Public consultation on the contractual public-private partnership on cybersecurity and possible accompanying measures

ECIIA response

II. Assessment of cybersecurity risks and threats

1.1 What are the most pressing cybersecurity challenges for users (indivuduals, business, public sector) ?

- Extraction and use of identity and payment data to commmit fraud
- Industrial or economic sabotage (eg disrupting or slowing down network and computer functioning)
- Loss of know-how and confidential business information (trade secrets) – industrial and economic espionage, and other types of confidential information

Commentary :

The boards of organisations need to understand and approach cybersecurity as a **strategic and organisation-wide risk management issue**, not an IT issue alone. It also needs to understand the cyber risks associated with outsourcing partners and third party service providers. In order to discharge their oversight responsibilities effectively, boards need awareness not only of incidents of cyber attack, but also data-breach attempts . They should discuss the organisation's overall risk management, control and crisis response frameworks on the basis of independent, objective, expert advice. Internal audit has a central role to play to support board discussion of these issues.

In some Member States, legislation requires that companies involved in critical national infrastructure have to perform regular, specific IT security audits . IT audits specifically related to cyber risks should be seen as a key measure to protect organisations.

1.2 Which sectors/areas are the most at risk ?

- Finance and banking
- Energy
- Transport
- Health
- Public administration

4.1 What will be the 3 main cybersecurity challenges by 2020 ? (Please explain)

A rapidly evolving landscape in terms of cyber threats : Organisations are subject to attackers who are part of sophisticated teams using specialised and targeted malware against systems and indivuduals in multi-stage attacks. These are able to innovate at a faster pace than organisations' capability to develop their defences, particularly for medium-sized and smaller enterprises ; and also than the marketplace's ability to develop effective proprietary cyber-defence products..

Greater connectivity leads to greater risk : Organisations are vulnerable to attacks not only to their own networks but also to those of their vendors, suppliers, partners and customers. Corporate Boards need to ensure that management is fully engaged in developing defence and response plans

as sophisticated as the attack methods. They must also ensure that the right controls are in place and the risks are minimized thanks to an effective governance model, and in paarticular the implementation of the **'3 lines of defence'** model. (See commentary on question 7 below.

Balancing cybersecurity with profitability : Boards and management teams must strike an appropriate balance between protecting the security of the organisation and mitigating downside losses, while continuing to ensure profitability and growth in a competitive environment.

A recent study (from the National Association of Corporate Directors *: Public company governance survey 2013/2014*) found that four basic security controls were effective in preventing 85 per cent of cyber intrusions :

-restricting installation of applications ;
-ensuring that operating systems are regularly and routinely patched with current updates;
-ensuring that software applications have current updates ;
-restricting administrative privileges.

For medium-sized and smaller organisations in particular, these should form the core of good practice. However, as noted above, the risk landscape is evolving so rapidly that updates are struggling to keep pace with attacker innovation.

III. Cybersecurity market conditions

5. What level of ambition do you think the EU should set itself for cybersecurity market development ?

Identity and access management : Make the EU more competitive
Data security : Make the EU more competitive
Applications security : Make the EU more competitive
All other domains (infrastructure security, hardware security, IT security audit, planning and advisory services, IT security management and operation services, IT security training : Strive for global leadership

6 : How does legislation influence the European cybersecurity market or how is it likely to do so ?

Current legislation does not include any element in relation to corporate governance and the management of cybersecurity risks in organisastions. This is a gap. The relevant legislative and guidance frameworks should promote an integrated, cross-departmental approach to managing cyber risk involving legal, internal audit, risk management, compliance, finance, HR and IT functions.

The senior management team should track and report on the business impact of cyber threats, and all risk management activity. For its part, internal audit evaluates the effectiveness of cyber threat risk management and reports to the audit committee and board on these issues.

Many organisations operate in multiple jurisdictions around the world, and reporting requirements are not harmonized across countries and continents. It is therefore difficult for the corporate

headquarters to monitor global reporting : there is a case for developing global best practice standards and frameworks.

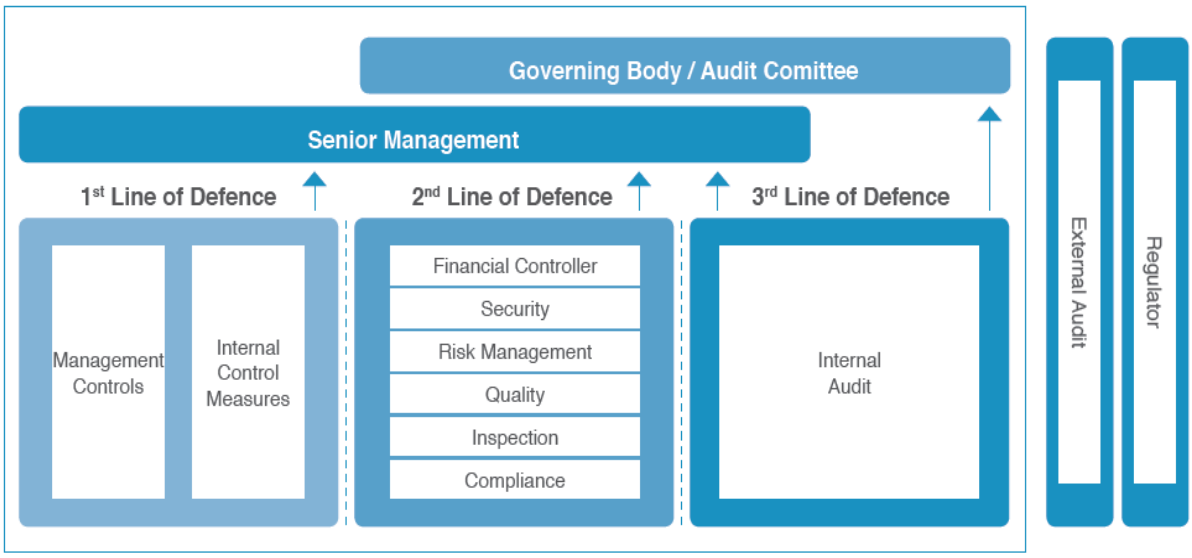
There is also a pressing need for adequate training for employees on the new risks, across all types and sizes of organisations.

VI. The role of research and innovation in cybersecurity

7 : What would be your contribution to fostering innovation and competitiveness of cybersecurity in Europe ?

As the body representing the profession of internal auditors across Europe and the Mediterranean basin, the ECIIA has a critical part to play in promoting best practice in terms of governance models which organisations should implement to manage risks, including cyber risks.

In particular, the ECIIA promotes the implementation of the internationally recognised **3 lines of defence** model summarised below.



In this model, the **second** line of defence is responsible for performing the majority of the governance functions related to cybersecurity : it should define the policies, standards and technical configuration standards, and should be responsible for reporting and tracking. The **first** line is responsible for implementing the policies and standards, and is responsible for day-to-day monitoring of networks and infrastructure.

The **third** line of defence - internal audit - is responsible for ensuring that the first and second lines are functioning as designed. nternal audit will assess cyber risk, give an independent and objective opinion and make recommendations for improvement action. Internal auditors analyse the data, in their audit review work, that can help identify potential breaches.

It is also important that organisations develop a strong **business continuity/crisis response plan** : the internal audit department will give an objective and independent opinion about the plan.

Internal audit will also review the processes implemented for continuous imrovements to anticipate and survive to cyberattacks.

Finally, internal audit can help organisations train their employees about cybersecurity processes and prevention.

ECIIA, Brussels, March 2016