

EUROPEAN RISK
MANAGEMENT
SEMINAR 2018
CYBER



FERMA[™]

Federation of European
Risk Management Associations

INTRODUCTION

Not long ago, it seemed like we could be heading for cybergeddon; the forecasts about the threats from cyber space posed such a threat to the digital revolution. Today, as this report illustrates, we are finding a way to make cyber risk manageable, quantifiable and insurable.

In this report, you will find more information on two new reports that FERMA has introduced so risk managers can support their organisations in managing cyber risks. One is a second edition of the cyber risk governance guide that we have published in cooperation with the internal auditors in ECIIA, following the first edition in 2017. It includes a case study from the Education Testing Service (ETS), an organisation that works with partners worldwide, showing how the risk governance scheme we recommend works in practice.

Second, we have a completely new guide, Preparing for Cyber Insurance, which we have developed with Insurance Europe, the intermediaries' organisation BIPAR and two of our strategic partners among the brokers. It was written with mid-market organisations in mind, but it is certainly useful for others as well in their conversation with the insurance market about insuring cyber risks.

As our organisations increasingly rely on digital technologies for their operations and development, FERMA continues to push for the management of cyber risks beyond the limited technical/security dimension of this technological revolution. Risk and insurance managers play an essential part in the enterprise-wide coordination needed for the governance of cyber risks, its quantification and mitigation. The articles which follow show how risk managers can accompany their organisations in securing cyber resilience and making the best of the huge opportunities linked to digitalisation.

Jo Willaert, President of FERMA

CONTENTS

PAGE	
1-2	Cyber risks key learning
3-6	Cyber risk governance report
7-8	Case study: Risk governance
9-10	Workshop session: Preparing for cyber insurance
11-12	Cyber attacks: Applying lessons learned – Q&A: Tobias Bunz
13-14	Panel session: Cybergeddon or manageable risk?
15-16	Expert view: Julie Cain
17-18	Expert view: Laurent Bernat
19-20	Expert view: Nick Kitching
21-22	Workshop session: Applying lessons learned
23-24	Q&A: Augusto Perez
25-26	Lessons learned: Sebastian Bregning
27-28	Workshop session: Quantification of cyber risks
29-32	The importance of quantifying cyber risks – Q&A: Olivier Allaire
33-36	Europe's new normal: Philippe Cotellet
37	Speakers
38	Sponsors

October 2018

© Federation of European Risk Management Associations

This work is copyright. Apart from any use permitted under the Copyright Law of the European Union, no part may be reproduced by any process without prior written permission from the Federation of European Risk Management Associations (FERMA). www.ferma.eu

CYBER RISKS

KEY LEARNING

FERMA has made the ongoing digital transformation a priority for our advocacy work for several years now. This is why, in 2017, we launched one of the first European cyber risk governance models jointly with our European colleagues and internal auditors from the ECIIA.

Events since then have only strengthened our view that corporate governance models will quickly become obsolete if they do not embed governance for cyber risks under the leadership of a risk and insurance

professional. This new edition of the Cyber Risk Governance Report includes a case study that illustrates how our cyber risk governance model works in practice.

FERMA's ambition is to put forward the risk and insurance management profession as the one that is able to bridge the gaps between the new, key digital functions and the usual business operations. In that way, we work together to enhance our resilience to cyber incidents while we take advantage of the opportunities of digital technologies.



DEEP DIVE INTO CYBER INSURANCE

1. **Cybersecurity is a cross-functional issue:** most functions to be involved in preparing for a dialogue on cyber insurance with other market participants.
2. **Positive side-effect of preparing cyber underwriting information:** a virtuous exercise for risk management readiness.
3. **Identify the critical cyber coverage:** they can help you distinguish one offer from another.
4. **Work with their intermediaries and insurers:**
 - To understand potential cyber coverages and gaps in current insurance policies
 - To evaluate the value of a stand-alone cyber insurance.

QUANTIFICATION OF CYBER RISKS

1. **The scenario exercise** works better if led by the Risk Manager.
2. **Both business and IT people** must be involved, as well as finance.
3. **The senior management** must sponsor the exercise, so all the key people with the know-how will participate.
4. **Checklist** for a successful cyber incident scenario exercise:
 - Rely on the company's business model.
 - Assess the exposure per scenario.
 - Assess the exposure along the timeframe.
 - Rely on the company's functional organisation.
 - Define the threshold and limits.
 - Use gross figures.

APPLYING LESSONS LEARNED

1. **Collaboration, transparency and resilience** are key for dealing with cyber risks.
2. **Good communication** between technical and non-technical teams within the business is essential.
3. When there is an incident, **engage** with key stakeholders, such as clients, vendors and regulators.
4. Being **transparent** gains understanding from clients and helps to motivate employees to find solutions for clients and keep the business going.
5. Attacks never turn out as expected. They test **resilience**. Learn and understand different frameworks.

CYBER

RISK GOVERNANCE NEW EDITION

Beyond the IT domain, cybersecurity is a matter of corporate governance. This aspect of cybersecurity, however, has not been fully explored by European legislation. The European Confederation of Institutes of Internal Auditing (ECIIA) and the Federation of European Risk Management Associations (FERMA), therefore, set up a joint working group of risk managers and internal auditors to provide guidance on the governance of cyber risk.

FERMA has now published a second edition of its cyber risk governance guide to include a case study from the Education Testing Service (ETS), an organisation that works with partners worldwide. It shows how the risk governance scheme recommended by the report works in practice. The guide, *At the Junction of Corporate Governance and Cyber Risk Governance*, is published in cooperation with the ECIIA. The first edition was released in 2017.

This document contains recommendations for a cyber governance model that will benefit European organisations – public and private – in managing their exposures to cyber risks. This is particularly relevant following implementation of the two major EU laws, the Network and Information Security (NIS) Directive and the General Data Protection Regulation (GDPR).

ECIIA and FERMA advocate that organisations establish a cyber risk governance system, supported by a cyber risk management framework. It must go beyond the implementation of IT measures, in order to efficiently protect their assets and ensure their resilience and continuity. The model is anchored in two strong sets of principles: the eight principles set out in the OECD recommendation on Digital Security Risk Management (2015) and the Three Lines of Defence model, recognised as a standard of Enterprise Risk Management (ERM).

To respond appropriately to cyber risks, FERMA and ECIIA believe that the leadership of an organisation needs to know with accuracy its level of exposure to cyber threats, expressed in financial terms. These exposures, discussed and accepted across functions, are the starting point for decisions on concrete plans to reduce or avoid the most significant cyber risks, in accordance with the organisation's risk appetite.

The proposed cyber risk governance model argues for the creation of **a dedicated Cyber Risk Governance Group** (the "Group") whose mission is to determine cyber risk exposures in financial terms and design possible mitigation plans. The Group reports to the Risk Committee.

Chaired by the Risk Manager, the Cyber Risk Governance Group brings together

operational functions from the first line of defence, including IT, and key functions from the second line of defence, notably the Chief Information Security Officer (CISO) and the Data Protection Officer (DPO). This cross-disciplinary group has the subject and organisational knowledge to establish what cyber risks would be the most harmful for the organisation and determine suitable responses.

The Group presents senior leadership with possible mitigation plans, including investments in security and risk transfer solutions such as cyber insurance. To ensure continuous improvement of these plans, cooperation between the Group and Internal Audit ensures that they are auditable "by design". Internal Audit will independently review the efficiency of the cyber controls, risks and governance processes implemented.

//

Cyber risks are like unpredictable storms of ever growing severity; nothing is stronger to weather them sustainably than a proactive alliance between anticipative risk management and farsseeing internal audit.

//

Carlos Ghosn
Chairman and CEO of Renault-Nissan
Mitsubishi Alliance



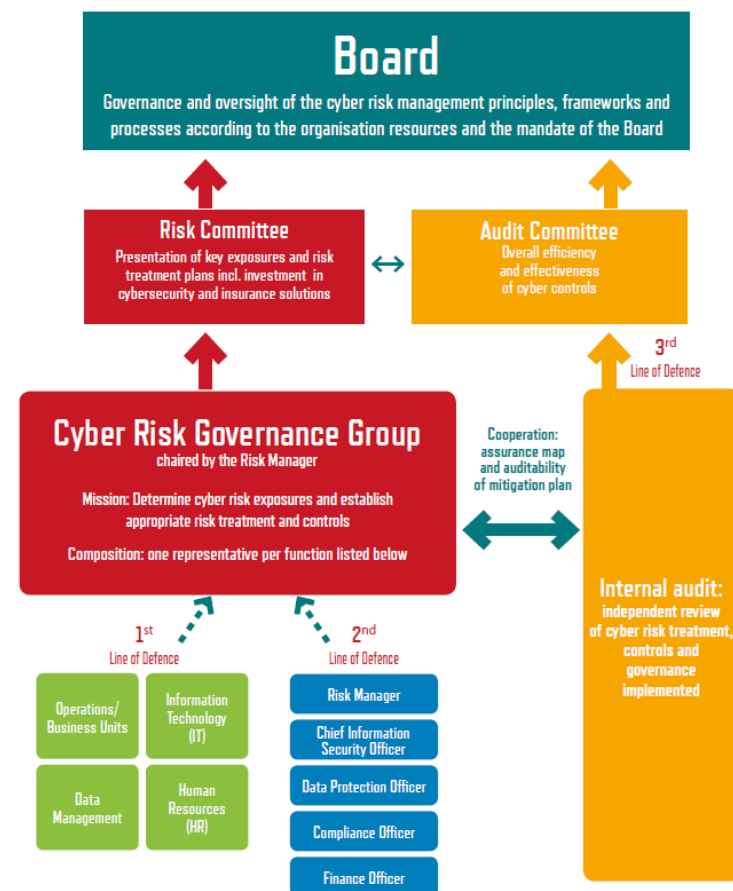
The Risk Committee, as a board committee, is responsible for enterprise risks and reviews the cyber risk assessments performed by the Group. The Audit Committee independently reviews the audit of the cyber risk governance system performed by the Internal Audit function.

This proposed cyber risk governance model constitutes an innovative way to

approach cyber security. It will allow the Board of Directors to demonstrate that cyber risks management is based on a rational and documented analysis of the risks across the organisation.

For more information on Cyber Risk Governance, download the [full report](#).

CYBER RISK GOVERNANCE FRAMEWORK



A dedicated Cyber Risk Governance Group

CASE STUDY

RISK GOVERNANCE



Julie Cain,
Senior Strategic Risk
Advisor Information
and Technology
Risk Management,
Educational
Testing Service

Within the organisation, alignment of accountabilities for decision making and resource prioritisation results in process efficiencies and enhanced control effectiveness.

Company snapshot:

Our mission is to advance quality and equity in education by providing fair and valid assessments, research, and related services. Our products and services measure knowledge and skills, promote learning and performance, and support education and professional development for all people worldwide.

Together with an extensive network of global partners, we operate and maintain a large number of complex and data-intensive IT systems under a variety of global legal and regulatory requirements while facing relentless and increasingly sophisticated cyber threats to confidentiality, integrity, availability of systems and data.

Security ecosystem:

ETS maintains dedicated functions and staff with responsibility for information security, physical security and test security, as well as disaster recovery/business continuity, privacy and internal audit. These organisations communicate and collaborate via a corporate-level Security

Implementing a cyber risk governance scheme is possible and has already been done as shown by ETS, a US-based not profit organisation. Cybersecurity issues are global and shared similarly across regions, thus a similar approach could be implemented anywhere in the world. The cyber risk governance scheme will always be perceived positively in a regulated sector. However, if the sector is not regulated, it still sends a positive signal to investors, authorities and the general public.



Steering Committee, led by our Chief Information Security Officer and comprised of the leaders responsible for each function.

The Security Steering Committee defines security policy, determines risk exposures and mitigating controls, proposes, prioritises and provides oversight of significant security initiatives and capital investments, and collaboratively responds to and reports on complex incidents.

Evolution of our approach:

Initially, the functions operated independently and reacted to only their own challenges and opportunities. Over time, technology innovations necessitated collaborative incident management and joint projects, which lead to more proactive risk identification and mitigating controls, then to true governance and executive decision support as guardrails for business innovation and value creation.

Over time, technology innovations necessitated collaborate incident management and joint projects.



PREPARING FOR CYBER INSURANCE WORKSHOP



Q) "Questionnaires often aren't specific. A simple Yes/No answer simply doesn't fulfil the requirements. How did the report overcome this?"
(from a Risk Manager from Germany).

A Nils Hellberg, GDV: We try to give you assistance within the report on cyber insurance because we didn't want to put in a variety of questionnaires and possible answers. Instead, we formed 7 blocks of information so that the company searching for cyber insurance can get more clarity.



PREPARING FOR CYBER INSURANCE

Cyber risks can be challenging for insurers to cover due to the difficulty in quantifying risks that are constantly evolving and can spread rapidly worldwide. Similarly, organisations can find it hard to assess accurately their cyber security exposures and how best to use insurance to mitigate them.

To respond to these challenges, FERMA along with the two insurance associations Insurance Europe and BIPAR have published practical guidelines to help organisations evaluate the potential value of cyber risk insurance, in association with two of FERMA'S strategic partners: Marsh and Aon.

Preparing for Cyber Insurance is a joint effort by risk managers, insurers and intermediaries

"Insurance will not solve everything; it is only one element. It means people need to be aware of cyber insurance coverage and to get that right cover we must understand what is expected."

Philippe Cotellet, Airbus Defence & Space – Head of Insurance Risk Management

to help organisations effectively discuss their cyber insurance needs. Its aim is to support insurance buyers in selecting the insurance solutions that are the best adapted to their needs.

Part 1 of the report helps organisations prepare for the discussion with their intermediaries and insurers.

Part 2 of the report provides organisations with tools to help them evaluate cyber insurance offers and describes situations where cyber insurance could be useful.

For more information on Preparing for Cyber Insurance, download the [full report](#).

KEY PILLARS OF A CYBER INSURANCE POLICY

PREVENTION

- Pre-breach assessments
- Access to pre-vetted vendors
- Cybersecurity information



ASSISTANCE

- Forensic investigators
- Legal services
- Notification
- Credit monitoring
- Call centre services
- Crisis management / public relations



OPERATIONS

- Costs incurred to keep or return the business to operational
- Loss of revenue, income, turnover
- Costs incurred to recreate / restore data and information



LIABILITY

Legal costs and damages from claims alleging privacy breach or network security failure



"We often say in cyber security the human factor is the biggest threat. I want it to be the biggest weapon if they are trained properly."

Jean Bayon De la Tour, Marsh

Q&A

Cyber attacks: Applying Lessons Learned -
a Q&A with Tobias Bunz



Tobias Bunz,
Expert Group
Insurance, E.ON

We caught up with Tobias Bunz, E.ON's Expert Group Insurance to find out why underwriting cyber risk insurance is so challenging and get his insight on two high profile cyber attacks in 2017 that were discussed at the FERMA Seminar. Tobias was a member of the FERMA working group that produced the report *Preparing for Cyber Insurance* and the moderator at the Seminar workshop "Applying lessons learned."

Tobias' workshop looked at the cases of Maersk and Telefonica in order to apply learnings from their own experiences of cyber attacks last year. Now that his workshop is complete, we asked Tobias for his summary of some of the workshop's hot topics.

How challenging is the underwriting process for cyber insurance for a company today?

I would say very challenging for the following reasons:

First of all, we have to be aware that insurers assess the cyber risks of the insured carefully. However, there is no standardised underwriting process within Europe. As such,

there are no standard rules for calculating the premium and there are only rough indicators such as those which are written by national authorities. So, insurers usually rely on underwriting questionnaires to get an overview of the IT profile of the company and its cyber risk management readiness. In addition to that, the dialogue on cyber insurance remains based on a high level of trust and good faith, so that personal relationships also play an important role. Although there are different standards within Europe, we have the need for standardised objectives and criteria on the one hand, and on the other hand, we have to find a way to deal with the influence of subjectivity.

As we see increases in the number of cyber attacks, how will the FERMA document, *Preparing for Cyber Insurance*, provide insight and guidance into understanding and managing cyber attacks?

This document supports the reader to be better prepared for the cyber underwriting process, however the client also has to reflect critically on its IT security measures and its organisation. The document allows the client to acknowledge potential threats in terms of its organisation, alongside their preparation and efficiency for cyber attacks. We wanted to avoid simply repeating the existing criteria and questionnaire. We wished to demonstrate why this information is valuable for us, and the client.



Could the enhanced insight have helped Telefonica and Maersk ahead of and during their cyber attacks?

I would assume that as multi-national companies they already possess a very good standard of cyber security. Nevertheless, I think they could have benefitted from several propositions. We must remember that it is impossible for 100% cyber efficiency to exist, otherwise we wouldn't need to consider the underwriting process for cyber insurance. As we talk about insurance, we have to keep in mind that insurance is a kind of annex to technical matters which are developed and prepared, but on the other hand, this also reflects the situation of the client and that 100% cyber security isn't possible and that cyber risks are not stable.

What link would you make between the report and the lessons learned from these two specific cases?

The report itself has been influenced by Telefonica's lessons learned process, hence the reader will surely profit from the valuable measures and information which has been derived from the incident. Although the document focuses on the middle market, and Telefonica and Maersk are large companies, the information and lessons are consistent.

CYBERGEDDON OR MANAGEABLE RISK?

PANEL SESSION SPEAKERS:

The accelerating worldwide trend of digitisation represents a key business opportunity for European organisations, but also brings key business risks. With recent cyber attacks increasing concerns on what risk experts see as a wider lack of focus on risk governance in cyber security, how can companies in Europe meet their obligations under EU regulations?

Jointly with the European Confederation of Institutes of Internal Auditing (ECIIA), FERMA set up a working group of risk managers and internal auditors to produce our cyber risk governance model. Similarly, the CRO Forum recently published their methodology on supporting the on-going capture and sharing of digital event data, through a common language.

The 'Cybergeddon or Manageable Risk' panel session moderated by Philippe Cotelte, Head of Insurance & Risk Management - Airbus Defence & Space focused these methodologies and explained their real-life value.



Julie Cain

Senior Strategic Advisor, Information & Technology Risk Management, ETS (Educational Testing Service)

Julie presented the case study for ETS that illustrates how FERMA's cyber risk governance model can work in practice.



Laurent Bernat

Policy Analyst, OECD

Laurent spoke about the OECD / FERMA collaboration, with particular focus on the joint pilot survey conducted with our 13 volunteering associations to establish international statistical indicators to measure digital risk management in businesses.



Nick Kitching

Chief Risk Officer, Swiss Re

Nick discussed the CRO Forum's proposed categorisation methodology for capturing digital risk events.



Julie Cain
Senior Strategic Risk Advisor
Technology Risk Management,
ETS

The difference here is that it's evolved into something that's expected; it's institutionalised.

EXPERT VIEW

with Julie Cain

As the cyber risk governance model is a new concept, how do you see the model developing in the future and how can risk managers prepare for this?

I think that people have been focused conceptually on the idea of cyber risk and cyber risk governance for a while. I believe what's changed, both as discussed in the FERMA-ECIIA report and by companies independently, is that it's necessary to work across silos in a way that is different. Cyber used to be the purview of the IT department and they would work with risk managers when it was necessary for them to do so. The difference here is that it's evolved into something that's expected; it's institutionalised. It has the mandate from senior leadership and the board that all who look after the various risk functions need to work together continuously to understand cyber risk in the context of rapidly changing business and provide the board with the information they to make decisions to dynamically manage that risk. I believe that, because of this, both conversation and collaboration will become more important and the cyber risk governance model provides a solid framework to help companies achieve this.



How can risk managers develop their understanding and treat cyber not as a standalone subject?

For years, ETS, as a paper-based, location-based business, thought of physical security, test security, information security, privacy, audit, and insurance as very separate and distinct functions. They're not anymore. They can't be. Everything is technology enabled. Everything is online and connected, everything is digital. I think people generally understand what that means for a business but for cyber risk governance it really is a paradigm shift.

We often hear people say that we need to 'break down silos'. It's revolutionary and especially as a risk manager it can be a bit scary. Each risk function has a unique perspective and expertise and we need them all to be successful in managing cyber risk for our companies. If you can have in your mind that you're reaching across and bringing people towards you for a common purpose rather than breaking down something that seems destructive and confrontational, that may help to gain some confidence and get over any reluctance to get started.

What were the key aims for risk managers attending your session?

I would hope that risk managers took away from our session the confidence to take cyber risk governance forward in their own company. Don't be afraid to start small or think it has to all fall into place and be perfectly structured before you begin. Take a look at the report and the model and think of just one collaborative structure or opportunity already in place in your company and build on that. Take your CISO or Head of Security to lunch and find ways that you can support each other.

Everything is technology enabled. Everything is digital. I think people understand that, they get that intently, but to help them understand what that means for a governance structure really is a paradigm shift.

EXPERT VIEW

with Laurent Bernat



Laurent Bernat,
Policy Analyst,
OECD

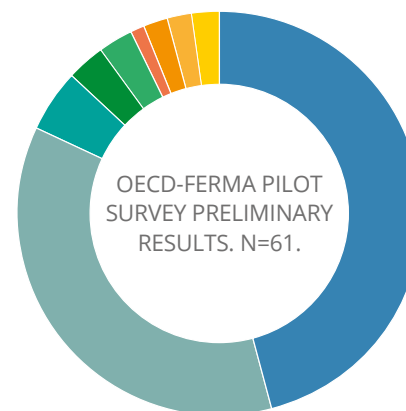
Can you tell us more about the OECD perspective on cyber security? How has this evolved and how will this develop?

A number of additional challenges will emerge because the technology cycles are very, very short. We have things like the internet of things, artificial intelligence, blockchain and other trends which aren't yet known. These make us rethink our approach and it is hard to predict where this will go. But, fundamentally, I would say it is the idea that digital security is not different from other risks when it comes to how you manage it in an organisation. I do not see that changing but there is still a lot of work to do to get all people in organisations to understand this and act accordingly.

How can risk managers be better prepared?

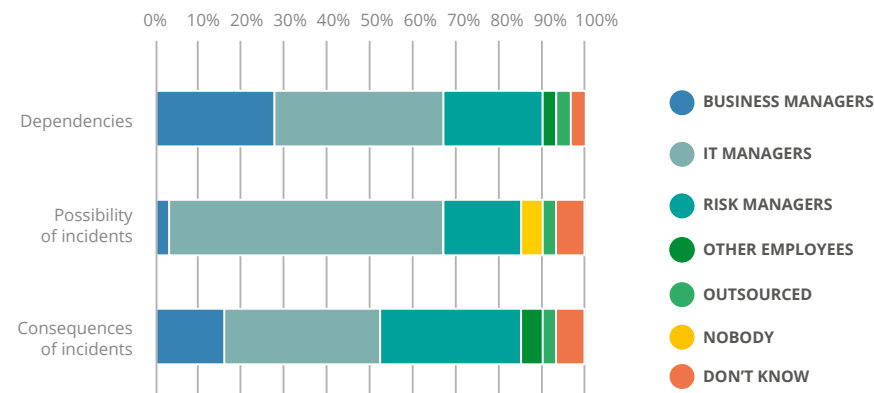
I would say those who have a more advanced knowledge and have started to do something practical have a lot to learn from the governance work by FERMA - rather than trying to invent something fundamentally new and specific to cyber. It's a great report - we have used it. It is based on our recommendations (partly), and there are great synergies. I think the FERMA Seminar is a great event because the workshop gives the opportunity to think collectively about aspects that are difficult to follow and understand.

WHO IS IN CHARGE OF MANAGING DIGITAL SECURITY RISK OF THE ENTERPRISE?



- 46% CHIEF INFORMATION OFFICER (CIO) OR IT MANAGER
- 36% CHIEF INFORMATION SECURITY OFFICER (CISO)
- 5% RISK MANAGER
- 3% CHIEF EXECUTIVE OFFICER (CEO)
- 3% CHIEF SECURITY OFFICER (CSO)
- 1% CFO+CIO+EVP INSURANCE
- 2% ISO: INFORMATION SECURITY OFFICER
- 2% MULTIPLE PEOPLE, DIFFERENT BUSINESS UNITS, NO ONE PERSON OVERALL
- 2% OTHER PERSONS EMPLOYED THAT ARE NOT IN MANAGEMENT POSITION

WHO CARRIES OUT THE FOLLOWING ACTIVITIES AS PART OF DIGITAL SECURITY RISK ASSESSMENT FOR YOUR ENTERPRISE?



I think the FERMA Seminar is a great event because the workshop gives the opportunity to think collectively about aspects that are difficult to follow and understand.

EXPERT VIEW

with Nick Kitching



Nick Kitching,
Chief Risk Officer,
Swiss Re

The session produced discussion around **taxonomy, a common language, to which Nick provided the following answers to pressing queries:**

How does the taxonomy affect risk management in a non-insurance company and what is its benefit for those functions?

Well, taxonomy is a way of allowing different languages to communicate in one common form, so different specialists within an organisation can come together around a common description of an event. Therefore, your information specialists, your security specialists, your insurance buyer, the risk manager and production/ process can all explain when a digital event happens in a common way that can then be collected over time. It's a bit like when you are driving a car. How well do you drive? Are there points on your license? You know how good you are. Therefore you can buy insurance or work out what you need to spend money on.

Were there interesting insights coming from the few hundred incidents captured in the last round of the trial that you can carry on or an area that needs to develop a bit of a better understanding?

The biggest learning is to get everyone around the table to want to discuss and engage on it. People want to understand the benefits, but it is an investment of time, and people need to realise that we cannot do it immediately. It took a long time, but that is what we need and we need people to engage on it.

Would the insurers have a more positive evaluation of cyber risks for companies having a governance model in place?

The new publication that FERMA has just released sets out seven areas that you need to evaluate in order to work out as an insured how you can buy insurance. I wasn't privy to that publication, but the taxonomy will give you the underlying data. By using taxonomy internally in those seven areas, when you come to buy insurance, you will have a better understanding. Therefore by definition the market starts to improve.

What do you think is the one key takeaway for risk managers from the Seminar?

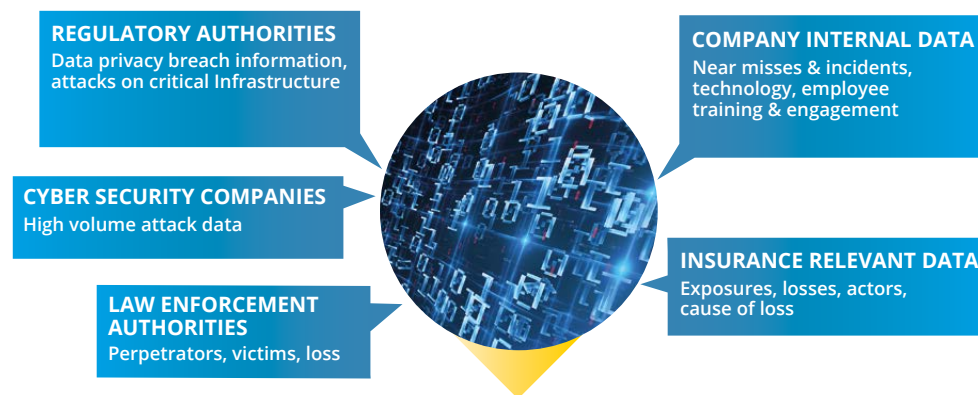
Help... build... common... communication.



Q) "Any common pitfalls from the communications side - areas of misunderstanding that we can learn from as risk managers?"
(from a Risk Manager from England).

A Nick: There is one which I can highlight, and that is the interaction between different functions. The IT specialists can understand the root cause of a cyber event, but this presents a challenge for the risk manager or insurer to get data. We need one common goal of a baseline description of detail that everyone can understand and work from.

FINDING A COMMON LANGUAGE BETWEEN STAKEHOLDERS



1-5 DIGITAL EVENT	6 EVENT TYPE	7 ROOT CAUSE	8-13 IMPACT / COVER
- Leveraging VERIS / STIX definitions - Capture: - Incident type (<i>technical impact</i>) - Asset - Affected kind of data - Actor	- Identifies what happened - Existing op risk framework	- Specifies why the cyber event occurred - Existing op risk framework	- Business impact based on RMS/AIR schema (22 types) - Financial impact - Date of detection - Impact location
IT FOCUSED	OPERATIONAL RISK FOCUSED	UNDERWRITING FOCUSED	

Source: Supporting on-going capture and sharing of digital event data.
CRO Forum. February 2018

WORKSHOP

A HISTORY OF TWO ATTACKS

Sharing their real-life experiences of large-scale cyber attacks, Maersk and Telefonica outlined the way in which they managed the crisis and the lessons learned from the attacks on their companies in 2017.

The workshop, moderated by Tobias Bunz, gave delegates the chance to understand how to –

- Engage with key business partners – including regulators, customers and vendors, and coordinate with non-technical teams within the business, such as HR, legal and operations, as well as the senior management team.
- Anticipate future events with the right governance and processes to improve the ability of the business to respond.
- Embed insurance within the overall cyber crisis management.

NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Process and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

Source: US Department of Commerce. 2018



Augusto Perez, Director of Corporate Risk and Insurance at Telefonica, explained to the Workshop how Telefonica applies a cyber resilience methodology underpinned by five key pillars – identify, protect, detect, respond and recover. During the attack by WannaCry in May 2017, Telefonica decided to communicate quickly and regularly with the Spanish security and cyber authorities and its business customers. It was also able to share its experiences with other corporate customers that had also been impacted by the attack.



Q) “What did you do after the attacks to strengthen your prevention systems?”
(from a Risk Manager from Germany).

A Augusto: Some of the pillars are prevention-focused. We concentrated on the timing of reactions and how to escalate them, and the importance of putting systems in place rather than patching.

WORKSHOP



Augusto Perez
*Director of Corporate Risk
and Insurance, Telefonica*

Q&A

Do you think risk managers have a greater understanding of the measures needed to both prevent and deal with an attack due to organisations sharing stories like yours and Maersk's?

Yes, I totally believe all these events are in the end a way of extracting conclusions and taking lessons for the risk management community - I totally believe they have learned quite a lot not only from the lessons that we and Maersk have explained but also many of them have researched what really was the problem with Wannacry. They have used this as a case to do their own test scenario for future events, and they are going to learn a lot of things.

Do you think that each of the five pillars of cyber methodology have equal weighting? Or are some more important than others?

Each organisation has to decide what is the right balance, in order to make the decision alongside collaboration with the risk managers and the other departments such as compliance is, CISO, CTO, legal and so on. It is not the same for every type

of organisation. It depends, on the specific sector or activity where you have to put more effort, but what is clear is that you should take into account these five pillars in a broader sense and have in mind that 100% security doesn't exist. Prevention is not the only pillar, so it is not worth it to only invest in prevention - you have to understand that sooner or later you are going to have a cyber incident. The only uncertainty is "when". Therefore, you have to plan what happens after. This means how to detect, react (which includes communication) and recover.

Do you think that organisations are sometimes more worried about the reputational damage of sharing their stories of cyber attacks than holding back the learnings that the rest of the industry needs?

Definitely, this is one of the big concerns of cyber risks. It is clear finally that a cyber event like this can have much more reputational impact than property damage or casualty claims. It always has much more media impact in the beginning - because there is some kind of common misunderstanding of the risk- but we have

to educate the people, the media and the public authorities that this transparency is needed. We shouldn't penalise or punish in excess the companies who finally decide to communicate and be transparent with the learning in order to help others to face a similar problem. Then we should educate general opinion to reward those companies that share and disclose in parallel with the responsibility requirements.

What is the underlying message you would like risk managers to take away?

We have been talking about how collaboration, transparency and resilience are key for these kind of risks. Risk managers can play an important role in spreading and transmitting the message to the rest of the organisation. They typically are not the expert to implement the 5 pillars (CISO, legal, communication, each have their role), but the message is there to be spread to do the right governance of cyber risks.

LESSONS LEARNED

with Sebastian Bregning

Sebastian Bregning, Head of Captive Operations and Risk Analytics at AP Moller – Maersk, shared his experience of managing and responding to a large scale attack and the lessons that Maersk has learned to make it better prepared for the future.

THE CYBER ATTACK THE IMPACT



ON 27 JUNE 2017, A. P. MOLLER - Maersk, among many global companies, were hit by the Malware Notpetya.



49,000
LAPTOPS INFECTED



ALL
PRINT CAPABILITY
INACCESSIBLE



1,200
APPLICATIONS WERE
INACCESSIBLE



1,000
APPLICATIONS WERE
DESTROYED



FILE SHARES
UNAVAILABLE



THE VALUE OF TRANSPARENCY

Being transparent gains understanding from clients and helps to motivate efforts from the employees to find solutions to keep the business going. Maersk COO/ CEO did public interviews on CNN to help amplify the learning.

We as risk managers try to have frameworks/protocols, but when an attack comes it tests our resilience, and it never turns out as expected, so we can best prepare and learn by understanding other frameworks.



OOPS,
YOUR IMPORTANT
FILES ARE ENCRYPTED

THE ROOT CAUSE

The default software for submitting tax returns in Ukraine is called MeDoc.

The software company that produces this was compromised and 'back doors' were put into the product giving the 'hackers' access to all companies that used the software – including Maersk.

The software automatically updates itself and in the June update it pulled the virus into our network.

Once on our network, it looks to move from system to system, but it can not jump from one network to the other, meaning our customers and partners that connect to us remained safe.

REFLECTIONS & LESSONS LEARNED

Integrate crisis management, business continuity management, ERM and insurance

<i>Crisis Management</i>	• Competences • Communication • Resources available
<i>Business Continuity Governance</i>	• Tested recovery plans • CISO, CIO and internal audit
<i>Risk Identification</i>	• Risk quantification • Frequency, severity and impact
<i>Risk Mitigation</i>	• Segregation of risk • Risk culture • Risk transfer
<i>Risk Reporting</i>	• Risk owners • Action plans • Key risk indicators



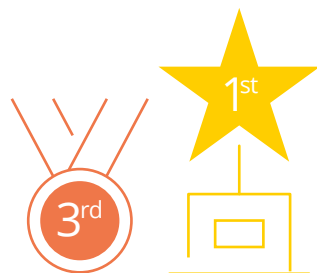
Q) "What would have made your lives easier with national / international authorities? What was the response of the global business?"
(from a Risk Manager from England).

A Sebastian: *Collaboration was key to dealing with them, alerting the forces as quickly as possible and exchanging information with them instantly to make life easier. The authorities are there not just to use communication just to punish or fine people as that only limits collaboration.*

After the observations from Augusto and Sebastian, delegates involved themselves in an energetic roundtable discussion, using a 'catch box', looking at – actors and responsibilities, governance and processes, insurance, the role of the risk manager and the vision for the future.

QUANTIFICATION OF CYBER RISKS WORKSHOP

FERMA EUROPEAN RISK MANAGER SURVEY 2018

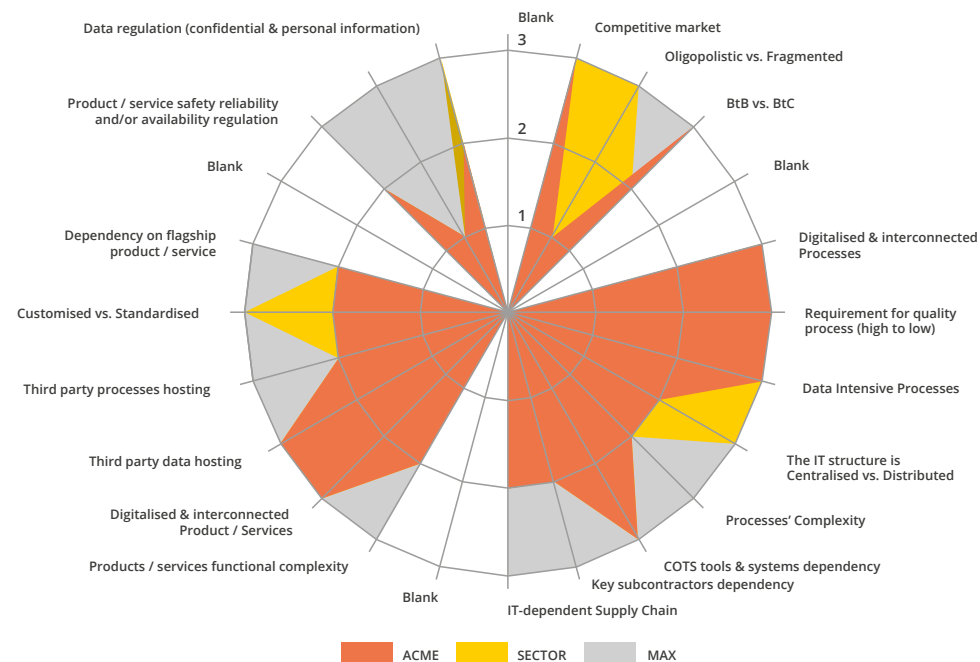


The interactions between the risk managers and the IT department are notably increasing since the 2016 survey from the third rank to the first one.

WHAT PARTICIPANTS LEARNED

- In the example used in the workshop, breach of personal data did not have an impact. However, in reality it will depend on factors such as the number of notifications required and the duration of the breach.
- By contrast, a cyber attack targeting the security of products, especially if the business requires authorisation to produce them, is likely to be significantly more extensive and expensive.
- It is possible to quantify the potential impact of a major cyber attack and identify cost-effective mitigation measures.
- The business costs are likely to be significantly greater than the technical IT costs.
- The number of catastrophe level cyber risks that need such analysis will be small.

CYBER EXPOSURE SCENARIO: ACME LOGISTICS



Source: Olivier Allaire, Lineon

CHECKLIST FOR A SUCCESSFUL CYBER INCIDENT SCENARIO EXERCISE



- Rely on the company's business model
- Assess the exposure per scenario
- Assess the exposure along the timeframe
- Rely on the company's functional organisation
- Define the threshold and limits
- Use gross figures

Q&A

The importance of
quantifying cyber risks –
a Q&A with Olivier Allaire



Olivier Allaire,
Founder & Managing
Director, Lineon

Olivier Allaire, Founder & Managing Director of Lineon, spoke at our 'Quantification of cyber risks' session.

He shared his thoughts on managing the frequency and impact of cyber claims and the importance for risk managers to understand how to quantify cyber risks.

The number of cyber claims seems to be increasing, as well as the costs. Should it continue, do you think companies really understand the likely impact of this trend on their business?

Many companies have yet to fully understand what it means to be exposed as a business to cyber risk - they approach cyber risk from a technical point of view, rather than a business one.

Companies tend to look at high-impact cyber risks such as a malware attack from a technical perspective and adopt fancy measures to protect themselves in order to reduce the probability of an attack - but do they also assess the potential business implications?

From a business perspective, you need to understand what could occur and why people might target you. Will production be interrupted? Will you lose the ability to keep track of orders from customers? There will be a huge impact. If you can assess this type of cyber risk from a business point of view, you can translate the cyber risk impact into cyber insurance quantification. This will provide the insight needed to work out how to avoid or reduce the risk and focus on the right protection and impact reduction - which I believe will reduce claims in the future.

Continued next page >



To summarise, businesses need to improve their understanding of how a cyber attack can affect all aspects of their business in order to translate the risk into financial quantification and plan the most effective ways to prevent a high-impact attack.

With the market suggesting that the frequency and severity of cyber claims will continue to increase in the next 10 years, how do you suggest companies manage these across their entire business and workforce? Does there need to be a change in thinking to cater for this increased threat? Have you any guidance in terms of calculating the financial impact?

There are two very different parts to this question - frequency and impact.

To tackle frequency – it is necessary to upgrade your protection to avoid ‘internet pollution’ to prevent an attack reaching the business. In my opinion, this is the best way to reduce frequency. You can make an attack ineffective, but if someone really wants to attack you, they can do it anytime they want - and it is very hard to avoid.

It is easier to take action to reduce the impact. You can define where the impact lies and how much it will cost to you if the attack reaches completion. You are then able to put in place protection, detection, response and recovery measures to tackle a small part of the frequency and a large part of the impact.

You use the phrase ‘internet pollution’. How would you describe this?

Internet pollution refers to all attacks that have been made by a specialised group of attackers that try to target unprotected devices. Anything that is connected to the internet without the proper protection is open to an automated attack – especially in a business scenario where employees have access to targetable devices on which they could help the attacker to go deeper into your network.

10% SUCCESSFUL ATTACK

Infected link emailed to 1,000 users. On average, at least 100 users will click on the infected link and activate the malware.

Other automated attacks physically target the user – for example, an email containing malware which is activated when clicked. The most efficient attack is an attack that targets a user, with some attackers using specific email templates for dedicated sets of companies in order to appear legitimate and encourage clicks. Let’s say they send this email to 1,000 users. On average, at least 100 users will click on the infected link and activate the malware.

The only way to reduce the frequency of these types of attack is to raise the awareness of the threat and the resulting impact.

The change in thinking required, therefore, is the need to invest where necessary in automated devices to respond to this internet pollution, and the need to educate members of staff.

Companies need to be a lot better at advising staff on these threats and what to look for. Sophisticated phishing mails are difficult to detect, so education is the key element here and staff must adopt an air of caution before clicking on links in emails.

Organisations should also take measures to reduce the impact of malware spreading through a network once a user clicks.

Why do you feel it is important for risk managers to better understand how to quantify cyber risks?

Cyber risk is not a new risk. It’s a new way for business risk to happen and it is posing a bigger threat. In order to assess and reduce risk, you must first understand and accept it.

To gain a strong overview of all aspects relating to your company’s cyber risk, the first step is to identify how a business risk can occur through cyber means. It is important to assess how your cyber

exposure will evolve over time as your company uses more and more digital technologies and strategies. This will all contribute to a growth in your company’s cyber exposure, and so must be evaluated at regular intervals.

If you can assess this type of cyber risk from a business point of view, you can translate the cyber risk impact into cyber insurance quantification.

You also need to assess your cyber security maturity and benchmark your level against that of your competitors and business sector, and assess the potential impact of your cyber risk. It may be worthwhile to obtain an impact assessment from a cyber security company.

This process of developing a risk manager’s understanding of how to quantify cyber risks can help in upskilling and polishing communications between risk management and IT. Typically, IT plays a key role in any cyber-related issue, yet IT technicians do not take a business-focused approach to the tasks they undertake and to the wider picture. Meanwhile, risk managers are focused on the business outlook, but don’t tend to speak the language of IT. Integrating cyber risk management with IT processes ultimately results in long-term benefits.

WELCOME TO EUROPE'S NEW NORMAL CYBER RISKS

PHILIPPE COTELLE IS THE FERMA BOARD MEMBER WITH RESPONSIBILITY FOR POLICY ON CYBER RISKS AND HEAD OF INSURANCE RISK MANAGEMENT FOR AIRBUS DEFENCE AND SPACE.



With at least seven parliamentary elections scheduled for in the European Union in 2019, plus European Parliament elections, the continent's leaders are in a frenzy of damage control. The European Commission has launched initiatives to harden information technology infrastructure and fight fake news and it is organising a high-level conference in October on Election Interference in the Digital Age. Austria, which currently holds the Union's rotating presidency, hopes to reach political agreement with the Commission and European Parliament on a new EU Cybersecurity Act before the end of the year.

Judging by the evidence, these efforts are desperately necessary to ensure that Europe's elections and markets run smoothly. They are also possibly too late to ensure that they do so anytime soon. That means Europe needs to step up its efforts to mitigate damage even as it redoubles its efforts to mitigate cyber risks in the first place.

A US Senate report has already presented evidence that—despite heightened awareness after the 2016 elections in the United States and Brexit vote in the United Kingdom—Russia has interfered in at least 19 important elections or referendums in Europe, including national elections in France and Germany, in the past two years. The Netherlands last year took the unprecedented step of counting all the



ballots in its national election by hand because they couldn't be sure that their election systems were immune to tampering.

The private sector, for its part, is the subject of almost daily news of data breaches and malware attacks by hackers more intent on collecting ransom than interfering in elections. The Belgian national Centre for Cybersecurity says it blocks an average 3-4 phishing sites—often the starting point for a malware attack or data breach—per day. An Accenture survey of more than 4,000 executives published earlier this year found that most have improved security to the point that they can now thwart 87% of attacks—but that still leaves 13% that can cause massive damage. The Wannacry ransomware attack in 2017 affected more than 200,000 computers worldwide and

inflicted hundreds of millions of euros in damages—some say a billion.

In the absence of strong mitigation measures, the frequency of such successful attacks and the scale of the damage are likely to grow. That's because the 4th industrial revolution, the ongoing fusion of technologies and scientific disciplines sometimes called "cyber-physical systems", is only just getting started.

Breakthroughs in artificial intelligence, machine learning, data mining,

Continued next page >

CYBER-TERRORISM ELECTION INTERFERENCE DENIAL OF SERVICE ATTACKS FAKE NEWS HYPER-PARTISANSHIP RANSOMWARE



the Internet of Things, wireless technologies, 3D printing and autonomous vehicles all create a vast and growing buffet for hackers, state-sponsored or otherwise, as more and more systems interact with one another autonomously on a scale that makes those connections difficult or even impossible to really track individually. In effect, the more we digitise, the closer we get to Cybergeddon—unless we do something to stop it.

The starting point for any organisation to better mitigate such risks is better governance, starting by breaking down barriers between silos. Organisations of all

sizes need at least a working group of people representing security, audit, legal, finance, information technology, data privacy and human resources, chaired by a professional risk manager. Ideally this team should report to the CEO or another Board-level executive. These teams need not only to ensure that an organisation's software and systems meet the latest security and compliance standards but also regularly monitor operations and run fire drills to make sure people know what to do in the event of an attack—among other tasks. The Federation of European Risk Management Associations (FERMA) and the European Confederation of Institutes of Internal Auditing (ECIIA) earlier

this year published a handy how-to guide on improved cyber risk governance.

Once this is in place, then cyber insurance can efficiently help to cover residual risks. Munich Re, the reinsurance giant, says it expects companies to more than double budgets for cyber insurance by 2020.

The bad news is that Europe still has a long way to go. A 2017 UK government report found that more than two-thirds of FTSE 350 companies' boards had no training to deal with a Cyber attack, while one in 10 had no plan in place. Only one-third of respondents to a recent survey by the European Federation of Risk Management Associations, FERMA, said their organisations had any cyber insurance.

The good news is that national governments, the European Commission and European Parliament have already taken significant steps to improve Europe's cybersecurity structures and capabilities. After years of stringing the European cybersecurity agency, ENISA, along with temporary missions and budgets, they have now given it a clear and permanent mandate. Now they also need to finish the job by finalising the new EU Cybersecurity Act by the end of the year and giving it all the political and financial support that they can.

Next, Europe's leaders urgently need to begin promoting a general risk management

culture—for private companies and other organisations big and small—that gives Europeans the political, social and economic stability that they deserve.

This article was originally published on Euractiv.com on 10 October 2018.



SPEAKERS



Olivier Allaire,
Lineon, Founder &
Managing Director



Jean Bayon de la Tour,
Marsh Continental
Europe, Cyber
Development Leader



Laurent Bernat,
OECD, Policy Analyst
Digital Economy Division



Sebastian Bregning,
Maersk, Head of
Captive Operations
and Risk Analytics



Tobias Bunz,
E.ON, Expert Group
Insurance



Julie Cain,
ETS, Senior Strategic
Advisor Information
& Technology Risk
Management



Philippe Cotellet,
Airbus Defence & Space,
Head of Insurance &
Risk Management



Shannan Fort,
Aon, Product
Development



Nils Hellberg,
German Insurance
Association, Head of
Liability, Credit, Marine,
Aviation, Accident and
Legal Expenses Insurance,
Assistance, Statistics



Nick Kitching,
Swiss Re, Chief Risk
Officer



Augusto Perez,
Telefonica, Director
of Corporate Risk
and Insurance



Dirk Wegener,
Deutsche Bank AG,
Global Head of
Corporate Insurance

Thank you for your contribution to the 2018 FERMA Seminar. As a guest speaker and moderator, you played a significant role in the success of this well attended event.

SPONSORS

ACKNOWLEDGMENTS

The present report is based on the presentations and discussions during the Seminar as well as FERMA documentation. We thank Professor Jean-Paul Louisot, Docteur en Sciences de Gestion de la Sorbonne, for his additional contributions.





***Be the Risk Professional of the
21st Century
by joining a dynamic learning path***

FERMA RIMAP certification is unique because it provides:

1. an **independent** confirmation of your professional competences and experience
2. a **European** standard developed by European risk managers and recognised by FERMA's 22 risk management member associations
3. a **continuous dynamic learning path**: earn CPD (Continuous Professional Development) points by participating in FERMA licensed events

For more information about Rimap Certification click [here](#).

**It's now time to seize your opportunity to
become the 21st century Risk Manager!**



**Federation of European Risk
Management Associations**

Avenue de Tervuren 273 Tervurenlaan B12
1150 Brussels (BELGIUM)

T: +32 2 761 94 32

F: +32 2 771 87 20

E: enquiries@ferma.eu

ferma.eu