KPMG

# Cyber In the Board Room

**John Hermans**
**EMEA Leader Cyber Security**

**https://www.kpmgcyberbenchmark.com/global**

## Agenda

- Little introduction to cyber security
- Who owns the cyber risk
- How to determine cyber risk profile?
- But what about risk quantification / risk appetite etc?
- To conclude

# Cyber security is here to stay!

1. Increasing / changing threat actors landscape
2. Increasing market for cybercrime tools and stolen information
3. Increasing cyber crime opportunities as result of hyper-connectivity, further digitalization of business process as well as use of emerging technologies
4. Too little cyber security awareness




# Companies barely report on cyber security

**800+ annual reports**
were selected from companies among 28 countries

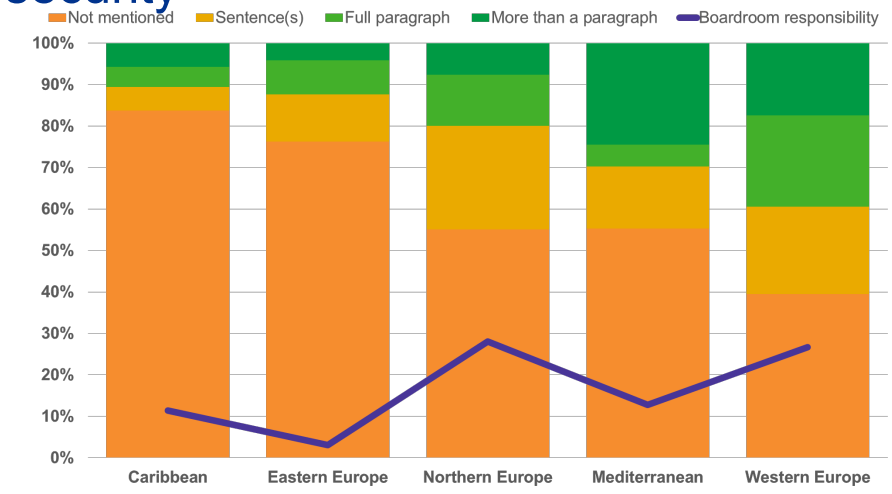
**26%**
dedicated more than a paragraph to cyber security

**18%**
dedicated one paragraph to cyber security

**56%**
do not mention cyber security risks at all

**18%**
consider cyber security risks a boardroom responsibility

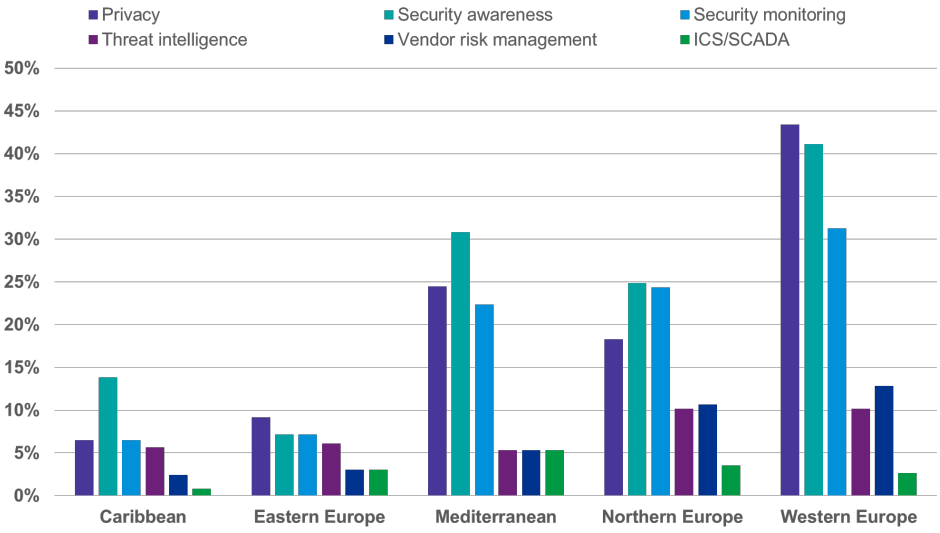
# Western Europe reports most on cyber security





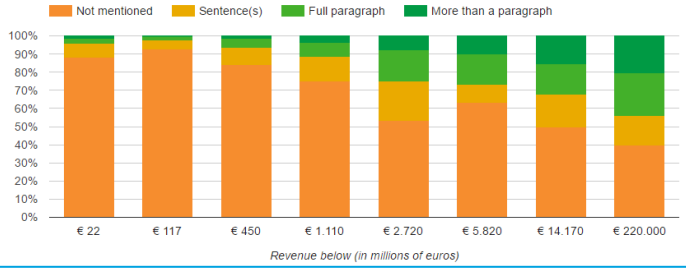



# Biggest focus on preventive measures

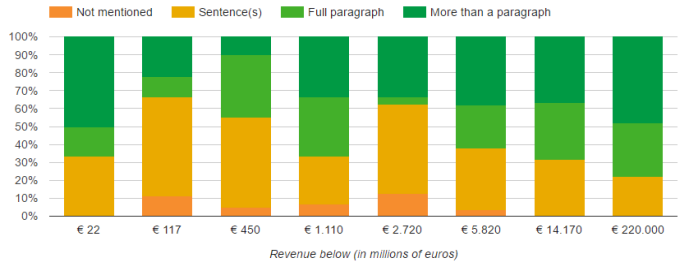


# Boardroom responsibility pushes attention

**No boardroom responsibility**




**Boardroom responsibility**








# Board engagement is improving, despite challenges

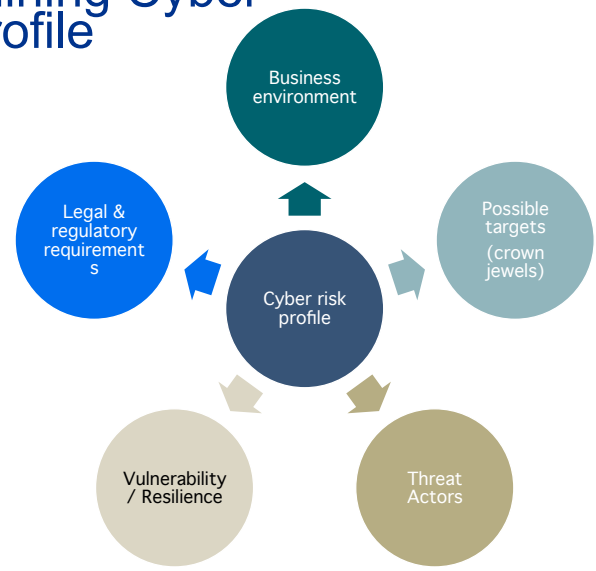
**IT limited the agenda of the supervisory board**

**IT knowledge / experience too low in most supervisory boards**

**Lack of common language (business risk vs IT security risk)**

**Lack of tailored cyber reporting – cyber risk quantification does not exist (yet)**

# Determining Cyber Risk Profile



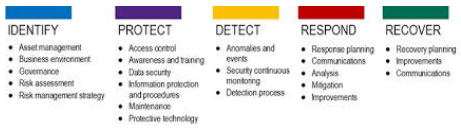




# Current maturity / capability models are based on proper risk management, however….

**NIST Cyber security framework** is getting more and more adopted

- For example - the European Central Bank is adopting a NIST-like model




**IRAM-2 – ISF model** – qualitative approac

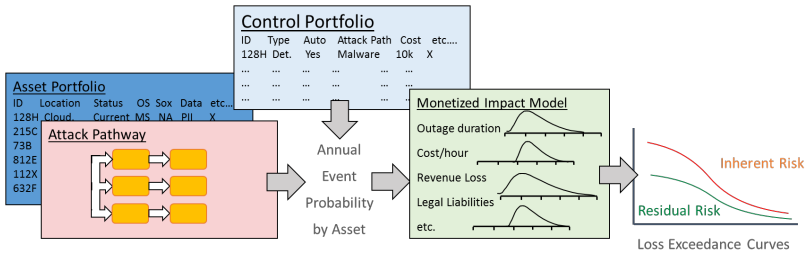
- Difficult to understand the financial imp decisions


**Strong focus on risk management**

- Risk-based decision management should steer level of investments, but how to calculate the final impact?

# Conceptual Overview of KPMG Hubbard Risk Quantification Model

- Attributes of the Assets and Attack Pathway are the basis for computing annual event probability for each asset.
- Controls reduce the probability and the impact of the event.
- The reduction in risk is represented as a reduced loss exceedance.
- The monetized risk reduction is compared to the control cost to compute Return on Control.








06/07/171

# To conclude

- Companies cannot ignore the cyber risk – it is here to stay
- Dealing with cyber risk must be a topic on the board agenda
- Board members need to be able to determine the cyber risk profile
- This cyber risk profile needs to steer investments in cyber security measures
- Early days for cyber risk quantification approaches that are really sound!

# John Hermans - Partner

**John Hermans**
Partner

KPMG Advisory N.V.
Laan van Langerhuize 1
1186DS Amstelveen

Hermans.john@kpmg.nl

**Function and specialization**
- Cyber Security Lead Partner, Advisory KPMG The Netherlands
- EMA Cyber Security Lead Partner and Member of KPMG global Cyber Security leadership

**Education, licenses and certifications**
- Bachelor degree in Information Management
- Executive Master of IT Audtiing (MSc) - Certifications as chartered IT auditor (RE).

**Background**
John is partner of the Amstelveen practice of KPMG IT Advisory and member of KPMG's Global Leadership on Cyber Security. In his current position he is heading the Cyber Security Services of KPMG in the Netherlands and, covering the following services:
- Security Strategy Services / Cyber Security In the Board Room
- IT Governance, Risk and Compliance
- Technical Security Services
- Cyber Security Services
- Identity & Access Management
- Business Continuity Services
- Data Privacy Services

Furthermore, John is leading KPMG's Strategic Growth Initiative on Cyber Security services within the Netherlands as well in Europe, Middle East and Africa, and member of KPMG's global Cyber Security Leadership.

**Professional experience**
John worked for numerous International and National organisations in most industry sectors, such as Financial Services, Oil & Gas, Retail and Government and is considered as one of the leaders in his field of expertise. John was involved in more than 100 national and international information security projects across the world. John's major involvements were in advising and supporting our clients in developing, defining and implementing their overall Information Security strategy, building the required business cases for Executive Boards as well as Supervisory Boards, and performing multiple program management activities as well as executing quality assurance assignments.

Next to being involved in many information security and cyber security programs and projects, John is involved in multiple Cloud Computing projects in both the private and public sector. John's major involvements relate to advising and supporting our clients in developing, defining and implementing their cloud computing strategy as well as advising on cloud security/assurance advisory topics.

**Industry experience**
- Financials Services: Insurance, Mortgages and Banking
- Oil & Gas
- Telecommunications
- Government
- Health Technologies