Arabia

M: +966 56860 8393
E: antondiemont@kpmg.nl