Conference report

The Federation of European Risk Management Associations (FERMA) and the European Confederation of European Institutes of Internal Auditing (ECIIA) launched their ground-breaking proposals on cyber risk governance to a packed audience at the European Parliament in Brussels on 29 June 2017. The host was MEP Antanas Guoga.

MEP Antanas Guoga opened the conference by explaining that citizens want to secure their private data as well as large multinational organisations want to secure their business secrets. In their representative role, politicians have therefore a critical role in Europe to speak out about the common interest for society to collaborate in order to increase trust and cyber resilience.

The event took place against the background of a second global ransomware attack, the so-called Petya, which followed the WannaCry attack in May. **FERMA President Jo Willaert** told the audience that these incidents illustrate how much we still need to prepare for cyber risks. He stated the principle at the heart of the report; "Risk management readiness for cyber risks can only be achieved within a strong governance framework and through a highly coordinated approach across all departments of an organisation."

"Cybersecurity had appeared for the 6th year consecutively as one of the top major risks of the company at Renault. Eventually, you cannot mitigate cybersecurity risk with only technical expertise, whatever competent and skilled it is. Because it is not a "mere" IT risk, but has wide and cross-functional implications; whether you measure those implications from the root causes dimension, or through the consequences dimension, it involves the whole organisation. Therefore, it needs a diversified set of expertise and disciplines, embarked in an adapted governance system" said **Farid Aractingi, Vice President ECIIA**

At the junction of corporate governance and cyber security calls for the creation of cyber risk governance groups, chaired by the risk manager, to operate across functions within the enterprise. The role of the group is to determine the potential cost of cyber risks, including catastrophic risk scenarios, across the whole organisation and propose mitigation measures to the risk committee and the board.

In addition to the risk manager, the group is to include representatives of all key functions at an enterprise level involved in digital risk, notably IT, human resources, communications, finance, legal and the data protection officer (DPO), and chief information security officer (CISO). Internal audit will provide the necessary independent assurance to the board/audit committee that the cyber risk controls are operating effectively and efficiently. They will collaborate with the cyber governance group extensively.

Jakub Boratyński, Head of Unit Cybersecurity & Digital Privacy, DG Connect, European Commission, welcomed the joint report saying*:* "I like it because it is simple. Anyone with a limited understanding can digest and understand it. It is a welcome development to see associations of professional groups investing their time in working together. This is essential for the discussion of the European digital single market project."

Philippe Cotelle, Head of Insurance and Risk Management at Airbus Defence & Space, was a member of the joint FERMA-ECIIA working group that produced the report. He said: "It will help boards take the right decisions in circumstances that have no precedent."

For **Rodney Naudi**, Head of Department - Governance, Risk & Compliance at the Malta Information Technology Agency (MITA), mitigations plans must be prepared, where business continuity is essential. When the risk materialize, the recovery plan must be implemented quickly and this is difficult for small businesses, citizens. The model proposed by ECIIA/FERMA can be applied by different stakeholders and adapted to the context of the organization (including for SMEs).

Alisdair McIntosh, Policy and External Relations Director, Chartered Institute of Internal Auditing (UK and Ireland), said that cyber risk had become an "existential risk" to which businesses are struggling to respond. "An effective approach to cyber risk requires a robust, systematic and holistic governance framework."

Discussion moderator **Julia Graham**, Technical Director of Airmic, said that the FERMA-ECIIA recommendations were a response with wide impacts to what FERMA and ECIIA had seen as a deficiency in cyber risk management frameworks. "It is a governance matter which supports the resilience of the EU economy to have effective and efficient risk management and compliance in dealing with cyber risks."

There is a need to build capabilities in the areas of cyber awareness according to **Daniel Dobrygowski**, Project Lead, Information Technology Industry and Global Leadership Fellow, at the World Economic Forum. There is no doubt that industries and governments should continue making partnership to collaborate at a global scale.

To give a more practical illustration to the interest of a strong cyber risk governance model, a specific session on blockchains and bitcoins took place right after the first panel. The use of virtual currencies is currently developing in many European businesses and panellists agreed that these new technologies should be managed with a strong collaborative model, including all the impacted functions. The governance model developed for cyber could be easily adapted for these risks.

Finally, **Farid Aractingi**, Vice President of ECIIA, and Vice President Audit, Risk & Organisation, encouraged national institutes of internal audit and risk management associations to take ownership of the recommendations, to translate and publicise it. "Such events will increase general awareness and help reduce the impact of cybersecurity attacks."

Concluding the event, Jo Willaert stated that key influences driving cyber security today include public opinion, regulators and investors. "They are pushing companies to take not only IT measures, but to also adapt their corporate organizations. As part of their mandate to secure the development of the company, Boards need a solid internal analysis to support future investments in cyber security more than ever before."

Photographs taken during the event can be seen at: http://bit.ly/2tQOoa0

Speeches

1.

Welcome address and opening remarks: Do we need a cyber defence forces? Antanas Guoga, Member of the European Parliament, EPP

Cyber security is becoming inevitable topic of discussions in a rapidly evolving digital era. The latest *WannaCry* cyber-attack has once again taught us, how costly such form of a crime can be. Moreover, these types of incidents know no national boundaries, affect globally and digitally. Have we done enough to brace ourselves against such attacks? Are there enough awareness and preventive tools? It is our wake-up call; hence we must act now and fast.

We have managed to convince EU Member States to accept a mandatory cooperation mechanisms on cyber-security. The General Data Protection Regulation (GDPR) and the Network and Information Security Directive (NIS), two legislative files I was directly involved in, are in the implementation stage. The NIS directive promotes a wider scope, tougher sanctions and accountability. However, cybersecurity policy in the EU should not begin and end with these legislative acts. It is about time to focus on a strong cooperation between EU governments and seriously consider the idea of a cyber-defence resilience. Moreover, transparency and ongoing implementation of the directive should ensure to improve the ability of the Member States to prevent, avoid and/or ease the response to cyber-attacks. We must take this threat seriously at Governmental and individual level. Let us see how.

Stimulating awareness

According to a Cyber-Risk Survey[1] (2016), just 31% of organisations have a full and comprehensive understanding of the present cyber risk. This is surprisingly little. The example of the *Wannacry* attack shows that these cyber-attacks do not respect national borders. It infected computers in over 150 countries. The security of a technological devices itself does not make it immune to attacks and it remains vulnerable through its interconnectedness with other global networks. Hence, we must think globally. I argue that it is critical for the governments and companies around the world to not only see the opportunities, but also calculate the risk inherent to our digital age.

We must raise awareness and educate leaders from different backgrounds. We need to ensure that governmental Representatives, CEOs, CIOs and board members understand that cybersecurity is not simply an IT issue, but a business and governmental issue. It is a national issue affecting everyone individually. I invite governments to foster shared comprehension of these existential threats by firstly developing a common language, to establish a regular communication on the topic. Promote an understanding that everyone, who is online when watching the news or using an online banking system is vulnerable to cybercriminals. In this context, I would like to mention #SWITCH, which is the largest ICT and entrepreneurship event in the Baltics, taking place in Kaunas, Lithuania in September. I have invited senior cybersecurity experts and EU governmental representatives to share best practises and discuss about the best cyber risk management models.

[1] Marsh Continental European study

Prevention better than cure?

A Lithuanian proverb states the obvious: it is easier to stop something from happening in the first place, instead of repairing the damage after it has happened. However, here I see an analogy to the sports industry. Cybercriminals can be compared to the producers of doping products. They will always be ahead of those, who are fighting against them. They are faster and more adaptable and due to the high profits always ahead of the game. The others are constantly in the defensive and solely reacting, instead of developing a pro-active and comprehensive plan. Given the rise in volume, sophistication, and automation of the attacks, a focus on preventing them is needed. According to the survey, companies that consider cyber risks a top five risk increased from 19% in 2015 to 32% in 2016. Great! Let's keep this pace and start with the most vulnerable sector, much depending on IT systems, for example online platforms or the finance sector. The banking sector faces strong threats from cyber-attacks, if they are affected we all are affected. The NIS directive gives a green light for systematic and common preventive work, reactive cyber threat or attack management. Preventing cyber-attacks is part of a holistic approach to cybersecurity risk management. Not all attacks can be prevented. But the right technologies and platforms can prevent many of them. Moreover, European Governments and EU institutions should invest more in prevention to protect their own IT system and networks. The private industry should lead by good example and should be the no. 1 partner.

Hand in hand with business

Cybersecurity sector is very young and opportunities for growth are limitless. We, citizens want to secure our private data as well as large multinational organisations want to secure their business secrets. When I am asked, where to invest to be successful, I always say - the best investment - in the growing sector. Businesses should open their eyes wide and look for the niche. The governments meanwhile, should give and ensure businesses an opportunity to share ideas, expertise and participate in Europe's cybersecurity-related policy development and implementation. Their participation can help ensure that policies are workable and meet the needs of businesses and citizens. Cooperative work could also encourage a greater voluntary sharing of information on cyberattacks, cybercriminal motivations, and the tactics of malicious criminals. Together with FERMA and ECIIA on 29th June at the European Parliament I organize a cybersecurity conference. We will present and discuss the proposed guidance and what other improvements can be done in the field.

Finally, the cyber-attacks are the biggest threats of the digital age against which we need to fight using our intelligence. To improve the lives of our citizens we need to think out of the box and implement new strategies. Countries have armies, navies, air force, but when was the last time any EU member had to defend their borders and use their physical defence tools? Perhaps it's about time to seriously think of the cyber defence forces? Which I think is currently needed as never.

2.

Cybersecurity during the Maltese presidency of the EU – status and upcoming challenges
Rodney Naudi, Head of Department - Governance, Risk & Compliance, Malta Information Technology Agency (MITA)

Distinguished guests, fellow speakers

I would like to start by thanking FERMA and ECIIA for inviting me to address this seminar. It is always encouraging to participate in events where we can share our experiences in tackling the safe use of cyber space.

With the Maltese presidency of the Council of the European Union coming to an end, we can look back at the last six months and reflect on how the security threat-defence landscape has changed: changes stemming from advances to secure our leverage of cyber space but unfortunately also by more pronounced tactics deployed by hackers. The stakes are higher than ever before.

Last January, in outlining the priorities that the Maltese presidency would be tackling within the realm of cyber security, I made a case that cyber risks not only effect Governments and large institutions but also extend to SMEs and citizens alike. Cyber threats know no boundaries. In todays connected, anytime, anything, anywhere world, whether we like it or not, we depend on cyber space for everything from communication to energy to transport to health. Cyber risks associated with cyber threats effect all users of cyber space – the difference lies in the perspective.

For governments, we have seen an increased focus on cyber risks attempting to hinder the ability of Governments to govern. Election hacking, cyberattack attribution, cyber warfare all have become topical news. News has in its own right become news with 'fake news' allegations, symptomatic swaying trends or passing covert messages. On another front, law enforcement agencies are being faced with issues stemming from hackers using strong encryption to cover their movements or from traceability issues related to late adoption of more recent technology. The balance between law enforcement controls and privacy is still not in an optimal stage and more work is required on this front.

SMEs and citizens are concerned about Government cyber risks. However, there are items which hit closer at home, a more personal perspective. Most SMEs and citizens see cyber space as a commodity and get to understand the risks bound to it too late in the day. Ransomware wiping a small company's customer records, ransomware wiping a family's records down memory lane might not have monetary value but for the effected SME or citizen they are irreplaceable.

Governments and larger organisations acknowledge cyber risks and hence prepare for mitigation, albeit with varying success. Business continuity has indirectly made a strong comeback as cyber risks will at one time or another materialize and then the recovery to a breach is what makes or breaks an institution. However, for SMEs and citizens, data loss following a cyber issue is more prevalent with weaker backup regimes in place.

During the Maltese presidency, we advocated that whilst technical controls are important to mitigate cyber risks, a stronger emphasis must be placed on raising awareness and consolidating structures that engage all stakeholders and encompass all dimensions.

The Malta Cyber Security Strategy launched in 2016 recognises that tackling cyber security entails the need to:

- Safeguard the rule of law
- Adopt a multi-disciplinary approach
- Ensure that all stakeholders of cyber-space; including the government, the private sector, and the civil society understand their shared responsibility and thus commit to collaboration and cooperation, to ensure a safe, stable and secure environment
- Adopt a risk based approach, based upon the premise that it is impossible to guarantee immunity from any cyber attack

Six goals were identified that would enable Malta to achieve these objectives, namely:

- Combat Cybercrime
- Strengthen National Cyber Defence
- Secure cyber-space
- Spearhead Cyber Security Awareness and Education, emphasizing the three-party notion of protect, detect and react from different stakeholder perspectives
- Foster National and International Cooperation
- Establish a Governance Framework

A model of Cyber risk governance will assist in better understanding the structure and locus of responsibility in identifying and dealing with cyber risks through:

- Capitalising on existing structures dealing with risks and involving them as required. We need to shy away from having structures dedicated to handle cyber risk without the intelligence and perspective that other structures already have.
- Building multiple levels of defence, firstly to encompass the wide range of disciplines that a cyber risk typically effects, as well as having a defined fall back in the safety net.
- Acknowledging that determining risk severity by computing likelihood and impact may be too simplistic when dealing with cyber risks – the perspective of 'how long it takes to understand the indicators of compromise are there' is itself a risk that must be accounted for.
- Relating cyber risk to its context, the government/organisation/SME/citizen perspective.

I am sure that today's discussion will cement another capability in building defences to contain cyber risks, a capability that will relate to stakeholders and extend upon lessons learnt from dealing with other risks over the years.

3.

The FERMA/ ECIIA Cyber Risk Governance Model: key findings, Philippe Cotelle, Head of Insurance Risk Management, Airbus Defence and Space, France

Of course we are fully aware that we have a variety of situation and the case of a large international group is very different from the one of a SME or a public hospital for example. However what is common to all of them is that they are all potential victims of cyber-attacks and suffer losses.

The recent Wannacry case just illustrated that industry like Renault, Service Provider like Telefonica, public transport like Deutsche Bahn or public service like NHS in UK are equally facing the same threat. Some analysis performed in France just highlighted as well that SME are common targets of attacks and suffer losses that are significant. So should they react differently to this threat bearing in mind their specific situation? Probably yes. Shall they all get prepared and implement a rigorous process to identify their exposure and allocate their resources in the most optimized way? Absolutely.

The document we have produced is not a one size fits all miraculous recipe. The framework which is described in order to answer those questions has to be adapted to the reality of the risk owner. However, the efficiency can be measured in the improved resilience of the companies as being more aware of the risk, having anticipated major issues and better prepared to react as their resources are better allocated.

This is not a moto, this is an efficient and pragmatic way for companies that are in the frame of digitalization, either to grow or to follow the competition, to help their Board to take the right decisions in this difficult transition phase, facing a challenge that has no precedent.

The basic idea comes from a simple fact. There are too many siloed functions in the companies and cyber had been for long considered only a technical security issue. We need to create a path of communication between the first line and the second line of defence (between Security and Business Operation). From this discussion, some credible scenarios of exposure will appear, implying security issues and business consequences. This is where the risk manager role is bringing its value in challenging those different organizations, to address situations that they had not envisaged previously.

And this is the risk manager who will interface with Finance in order to evaluate the impact which could affect the company. This step is essential and is so far rarely performed. One value of this document is to highlight those points and hopefully convince all organisations to exercise them.

At that stage, this group is able to give to the Board a consolidated view of the financial exposure of the company to cyber risk, validated by the entire organization. This is a very strong asset and key value for Top Management, because they have a solid basis for supporting their decisions.

This is only part of the work of this cyber risk governance group. It shall not only declare problems but also propose solutions! The risk manager will therefore work with Security which will elaborate mitigation plans proposals. This is no more a competition for budgets and recognition. This is a coordinated approach where the proposal of investment from IT Security will be supported by the analysis performed just before. For the first time, management is really empowered to take decision on effective exposure and remediation.

For the first time, allocation of resources which are always limited will be optimized and guided towards the most efficient use to reduce company's exposure. This is not just for large corporate companies! This logic can be and shall be adapted to all type of organizations.

Finally insurance can be part of the solution. In too many cases, cyber insurance is a tick in a box exercise, with limited coverage and capacity and no clear understanding of its value. Once the exposure is clearly identified, remediation is defined, then Insurance is becoming part of a consistent risk management policy.

And this is also a win win situation for insured and insurers! For the companies, because they are now aware of the value of the coverage that they purchase but also for the insurers!

Why? Because it is for them much more comfortable to deal with an insured that has a clear cyber risk governance in place, which is a sign of awareness and good risk control and therefore a much better risk!

In summary, we are proposing a framework, which will support the digital development of the companies, identifying clearly the exposure, and optimizing their resources deployed in its risk management process, both in terms of internal mitigation efficiency and higher value of external risk transfer through insurance.

Cyber is now an Enterprise risk and not anymore a technical risk. Nevertheless this is not the ONLY risk that a company or an organization can face. This is the reason why this cyber risk governance group would contribute through a Risk Committee which aims at addressing all the risks in a synthetic way.

However having a strong and solid position on this matter will be appreciated as this topic is now clearly part of the Board Agenda.

4.

Alisdair McIntosh, Policy and External Relations Director, Chartered IIA (UK & Ireland)

Delighted to be here, and delighted to have been able to participate in this innovative joint project with colleagues from the internal audit and risk management professions.

Cyber technology represents a transformational opportunity for our businesses, our economies and our societies: but in step with the opportunity comes a growing threat.

To quote the Global Institute of Internal Audit, '*it is not solely a technology risk: it is a business risk*'. I would go further – it is existential.

And businesses are struggling to respond.

On the basis of global surveys, nearly 90 per cent of company boards and leadership teams lack confidence in their organisation's level of cyber security. Nearly as many think that their cyber functions do not meet their needs. [EY]

One third of audit committees see managing cyber risk as the single biggest challenge for their company. Most consider themselves to be sufficiently focused on the issue, but see real gaps in their organisation's ability to manage cyber risk effectively. [KPMG]

And from the perspective of internal auditors, only half think that their own organisation uses a robust framework designed to address cyber risks. [IIA Global]

This explains why the Chartered Institute of Internal Auditors, which represents the profession in the UK and Ireland, was so keen to contribute to this exercise. Because the profession we represent has a stake in the adoption of effective solutions, and a distinctive contribution to make, in organisations of every type in every sector. As do our colleagues in the risk management profession.

An effective approach to cyber risk – identification, prevention, management, mitigation, and all too frequently recovery – requires robust a robust, **systematic and holistic** governance framework.

The approach put forward in this paper takes as it twin points of departure two well-known and universally applicable models – the 3 Lines of Defence [page x] and the OECD Principles for Digital Security [page y] - and applies them to the cyber context.

It looks at the key themes and activities, and the key functions in organisations – both 'horizontal' and 'vertical' functions - and seeks to describe how they fit together.

And specifically it spells out the respective and complementary roles and responsibilities of internal audit and risk management and how they interact – in an Enterprise Risk Management model [page z].

Although the paper is concerned with function more than form, it does propose [page a] a new structure – a Cyber Risk Governance Group – bringing together the key business units required to determine cyber risk exposures and establish appropriate risk treatment and controls – which would report into the Risk Committee, to ensure that they have a holistic and systematic view.

The new group would have a close and co-operative relationship with internal audit, as the independent provider to the Audit Committee, and through them the board, of assurance, advice and insight on the range of risk and control issues within the organisation.

That collaboration between the new group and the internal audit function would focus on two specific aspects – the **assurance map** and the **auditability of plans** to manage, mitigate and recover from incidents.

The assurance map is an absolutely critical tool in ensuring that organisations have a complete view of their risks and where responsibilities lie in relation to them. It is a vital area of co-operation between internal auditors and risk managers, drawing also on the technical expertise and knowledge of the specialist information security and technology functions elsewhere in the organisation.

And it is crucial that plans and control mechanisms are 'auditable by design', so that organisations can keep them effectively under review over time. Internal audit has a unique perspective to bring to this issue.

One caveat here. The model put forward in this paper assumes that there are separate Audit and Risk Commitees in an organisation. That is frequently, but not universally, the case. It is straightforward to adapt the model where there is a single joint committee.

But it is absolutely essential that there is effective communication and co-ordination between all relevant board Commitees on cyber risk issues (as it is for other areas of risk), whether that is achieved by cross-membership or other means – and also that the global view developed through the cyber risk governance group is seen and heard clearly around the main board table.

Of course, organisations differ; and there is no single miracle solution to creating a governance framework for what is a complex and shifting landscape of cyber risk. The proposal we put forward is one way companies could get to grips with the challenge – there may be others.

We hope, however, that we have underlined the need for 'the whole to be more than the sum of the parts', and that our paper will stimulate some reflection and a debate on ways forward. I look forward to the discussion.

5.

Closing remarks, Jo Willaert, President FERMA, Corporate Risk Manager Agfa-Gevaert

It's a real pleasure for me today to see so many of my colleagues for the first time in the house of European citizens. I warmly thank Mr. Guoga for hosting this event and I also want to thank all the speakers for the quality of the exchanges. Although the problem of cyber is global, the management of cyber security issues will be more efficiently handled at a European level.

This is why we have included speakers from the three institutions of the European Union (the European Parliament, the European Commission and the Council of the EU). We want to stress that **Europe is the right scale** to help European businesses increase their cyber resilience.

My first point is about cyber security as a corporate governance issue. In our opinion, risk management readiness can only be achieved within a strong governance framework, and through a **highly coordinated approach across all departments of an organization**.

As we've seen today, in the discussions and the presented report, the **approach to cyber security is changing radically**. Sadly, the WannaCry attacks in May and the further attacks this week illustrate further how much we still need **risk management readiness**.

The future of our initiative is definitely here: in the **continuous improvement** of our proposed governance model and its **gradual acceptance and implementation** by businesses and public bodies.

My second point is about the driving forces behind cyber security. Public opinion, regulators and investors are key influencers, and they're pushing companies to take not only IT measures, but also to adapt their corporate organization.

As part of their mandate to secure the development of the company, Boards need a **solid internal analysis to support future investments in cyber security** more than ever before.

Finally, I would like to conclude by saying that our proposed cyber risk governance model is not intended to **list vulnerabilities**. It is **not about creating a new bureaucracy** with heavy processes.

From the very beginning of this project six months ago, our intention was to **define the elements of an efficient cyber risk governance across functions**.

- By leveraging existing functions and relationships, a cyber risk governance model will avoid cyber management in silos and make an organization **more agile**.
- We expect cyber risk governance to become **an essential condition for seizing opportunities from digitalization**.

By working jointly with the internal auditors of the ECIIA, we have demonstrated how representatives of two professions can **reach a consensus on a moving target** such as cyber, and deliver an innovative proposal that will complement the work of policy makers. I want to thank the 14 members of the joint expert group.

It is now time for our organisations not only to manage cyber risks, but also to make the best from digitalization.

6.

Farid Aractingi, Vice-President ECIIA, VP, Audit, Risk & Organisation, Renault, Chairman Renault-Nissan Consulting

The experience at Renault:

"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 far-seeing internal audit."

When we got this quote from the Chairman and CEO, Mr. Ghosn, for this position paper still under preparation, we could not imagine that Renault would soon be hacked by the infamous WannaCry (*infamous means both notorious and shameful!*).

Indeed, cybersecurity had appeared for the 6th year consecutively as one of the top major risks of the company, and one of the few that we did follow at the level of the executive committee, twice a year.

In terms of governance, we adopted in Renault a model inspired by the one which is publicised in this new position paper, and we also selected a reinforced three-level framework to govern cybersecurity:

- CRI: IS/IT Risk Committee, chaired by the CCO, one of the two most senior executives of the company after Mr. Ghosn;
- CRCI: Risk and Internal Control Committee, chaired by the Secretary General;
- EC: Executive Committee;
- CARE: Audit, Risk and Ethics Committee of the Board of Directors – it is, like in most/all non-financial companies, a unique committee.

Now, when we were hit by WannaCry, we deliberately decided to communicate. Transparency and openness proved to be very positive to mobilise the whole company. Not only to mobilise, but also to demonstrate that we would never succumb to the hackers blackmail to get a momentary peace. Actually, this attack was an effective real-life test, reinforcing our crisis-management system, fostering awareness, and acting as a tremendous education program for all our employees. Let me add one thing: in this case, like in society: **never be a silent victim.**

More globally

Eventually, you cannot mitigate cybersecurity risk with only technical expertise, whatever competent and skilled it is. Because it is not a "mere" IT risk, but has wide and cross-functional implications; whether you measure those implications from the root causes dimension, or through the consequences dimension, it involves the whole organisation. Therefore, **it needs a diversified set of expertise and disciplines, embarked in an adapted governance system. So, what we call a framework is both:**

- **"Hardware": the global architecture of the governance,**
- **"Software": the Delegation of Authorities and the RASIC roles and responsibilities**.

This is a key message for the European regulators and other stakeholders.

It is therefore vital to understand the 3 Lines of Defence model, which both ECIIA and FERMA developed in 2012. Understand at least its spirit and principles, then implement it in the organisation, and finally explain it – relentlessly explain it. **Let me stress on two things you need to ensure:**

- **a trustful coordination between risk management and internal audit,**
- **a fast and transparent information vis-à-vis the BoD through its specialised committee.**

As a conclusion, I would like to encourage European regulators and other involved bodies and stakeholders to promote the implementation of a robust governance model and framework; it is a critical success factor to anticipate and tackle the ever-changing aspects and always-growing harmfulness of cybersecurity risks.

And the more keen you are to ensure the real effectiveness of your global framework, the more impactful will be the new European directives on GDPR and NIS.

Finally, I would also like to encourage the national institutes of internal audit and risk management to take ownership of this document, translate it, and publicise it: such events will increase the general awareness and will help reducing the impact of cybersecurity attacks.

About FERMA

The Federation of European Risk Management Associations (FERMA) brings together 22 national risk management associations in 21 European countries. FERMA has 4700 individual members representing a wide range of business sectors from major industrial and commercial companies to financial institutions and local government bodies. These members play a crucial role for their organisations with respect to the management and treatment of complex risks and insurance issues.

Member associations are from the following countries: Belgium (BELRIM), Bulgaria (BRIMA), Czech Republic (CZRMA), Denmark (DARIM), Finland (FinnRima), France (AMRAE), Germany (GVNW), Italy (ANRA), Luxembourg (ALRiM), Malta (MARM), Netherlands (NARIM), Norway (NORIMA), Poland (POLRISK), Portugal (APOGERIS), Russia (RusRisk), Slovenia (Sl.RISK), Spain (AGERS and IGREA), Sweden (SWERMA), Switzerland (SIRM), Turkey (ERMA) and United Kingdom (Airmic).

About ECIIA

The European Confederation of Institutes of Internal Auditing is the consolidated voice for the profession of internal auditing in Europe, by dealing with the European Union, its Parliament and Commission and any other appropriate institution of influence and to present and develop the internal audit profession and good corporate governance in Europe. ECIIA has 35 members representing 46.500 internal auditors.

Members associations are from the following countries: Armenia, Austria, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Montenegro, Morocco, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and UK & Ireland.