CYBER INSURANCE DIALOGUE

HOW EUROPE CAN LEAD THE WAY TO CYBER RESILIENCE

JUNE 2023

A joint-report by

Allianz

AXA

HDI

howden

Marsh

LLOYD'S

Munich RE

FERMA

KEY TAKEAWAYS

OVERALL

- An annual international conference bringing together key stakeholders from insurance value chain and policymakers is needed. Conference on 26 June as template.

PART1 IDENTIFICATION & PREVENTION

- For large corporates, improve identification and prevention by investing in quantification, benchmarking and crisis management training & protocols.
- Development and continuous review of common EU cybersecurity standards for the SME segment.
- Awareness-raising campaigns/tools and incentivisation schemes for SMEs to invest in cyber security controls by public authorities.

PART 2 UNDERWRITING

- Continuing work towards a standardised baseline questionnaire to be used in underwriting discussions.
- More training around the technologies embedded in business processes and the necessary security.
- Transitional coverage to be offered to SMEs on cybersecurity journey.
- A more continuous underwriting approach for larger corporates with a focus on more and better feedback.

PART 3 COVERAGE

- Europe to become global leader by addressing solution for risks that cannot be covered by private insurance market alone.
- Further discussion required around public and private cooperation to find solutions for evolving cyber risks (for example Cyber War and Systemic Risks).
- Stress-scenarios to be developed and worked on by all stakeholders (public and private).

PART 4 CLAIMS

- More knowledge sharing from claims, with help of public authorities.
- Common language around claims incidents in context of trusted community (using language of DORA).

STRUCTURE OF REPORT

In this report, we visit the fundamental steps on the cyber risk management pathway to equip risk stakeholders with the latest insights on the state of the market and to provide a starting point for a cross-functional, European-wide dialogue on how to improve cyber resilience and protection. We cannot claim to provide an exhaustive commentary on the status of the market and have collectively focused on the main issues. There is ample possibility to explore certain topics in more depth in the future.[1]

The report follows the key steps in the sequence followed by participants in the cyber insurance marketplace, namely; identification and prevention of risk; underwriting; coverage; and claims. It highlights issues and potential next steps in every stage of that sequence. Although they are not silver bullets, we hope these will illustrate some of the challenges and some potential solutions that will create a sustainable cyber insurance marketplace to build the resilience of businesses both large and small in Europe and beyond.

(1) For example, out-of-scope of this report is Cyber CAT bonds, or a Cyber Re(insurer) [SOURCE]
(2) FERMA (2018) Preparing for Cyber Insurance [SOURCE]

FOREWORD

OPENING

In today's digital economy, cyber attacks represent an ever-present and evolving threat for businesses across all sectors and of all sizes. Cyber risks are as much about human and systems errors as they are about malicious threats.

Effective cyber risk management is an essential business practice. It is complementary to overall cyber security and vice-versa, akin to sprinklers for property insurance. Cyber insurance in turn is an important tool in managing the transfer of some of this risk. A workable, relevant and affordable cyber insurance market is therefore vital to ensure that the system is robust and resilient and that European businesses can respond swiftly to these changing exposures.

This report **Cyber insurance dialogue: how Europe can lead the way to cyber resilience** is the result of a pan-European, multi-stakeholder exchange convened to address the challenges faced by all participants in the cyber insurance chain and to discuss solutions to this societal issue.

WHAT HAS HAPPENED SINCE 2018'S *PREPARING FOR CYBER INSURANCE REPORT?*

In 2018, a landmark year in the cyber world thanks to the GDPR, a joint effort by risk managers, insurers and intermediaries resulted in a first-of-its-kind guidance document to prepare organisations for the dialogue on cyber insurance[2]. Since then, the cyber risk landscape has evolved rapidly, demand for cyber insurance coverage has grown and the cyber insurance market has become more mature.

Cyber risks are an unwelcome side-effect of the fast-paced digitalisation that has benefitted the European economy in recent years. Cyber attacks are a constant and evolving threat, that can result in increasingly complex incidents for enterprises. Cyber attackers are using ever-more sophisticated techniques to exploit targets and the cyber security tools on which many businesses rely may become less effective over a period of time without continued investment.

The ability of businesses - both large and small - to adapt and respond to these threats is crucial for the economy and society as a whole. And while cyber exposures have increased, so too have the minimum standards required by insurance underwriters in order for this risk to be transferred. And yet, for many companies, the uncertainty around the likelihood and impact of a catastrophic loss scenario is creating further challenges, which is also true for the insurance market.

Recently, two major points of discussion for insurance market participants and buyers have emerged: i) cyber war, and ii) the potentially systemic nature of cyber risks . These factors have likely been among the considerations for buyers of insurance—some of whom have found the market backdrop challenging.

AIM OF THIS REPORT

The various stakeholders that contributed to this dialogue, drawn from the insurance, reinsurance, insurance broking and risk management communities, believe that a collaborative approach is fundamental to balance the risk appetite of the insurance market with the coverage requirements of corporate insurance buyers. Ultimately, solutions must reflect the interests of capacity providers as well as buyers to create a balanced and sustainable market.

The stakeholders highlight the fundamental need to address any potential cyber coverage gaps in order to mitigate the effects of cyber attacks and their financial consequences on the European economy and society as a whole. Furthermore, for the private wholesale cyber insurance market to succeed it must be attractive to capital investors ready to accept these types of risks.

Collectively, we would welcome an annual high-level international summit, where the topic of discussion is the contribution of cyber insurance to cyber resilience, involving all key stakeholders including (re)insurers, brokers, intermediaries, enterprises and public authorities. The aim of this summit would be to advance the dialogue and discuss possible policy solutions or mitigating measures. FERMA and the project partners are providing a template for such a summit with their Cyber Insurance Conference in Brussels on 26 June, 2023.

As part of this dialogue, stakeholders have identified that public-private partnership may be necessary if systemic cyber risks are to be managed and transferred in the long-term. We believe that a more sustainable cyber insurance market will only be made possible through effective collaboration between risk and insurance managers, insurance intermediaries, insurers and reinsurers, and public authorities.

We collectively look forward to continuing these discussions at EU-level and engaging with policymakers on this societal issue. We hope that this report will not only highlight some of the challenges facing both buyers and underwriters of cyber insurance coverage, but provide various pathways to solutions to some of those challenges. Collaboration between all the actors in the insurance space, as well as public authorities and policymakers, is needed to address these issues and improve the cyber resilience of the European economy as a whole.

Dirk Wegener
FERMA
President

Scott Sayce
Allianz Global Corporate & Specialty
Global Head of Cyber and Group Head of The Cyber Centre of Competence

Carlos Rodriguez Sanz
AXA XL
Regional Product Leader, Cyber for A PAC & Europe

Meike Röllecke
HDI Global
Head of Cyber & Financial Lines

Amelie Breitburd
Lloyd's Europe
CEO

Shay Simkin
Howden
Global Head of Cyber

Jean Bayon de La Tour
Marsh
Managing Director, Head of Cyber - Europe

Jürgen Reinhart
Munich Re
Chief Underwriter Cyber

PART 1

IDENTIFICATION AND PREVENTION[3]

The identification and prevention of risks is the first step on the path to building greater cyber security and resilience. Generally, larger corporates and SMEs adopt different risk management approaches in addressing cyber threats.

Larger corporates typically have greater experience in identifying and preventing these risks, greater maturity in so doing, and more in-depth and in-house expertise. SMEs, by contrast, often have a lower awareness of cyber risks, fewer risk identification and prevention resources and potentially also less ability to invest in prevention measures, which often, but not always, reflects the perception that they face lower exposures, as well as a different risk landscape.

LARGE CORPORATES

It is our belief that, despite their greater enterprise risk management maturity, large corporates must continue to find ways to improve identification and prevention, for example by continuing to invest time and resources in the quantification of risk. The private insurance market can help in this area. For instance, as exposure grows, once risk identification has been carried out, the insurance market including brokers, may be able to help guide larger corporates in identifying priorities for prevention that would improve their access to the best available insurance products.

This would also provide enterprises with a basis for benchmarking. When risk teams can quantify and benchmark risks this helps to gain buy-in at the C-Suite for greater investment in risk management.

Investment in risk prevention not only builds the resilience of companies to attack, it also makes the risk more insurable for underwriters. Preparing for and preventing cyber losses is inextricably linked to the insurability of a cyber loss. It is in the interests of the insurance market to ensure that corporates have invested in proactive risk management and cybersecurity measures to reduce the likelihood and impact of a loss – and consider measures such as ongoing processes and improvement, which might eventually be reflected in premiums paid by the insured.

Examples of some of the measures and controls to be taken in current market conditions can be found in Appendix 1

Innovation in technology could, we believe, help these larger corporates to improve their identification and prevention protocols. Threat intelligence that complements an organisation's own IT security framework, or add-on services such as technology scanning tools, can make a real difference to the overall cyber risk hygiene of an organisation - and make it a more insurable prospect for underwriters.

Crisis management protocols form another important pillar in the identification and prevention of cyber risks and the ability of organisations to recover from a cyber event. Investment in these protocols, and robust testing of them, ready organisations to recover more quickly when an event occurs and, again, ultimately make them a more attractive and insurable risk for underwriters. It is vital that organisations both large and small understand the importance of recovering data and restoring operations as quickly as possible in the event of an attack.

More of this can be discovered in Appendix 2

SMALL AND MEDIUM-SIZED ENTREPRISES

In general, some SMEs may find it challenging to identify and prevent cyber risks. In comparison with their larger counterparts, they often have leaner risk management departments (if any) and less ability to invest in identification and prevention measures.

Unfortunately, there is still some lack of cyber risk awareness among many SMEs, despite the fact that their smaller size does not make them immune to cyber threats - indeed, quite the contrary. SMEs need to reach a level of cyber security consistent with their size and maturity and yet this is not easily done. In addition, there is the tendency among SMEs to be dependent on a limited range of service providers or applications, which means they often have virtually no influence or control over the cyber security of these services.

Insurance penetration among SMEs is still extremely low. A recent report by the French risk management association, Association pour le Management des Risques et les Assurances de l'Entreprise (AMRAE), found that only 3% of medium-sized enterprises in France purchase cyber insurance coverage, for example[4]. In another report, Munich Re found that 14% of SMEs around the world have a cyber insurance policy in place[5]. While the samples and definitions of size of enterprise differ, the data suggests the take-up of cyber insurance is lower outside of the large enterprise segment.

Small and medium enterprises have been described by the European Commission as the 'backbone' of the European economy. It is this segment that has the greatest opportunity to improve its cyber resilience. But it also represents a major challenge , which continues to be on the radar of the insurance market and policymakers.

It is accepted that SMEs may not have the same internal enterprise risk management resources as larger organisations. And cyber security measures represent a financial outlay that many SMEs might not have the budget to implement. In recent years, innovation, and investments in technology led by insurers, insurtechs and managing general agents (MGAs), has seen the adoption of scanning technology and pre-breach tools used for identification and prevention assessments for key risks for SME clients in order to help to support their journey to cyber resilience.

(3) See Appendix 1 for stylised list of controls worked on by the Project Group

(4) AMRAE (2023), LUCY: Lumiere sur la CYberassurance. [SOURCE]

(5) Munich Re (2023), Cyber insurance: risks and trends 2023. [SOURCE]

WHAT HAPPENS NEXT?
INCENTIVISING PREVENTION

For large corporates

Continuing to improve identification and prevention by investing in quantification of risks. Also, for corporate insurance buyers more benchmarking would help. So too would crisis management training and protocols.

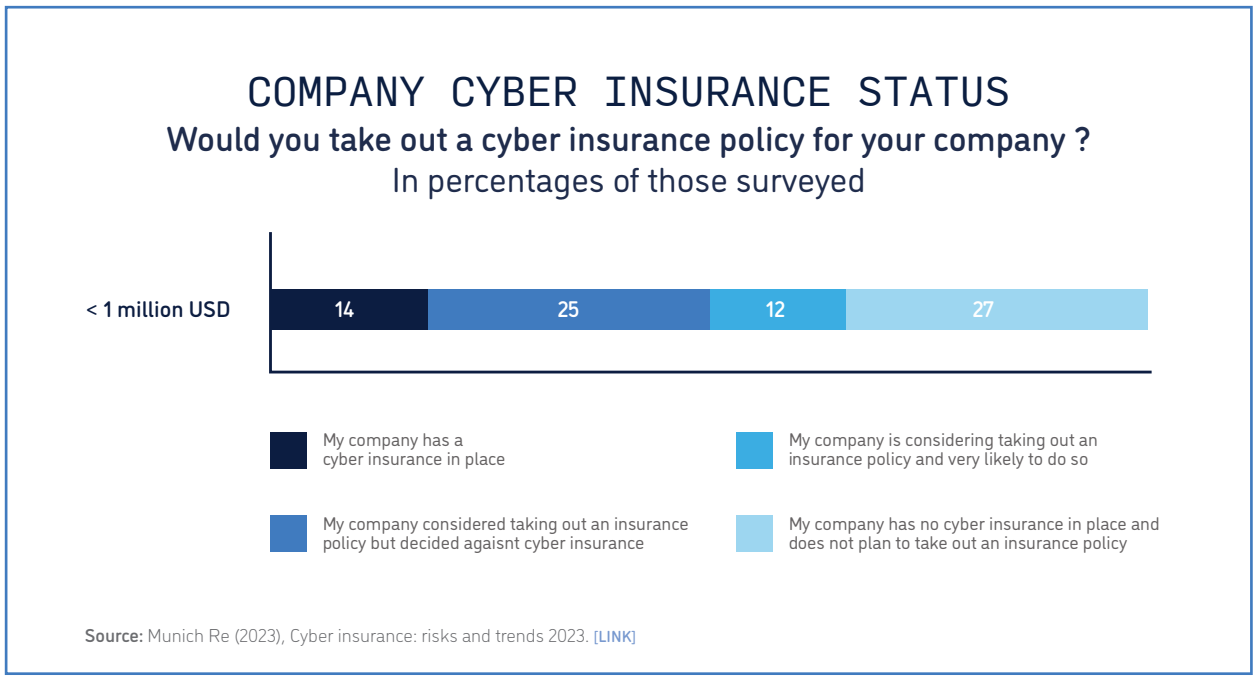
For SMEs

We believe that a set of minimum cyber risk standards, applicable to the size and activity of an organisation, is needed to boost awareness, identification and prevention of threats and, ultimately, the ability for these risks to be insured.

These standards need to be an appropriate target for SMEs, defined according to the size and industry sector of the company. We believe that collaboration between enterprises and the insurance market, supported by European authorities and agencies with a focus on cyber security, to create a set of appropriate, reasonable standards would be welcomed. These could also help to develop standardised cybersecurity maturity assessment tools for SMEs, such as the one developed by the European Union Agency for Cybersecurity, ENISA.[6]

We would like to see policymakers incentivise self-assessment against these standards which, we believe, would drive investment among SMEs in appropriate cyber-security controls. There are some examples from the Netherlands[7] and the UK[8], which could inspire other countries.

Once enterprises can demonstrate they are well-protected by performing against these standards they will become a more insurable risk for the insurance market to take on. This ongoing effort will boost the resilience of the European economy to cyber threats by ensuring that the most vulnerable targets are better protected.



(6) ENISA (2023), Cybersecurity Maturity Assessment for Small and Medium Enterprises. [SOURCE]
(7) Center for Crime Prevention and Security (the CCV), Digital Security Risk Classification. [SOURCE]
(8) National Cyber Security Centre (NCSC), Cyber Assessment Framework [SOURCE]

PART 2

UNDERWRITING

Once organisations have cyber protection in place they are in a position to be able to transfer some of their residual risk to the insurance market. The demand for cyber insurance coverage is expected to grow as more economic activities grow more digitally dependent, meaning cyber risks and exposures are likely to increase commensurately.

Cyber insurance is still in its relative infancy compared with other classes of insurance. It is important to note that data and insights, so vital in underwriting and in the modelling of risks and exposure management, are not static either in the case of cyber risk. This class of business requires dynamic assessment to reflect its changing nature and evolving threat, notably to better understand the aggregation of risks.

Just as the underlying exposures are evolving, so too must the way these risks are underwritten adapt and change. Cyber insurance underwriters will want to see up-to-date measures in place in terms of cyber risk management and will look to use every tool in their kit to manage exposures.

From the point of view of businesses seeking insurance cover it is important to have clear and reasonable expectations on insurance requirements. Moreover, businesses, demand for cyber coverage will change and grow with the evolution in their business and trends in cybersecurity.

IMPROVING THE DIALOGUE

Overall, our multi-stakeholder group, which represents the voices of not only buyers of insurance but insurance and reinsurance underwriters and intermediaries too, believes that the quality of the dialogue between insurer and insured is of the utmost importance.

To ensure that this dialogue is constructive, and that feedback is two-way (from insured-to-insurer and vice-versa), we believe that more direct engagement between risk managers, their brokers and underwriters, would facilitate better understanding of risk underwriting requirements. This is particularly true in the segment of large enterprises.

With advances in technology, some insurers are moving towards continuous underwriting, with frequent dialogue, and offering a suite of risk management support services on an ongoing basis and not solely at the inception or renewal of a policy.

Further continuing collaboration between all the parties involved in the underwriting process from claims departments, brokers, to risk managers to underwriters and so on, could create a 'positive feedback loop' that could further support innovation in the insurance and reinsurance market to continue to develop meaningful solutions and products as the risk evolves. Using intelligence from claims will help in identification & prevention of risks, as well as in the underwriting process—there are many interlinkages and interconnections.

As human behaviour is one of the main drivers of cyber risks, education is needed around the technologies embedded in business processes and the necessary security. This would reduce the impact of cyber attacks and financial consequences on economies.

We would also like to see better benchmarking to enable this constructive dialogue between all parties in the cyber insurance risk process including risk managers, brokers, insurers and claims. This would help to prioritise actions or measures to be taken by organisations to strengthen their cyber resilience and therefore their insurability.

Continuing advancements in technology led and adopted by insurers, insurtechs and MGAs is bringing even more innovation to the cyber insurance market, in particular for SMEs, presenting more options for this segment.

Risk managers working with partners such as IT security firms, which can offer risk information that might help further demonstrate a strong cyber maturity and risk posture sought by underwriters, may be one viable option for larger organisations.

According to data on the French market, large corporates account for more than 80% of the cyber insurance premium volume[9]. SMEs, however, are at the very heart of the European economy and account for more than 50% of its Gross Domestic Product. Therefore, many insurers are enhancing their market offerings to directly target the SME sector with cyber insurance solutions and services.

QUESTIONNAIRES

Over the past few years, the cyber insurance market has evolved towards a similar set of baseline questionnaires to be used in underwriting discussions. However, from the point of view of the client, i.e. businesses purchasing cyber insurance cover, facing multiple different questionnaires could be a challenge.

Simultaneously, it remains necessary for insurers to continually adapt the questions in their underwriting questionnaires to keep on top of the evolution of the threat landscape. These questionnaires assist insurers and reinsurers to continue to derive more comparable and meaningful data about cyber risks, and to benchmark them; tools that are vital to their ability to underwrite them.

We therefore would welcome continuing initiative working towards a common set of baseline questionnaires.

TRANSITIONAL COVERAGE, CONTINUOUS UNDERWRITING

For SMEs

A form of transitional insurance coverage, for those organisations that are on the pathway to improving their cyber resilience, might be considered to support companies in the evolution of their cyber risk management. We support underwriters providing such coverage alongside cyber policy value-added services, which reward the risk management steps already taken and incentivise progress, to bolster organisations, particularly SMEs on their journey to improving cyber risk management, prevention and transfer.

For large corporates

Cyber risks are, as we have already outlined, dynamic and evolving. We believe, therefore, that the dialogue between insurer and insured must also be dynamic, in particular for large corporates. Once-a-year renewal discussions with brokers and insurers may not be appropriate for all clients, when risks are changing, technology is evolving at pace and both exposures and resilience are not static. On the other hand, an overload of communication, notably non-event-related, should be avoided, since numerous internal stakeholders must be involved in risk discussions.

(9) AMRAE (2023), LUCY: Lumiere sur la Cyberassurance. [SOURCE]

PART 3

COVERAGE

What is covered and what is not covered, i.e. finding any potential gaps in coverage, are among the most contentious issues in discussions around cyber insurance. After all, it is important for everybody involved to have clarity and certainty.

On one hand, there is a widely-held perception that most cyber insurance claims are paid, currently. One source on ransomware[10] claims shows in excess of 90% of ransomware claims were paid out in 2022—the most recent data available. On the other hand, the relatively new, and evolving, nature of cyber risk and insurance means that there may be a minority of coverage terms and conditions, such as property physical damage, in some policies which may not be covered subject to policy terms and conditions.

Since 2018, dialogue and developments within the risk and insurance community have highlighted concerns around two key coverage issues – among others – from the point of view of insurance and risk managers, namely cyber war and systemic risk. A key component of this dialogue surrounds the potential accumulation risk. Enterprises looking for coverage ultimately need to know they are covered for the risks they face. These two 'elephants in the room' require an all-stakeholder approach to find solutions. A public-private partnership could be one way of addressing either, or both, of these elephants in the room; and this represents an opportunity for Europe to become a world leader in this area.

ALTERNATIVE MECHANISMS FOR CYBER RISK TRANSFER

Recent market developments have led to some large corporates exploring the use of alternative risk transfer mechanisms, such as captive insurance solutions, whereby risk is retained and self-insured, for cyber risk financing. This can sometimes help organisations in managing their exposures, gaining an enterprise-wide view of them, and thus increasing confidence in their risk modelling, risk management and protection.

Several other large corporates that have found it difficult to access sufficient cyber insurance policy limits for their needs have turned to other solutions, such as making use of a mutual insurer for cyber[11].

The captive insurance mechanism of risk retention however, may not be available to many smaller companies and requires a sophisticated, enterprise-wide risk management approach that is not accessible or applicable to all.

Some insurers also are exploring the development of parametric insurance, whereby coverage is defined upon a trigger rather than quantum of loss. This method of risk transfer could work as a transitional solution for organisations seeking coverage for some types of risk. Again, however, this may potentially not be a solution for all organisations.

As modeling and data quality around these risks improves, reinsurers and alternative capital providers likely will show a greater interest and willingness in devising coverage to address these gaps. However, some fear that the magnitude and scope of these risks, coupled with issues around dependence on the cloud, for example, could be a challenging problem for the private insurance market to address alone.

CYBER WAR

War exclusions are common in cyber policies. But many enterprises still feel there is further adaptation required for cyber risks. For example, in a traditional war exclusion, if a nation-state is behind the attack, what are the implications of this in comparison with a situation whereby a cyber actor declares its support of a nation-state and as a consequence launches a cyber-attack to which the company falls victim. The attribution of cyber events remains challenging for all involved.

Some traditional war exclusions commonly available in non-cyber policies may not adequately address cyber-specific disruptive exposure. In this context, war exclusions that are fit for purpose for cyber (re-) insurance must reflect the interests of both the insured and the (re-) insurer by preventing uncontrollable accumulation risk while at the same time considering the insured's interest of being sufficiently protected against a cyber-attack. Furthermore, this must not jeopardise the cyber insurance value proposition by taking too unclear or strict an approach.

At one level, it is unlikely that insurers can absorb the size of the risk related to cyber war on their balance sheets. On another, companies cannot alone bear the possible range of risks and exposures. It is therefore important that the entire market work together on possible ways forward regarding cyber war. What these solutions are likely to look like, and how they deal with issues around cyber war in society and the economy, is a topic of great interest and debate.

SYSTEMIC RISK

The modelling of possible of systemic risk in the cyber insurance market is a preoccupation of supervisors and regulators across the world[12]. There is some growing concern that the pervasive digitisation and hyper-connectivity of the digital age greatly increases the likelihood of a catastrophic cyber event. Such an event could have a global economic impact, including within the cyber insurance marketplace.

There is also increasing debate among enterprises, which seek clarity on the status of systemic risk in their coverage. From the point of view of the insured, an attack on critical digital infrastructure(s) would clearly have dire economic consequences, but enterprises might understandably worry that an attack on a system might preclude them from being indemnified.

This uncertainty needs to be addressed. Achieving a balance between insureds' and insurers' needs and expectations regarding cyber risk transfer involves a shared responsibility — and, ideally, a partnership, notwithstanding the potential for friction between those that cede risk and those that accept it. If systemic risk is to successfully be addressed it will require the participation of public authorities as well as the private insurance market—and of course business representatives.

(10) Sophos (2022) The State of Ransomware 2022. [SOURCE]

(11) For example, ref. to page 160 of the Solvay 2022 Annual Integrated Report [SOURCE]

(12) See for instance the special topic of the Global Insurance Market Report (GIMAR) by the IAIS in April 2023 on cyber. [SOURCE]

A PATHWAY TO FUTURE COVERAGE

We are collectively calling upon all stakeholders to seize the opportunity to make Europe a global leader by continuing to promote innovation across the cyber insurance industry.

It is in the interest of all participants to have a sustainable cyber insurance market with transparency and certainty for the businesses insured. It could be beneficial for all stakeholders to elaborate on specific stress scenarios, and what solutions might look like even in a catastrophic cyber event. We would therefore welcome an initiative whereby a "whole-of-economy" stress-scenario were developed to better understand if the cyber insurance protection needs of insureds are being met by the product in a hypothetical stress scenario. Reference here can be made to the Bank of England's stress-test[13].

Such stress-testing could give greater clarity on where further action is needed to address potential gaps, as well as providing insights into which actor could intervene. These stress tests could also assist in improving risk quantification and modelling.

Secondly, we call upon public authorities to push for EU leadership on a public-private-partnership solution for the risk that cannot be covered by the private insurance market alone.

We call on businesses, the insurance market and the public sector to intensify their work together in this area. Insurers should continue to distinguish between commercial, industrial and large industrial sectors in their considerations and, where appropriate, act differently in these different segments.

(13) Bank of England (2022) Thematic findings from the 2022 cyber stress test [SOURCE]

PART 4

CLAIMS

An insurance policy is, in essence, a promise to pay valid claims. This hitherto little explored area of the cyber insurance market is where the insurance product really proves its worth to the buyer.

It's vital, therefore, that buyers can see this value; while each €1 invested in prevention and protection immediately improves risk management, each €1 invested in insurance only shows its value if a claim is made and paid. Incident handling is a part of the service and part of the value of a cyber policy.

The days of shame and reluctance to admit having been the victim of a cyber attack should have passed by now, and we believe, therefore, that greater sharing of knowledge and experience will help to improve the claims picture for all market participants.

As previously discussed, there is a relatively shorter claims history for cyber compared with more established lines such as property insurance, meaning that intelligence sharing and robust data are vital to supporting the evolution of claims processes and, ultimately, illustrating the value of the insurance product. The experience, intelligence and insights gained from a thorough analysis of claims would also feed into the other parts of the process (identification & prevention, and underwriting).

To improve claims processes we all need to be better informed about what happens when an incident takes place. Are there differences in the way cyber attacks affect large corporates compared with SMEs, for example? How do claims manifest and what can we learn from them?

The necessary steps to take during a cyber event typically vary depending on the nature and severity of the attack and the size of the company being targeted. It is essential, however, for companies of all sizes to have a detailed incident response plan in place before a cyber event occurs.

This plan should outline the steps to be taken in the event of an attack and who is responsible for those steps, as well as communication protocols. Regular testing and review of the incident response plan can help ensure that it is up-to-date and effective.

The claims protocol in Appendix 2 is an example of how this can be done.

We also believe that investment in more training and education is a positive step to improve the skills and knowledge in this area. As we have mentioned, cyber is a dynamic and changing area and there are continued lessons to be learned in every step of the incident recovery and claim process. Insurers that offer cyber coverage could also put in place claims-handling departments designed specifically for cyber claims, and staffed by specialists.

Immediately following a cyber event, organisations likely will engage multiple third-party vendors to assist in the response and recovery process. These firms provide a wide range of services including public relations and crisis management support, legal counsel, breach management services, forensic investigation and data/system restoration.

Many organisations' first inclination is to engage vendors with whom they have preexisting relationships, however it's important to note that cyber insurance policies typically include clauses requiring the use of vendors from a pre-approved panel. Some insurers are open to the use of other pre-agreed providers that are not on the panel - provided they have proven knowledge and expertise in handling cyber claims.

The potential severity of a cyber claim - which could bring down a whole company - means that ensuring good dialogue and effective communication during a claim between all relevant stakeholders is imperative to ensure that the best advice is given to the victim of an attack, and that sensible decisions are taken to ensure a crisis is managed and swiftly recovered from.

IMPROVING CLAIMS; SHARING KNOWLEDGE

Cyber attackers share information within their community to enable more effective attacks; we believe, therefore, that better sharing of information about how these attacks affect organisations -the claims that they incur - can help to improve resilience.

We welcome initiatives that promote greater knowledge sharing to enable those organisations that have not suffered an attack to learn from some of the lessons of those that have.

We believe that sharing of incident and claims information, facilitated by organisations such as ENISA and EIOPA, cyber security incidents response teams, and accessible to insurers and brokers will improve the overall resilience of the entire European economy to cyber threats.

There is, of course, sensitivity around claims data and we recognise the need for this to be robustly protected by, for instance, an independent third party such as an association or EU agency collecting and aggregating data.

Devising a common language around claims incidents, across the public and private sectors, will enable us all to learn and build a trusted community in line with the aims of the Digital Operational Resilience Act.

PART 5

THE ROUTE TO CYBER RESILIENCE

This report represents the outcome of a groundbreaking, pan-European dialogue, bringing together stakeholders from across the cyber insurance landscape. We recognise the need for a dynamic, robust cyber insurance marketplace to build resilience for organisations big and small, and the economy as a whole.

Cyber risk is an evolving and growing threat to organisations of all types, whatever their size, wherever they may be located and whatever their principal activities. This is a risk that cannot be ignored, and relevant insurance coverage is a vital element in building resilience.

Across every step of the cyber insurance journey, improving the availability of and learning from data is key. We all have a part to play in ensuring we have robust data to gain insights that will help better identify, prevent, manage and ultimately transfer cyber risks.

The insurance market cannot act alone to solve all the challenges regarding cyber risk and cyber insurance. Neither can it, in isolation, find ways to increase the insurance penetration rate among enterprises of all sizes. Each company needs to make cyber resilience a priority: a comprehensive approach to IT security is vital for defending against attacks and, if an incident cannot be avoided, resuming business continuity quickly. In turn, the greater the cyber resilience of an enterprise, the greater the insurance coverage it will be able to secure, the stronger the cyber insurance market in Europe will become for all organisations, large and small.

An improved dialogue between all stakeholders in the insurance chain, including public authorities is vital in this effort. Therefore, FERMA is organising a cyber insurance conference, which will take place at the National Bank of Belgium (NBB) on 26 June, 2023, where speakers from the European Commission, EIOPA and the NBB, as well as the project partners, will unpack the findings of this report and more.

We hope to see the development of an annual event where there is a forum to discuss the contribution of cyber insurance to cyber resilience with all parties. Further, we look as a collective to see the development of standards to help boost investment in this area, as well as towards frameworks for collective solutions. Europe has an opportunity to lead the charge in finding a solution.

TABLE OF PROJECT PARTNERS

Name	Organisation(s)	Position
Paulina Vélez	Marsh	Risk Management Cyber Leader - Europe
Jean Bayon De La Tour	Marsh	Managing director Head of Cyber
Sophie Farhane	HDI Global SE	Head of Cyber Local Risk & Financial Lines
Christian Reimann	HDI Global SE	Head of Risk Engineering Tech Cyber
Olli Laitinen	SOK FINNRIMA	Chief Business Continuity Officer at SOK
Hanneke Van Oss	Bluewater NARIM	Department Head Insurance in Bluewater Board Member at NARIM
Tobias Bunz	E.ON GVNW	Insurance Expert for financial lines and credit Legal Counsel
Martin Kreuzer	Munich Re	Senior Risk Manager Cyber Risks
Carlos Rodriguez Sanz	AXA XL	Regional Cyber Product Leader APAC & Europe
Julien Bedhouche	Lloyd's Europe with the support of the Lloyd's market participants Beazley and CFC	Corporate & Legal Affairs Officer
Benoît Waltregny	Lloyd's Europe	General Counsel
David Franco	Lloyd's Europe	Head of Strategic Intelligence
Sabrina Sexton	Allianz Global Corporate & Specialty (AGCS)	Head of Global Cyber SME and Mid-corp
Scott Sayce	Allianz Global Corporate & Specialty (AGCS)	Global Head of Cyber and Group Head of The Cyber Centre of Competence
Paola Radaelli	ANRA Strategica Consulting Srl	Vice-president, ANRA Senior Risk Management Consultant, Strategica Consulting Srl
Shay Simkin	Howden	Global Head of Cyber
Yves Brants	NRB BELRIM	Risk Manager
Philippe Cotelle	Airbus Defence Space AMRAE & FERMA	Head of Insurance Risk Management Vice-President
Typhaine Beaupérin	FERMA	CEO
Charles Low	FERMA	Head of EU affairs

APPENDIX 1

LIST OF CONTROLS

The table below, the outcome of collaboration between the members of this project, details some of the key controls that organisations, of all sizes and across all industries, could consider implementing to achieve cyber resilience and insurability in Europe and globally.

This table highlights the evolution and definition of the key cyber-security controls that the insurance market has identified based on reviews of cyber losses.

It is important to establish that not all controls are applicable for all types of companies. For example, not all SMEs in all sectors are expected to have deployed a priveleged access management (PAM solution). Also for some types of activities, it is important to consider other types of key controls, such as access management an operational technology environment in companies that rely on this type of technology.

Ultimately, there is no silver bullet control that can guarantee security and protection and it should be made clear that, because of changing attack-methods and evolving technology, businesses of all sizes and in all industries, even with best in class controls, are at risk of being susceptible to a cyber incident in the current threat landscape.

This selection of key controls is meant to be a non-exhaustive guide for what any type of company needs to take into consideration before considering cyber risk transfer.

KEY CONTROLS

GOVERNANCE

According to NIST, governance is integrated by "the policies, procedures, and processes to manage and monitor the organisation's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk".

WHAT SHOULD A COMPANY CONSIDER TO PUT THIS CONTROL IN PLACE?

- Designate a Chief Information Security Officer (CISO), Chief Security Officer (CSO) or functional equivalent.
- Designate a Chief Privacy Officer (CPO) or a functional equivalent.
- Formalise and implement information security policy.
- Formalise and implement data privacy policy that met all the legal requirements.

ACCESS MANAGEMENT, INCLUDING MULTIFACTOR AUTHENTICATION (MFA) FOR REMOTE ACCESS AND PRIVILEGED OR ADMINISTRATOR ACCESS.

WHAT SHOULD A COMPANY CONSIDER TO PUT THIS CONTROL IN PLACE?

- Require MFA for all remote logins to the corporate network by using secure remote access, such as virtual private network (VPN) and remote desktop protocol (RDP).
- Require multifactor authentication and encrypted channels for all administrative account access, irrespective of a user's location.
- Require MFA for access to the most critical or sensitive data or systems, irrespective of a user's location.
- Enforce complex long passwords that are longer than 14 characters and use upper and lowercase letters, numbers, and symbols.
- Change default passwords.
- Establish a process to lock out users after a set number of failed attempts

SECURED, ENCRYPTED, AND TESTED BACKUPS

WHAT SHOULD A COMPANY CONSIDER TO PUT THIS CONTROL IN PLACE?

Organisations should review their critical systems and assets, and ensure that:

- Require MFA for all remote logins to the corporate network by using secure remote access, such as virtual private network (VPN) and remote desktop protocol (RDP).
- Require multifactor authentication and encrypted channels for all administrative account access, irrespective of a user's location.
- Require MFA for access to the most critical or sensitive data or systems, irrespective of a user's location.
- Enforce complex long passwords that are longer than 14 characters and use upper and lowercase letters, numbers, and symbols.
- Change default passwords.
- Establish a process to lock out users after a set number of failed attempts.

PRIVILEGED ACCESS MANAGEMENT (PAM)

WHAT SHOULD A COMPANY CONSIDER TO PUT THIS CONTROL IN PLACE?

Privileged access management (PAM) is a security technology that offers an elevated or "privileged" level of access to protect accounts, credentials, and operations. Privileged access differs from "normal" access because it can allow security or maintenance functions, system- or application-wide configuration changes, and the bypassing of established security controls through super user access.

At the outset, an organization needs to identify the use case — that is, the actions or event steps it wants to invest in a PAM for. For example, it can adopt a risk-based approach to identify critical assets that are at the highest risk of exposure, as a result of the compromise of privileged accounts, and then only implement the solution for those assets.

Once PAM is in place, to overcome any misconception about the solution, an organization can distribute content to its employees on its different components, their purpose, and why they are required as part of the overall cybersecurity mix. An organization also should establish a governance and monitoring program for PAM so that performance does not degrade over time. This should include setting selection and performance criteria for vendors and products and conducting post-implementation performance evaluations.

Regarding the scalability of PAM, roadmaps for business growth can factor in additional relevant assets requiring this control, so that licenses are available to accommodate them when implemented.

Not all companies are prepared or are able to deploy a PAM solution. But privileged account management is important for all type of companies, regardless the company size or sector, and it is recommended to, at least, implement the following actions:

- Eliminate or limit and protect the assignment of local administrator rights.
- Users with privilege accounts must have another account for everyday tasks.

ENDPOINT DETECTION AND RESPONSE (EDR)

WHAT SHOULD A COMPANY CONSIDER TO PUT THIS CONTROL IN PLACE?

Having a strong baseline of cybersecurity best practices usually enables an organisation to implement EDR seamlessly. It is also vital to find an EDR solution that can provide the maximum level of protection while requiring the least amount of effort and investment, ultimately adding value to the security team without demanding a lot of resource. Key aspects organisations should look for in a solution include:

- Visibility across all endpoints. It should provide real-time visibility to view suspicious activities, even as criminals attempt to breach your environment, and to stop them immediately.
- A solution that collects a significant amount of telemetry from endpoints, so it can be mined for signs of attack with a variety of analytic techniques.
- Effective endpoint detection and response requires behavioural approaches that search for indicators of attack (IOAs), so organisations are alerted of suspicious activities before a compromise can occur.
- A solution that integrates threat intelligence, including details on the attributed adversary that is attacking and/or other information about the attack.
- A quick-response;solutions should operate in real-time, provide accurate alerting, and automated threat response. This requires detection engines that produce minimal false positives and the ability to set automated response policies.
- Having a cloud-based endpoint detection and response solution is the only way to ensure zero impact on endpoints. This solution should
- smoothly integrate with current systems and provide intuitive remote access to controls.

PATCH AND VULNERABILITY MANAGEMENT

WHAT SHOULD A COMPANY CONSIDER TO PUT THIS CONTROL IN PLACE?

While the implementation of a vulnerability management process is very complex, it can be summarised in five steps[1]:

1. **Preparation.** Conduct a vulnerability analysis, define the scope of assets, inform stakeholders and asset owners, and plan vulnerability scans.
2. **Identification and detection of vulnerabilities.** This can be achieved through a vulnerability scan.
3. **Definition of remediating actions.** To properly define the remediating actions, an IT risk assessment must be conducted. Depending on the remediation (such as a patch or a change in configuration), software restrictions, and availability of solutions, different options can arise including:
   - Mitigate by implementing remediating actions.
   - Accept by launching an exception[2], process and investigating potential indicators of compromise (IOC).
4. **Preparation.** Conduct a vulnerability analysis, define the scope of assets, inform stakeholders and asset owners, and plan vulnerability scans
5. **Implementation of defined actions.** Deployment of the tasks identified in the previous activities.
6. **Monitoring of vulnerabilities.** As new vulnerabilities arise every minute, committing to real continuous monitoring is essential to properly manage them.

INSURANCE COMPANIES ARE ALSO LIKELY TO REQUIRE THE FOLLOWING ACTIONS:

- Periodic performance of a vulnerability analysis.
- Performance of penetration testing — that is, a simulated cyberattack to check for exploitable vulnerabilities — at least annually.
- Ongoing maintenance and updating of the information technology and communications landscape.
- Patches with CVE[3] 8 or above to be applied in less than three to seven days, after their publication, on exposed IT systems.
- Non-critical patches are expected to be applied in less than 30 days after their publication.

(1) These steps are enlarged upon in the SANS Institute paper [SOURCE]
(2) Exception process: a condition that is not aligned with formal security expectations as defined by policy, standard, and/or procedure — for example, a patch isn't applied.
(3) CVE stands for common vulnerabilities and exposures. It is a program launched by MITRE to identify and catalog vulnerabilities in software or firmware.

INCIDENT RESPONSE PLANS

WHAT SHOULD A COMPANY CONSIDER TO PUT THIS CONTROL IN PLACE?

Organisations are advised to encompass the following core capabilities in their approach to incident response planning and testing:

- The incident response plan must contain defined processes and procedures for performing cyber incident handling, reporting, and recovery.
- The incident response team members' roles, tasks, and responsibilities during a security incident must be clearly defined. Additionally, strong definitions of escalation paths and decision-making processes/responsibilities are obligatory.
- The parts of incident response that will be covered externally (such as IT forensic investigations) should be planned and documented, and the relevant contact information noted.
- Due to the significant uptick in ransomware incidents and their enormous loss potential, a specific response playbook tailored to the ransomware crisis scenario should be defined.
- Incident response plans are only valuable when the response team members are familiar with their roles and responsibilities, and when there is clarity on the underlying processes. An annual table-top exercise should be conducted to train the team for specific scenarios, and to evaluate an organization's incident preparedness.
- Additionally, the plans need to be reviewed and updated periodically, incorporating recent developments, such as staff changes and new expected threats.

CYBERSECURITY AWARENESS TRAINING AND PHISHING TESTING

WHAT SHOULD A COMPANY CONSIDER TO PUT THIS CONTROL IN PLACE?

Organisations may want to take the following actions when establishing cyber awareness training:

1. Perform an annual analysis to identify gaps in their cybersecurity skillset and develop and implement training roadmaps and/or project plans to close identified gaps.
2. Establish annual (at a minimum) cybersecurity training and a cybersecurity awareness programme that:
    - Are mandatory for all employees, vendors / contractors, and third party partners with access to the corporate network.
    - Train users to avoid common cyber risks and threats, such as social engineering and phishing.
    - Provide frequent — at least annual — updated content to embody the latest attack and social engineering techniques.
3. Conduct, at least bi-annually, internal phishing campaigns.
4. Have a process to report suspicious emails to an internal security team to investigate.
5. Have a process to respond to phishing campaigns.
6. Tag external emails to alert employees that the message originated from outside the organization.

NETWORK SECURITY

NETWORK SEGMENTATION ACCORDING TO PREVIOUS RISK ASSESSMENT
DEPLOYMENT OF NEXT GENERATION FIREWALL
LOGGING AND MONITORING

COMPANIES ARE RECOMMENDED TO

1. Outline and implement the audit logs and systems or platforms to be monitored, including firewalls, intrusion prevention systems and intrusion detection systems, active directory, antivirus/antimalware, endpoint security technologies such as EDR and XDR, data loss prevention (DLP).
2. Implement a security incident and event management system (SIEM) and integrate the main platforms into this system. Logs should be accessible for at least the last three months and backed up for a minimum of one year.
3. Analyze the logs in the network and define a set of use cases or common patterns that the organization would like to monitor and react to, in the instance that they are found. The information should also be used alongside threat intelligence information.
4. Define processes for reviewing, periodically, the administrators' or high-privileged users' activities on critical systems.
5. Define and train a team of professionals specialized in the monitoring of security events and incident response.

    - Specific processes or playbooks should be defined in order for the SOC and MSSP to react if a cybersecurity incident is detected. If this service is outsourced, these procedures should also include the tasks that the organization would need to execute in order to contain, eradicate, and restore the operations to normality.
    - Define and monitor key performance indicators for continuous improvement.

REPLACEMENT OR PROTECTION OF END-OF-LIFE (EOL) SYSTEMS

WHAT SHOULD A COMPANY CONSIDER TO PUT THIS CONTROL IN PLACE?

Ideally, organisations should stop using any obsolete products. If this is unfeasible, it is essential to ensure that legacy systems are protected. Limiting access to these products from outside the environment is a critical step — if attackers cannot reach a device, the risk of exploitation is significantly reduced. Where possible, network air gaps should be implemented. If this is not possible, a discrete network firewall and monitoring of data flows to obsolete servers should be considered. A good rule of thumb is to treat all access from the internet as untrusted.

Steps can also be taken to limit the potential impact of compromise, such as preventing those EOL systems from accessing or storing critical and sensitive data or systems, meaning that a compromise of the EOL device would not be as damaging.

Upgrading EOL systems and products will come with a potentially hefty price tag. For organisations with significant legacy estates and operational technology systems, an EOL product may mean that the whole system needs to be overhauled, upgraded, or replaced.

Where organisations opt to continue to use the EOL product, the necessary protection and risk mitigation steps will require thorough implementation and will typically necessitate the collaboration of both the IT and OT security teams, and may also call for external expertise and tools. For manufacturers and other organisations with extensive OT systems, this implementation can be complex and time-consuming.

DIGITAL SUPPLY CHAIN CYBER RISK MANAGEMENT

WHAT SHOULD A COMPANY CONSIDER TO PUT THIS CONTROL IN PLACE?

Organisations are advised to consider the following actions to manage digital supply chain risk:

- Adopt a digital supply-chain risk-management framework, including risk rating of first tier vendors/suppliers, based on an advanced risk quantification. This will help an organisation take strategic decisions on risk management and capital allocation.
- Implement a cybersecurity framework. This can include, but is not limited to
  - Account management based on "zero trust" expectations and the "need-to-know" principle. Strict limitations of privileged and generic
  - accounts apply.
  - Enforced appropriate risk-based multifactor authentication (MFA).
  - Engagement with the internal security operations center to develop specific use cases for monitoring third party accesses.
- Develop and test an incident response playbook for vendor/digital supply chain scenarios and include third parties in this playbook.
- Assess contracts, service agreements, and escalation protocols for each vendor or digital supplier.
- Engage with the procurement department to include appropriate cybersecurity hygiene controls and responsibilities in new contracts and renewals. This can include security trainings and certifications.

REMOTE DESKTOP PROTOCOL (RDP) MITIGATION AND OTHER HARDENING TECHNIQUES

WHAT SHOULD A COMPANY CONSIDER TO PUT THIS CONTROL IN PLACE?

Normally, organisations define a set of secure configurations for their main systems and services, based on best practices, commonly known as security baselines or hardening guides. A process is implemented to deploy these configurations, and review them periodically, in order to identify any misconfiguration or deviation. Although they vary between each platform, the configurations that commonly are part of these security baselines may include the following:

- User and access management.
- Password policies.
- Secure services and protocols.
- Firewall configurations: reviewed rulesets and segmentation in place.
- Network configurations.
- Remote access.
- Log management and audit policies.
- Antivirus/antimalware protections.
- Application control.
- Security updates.
- Encryption.
- Other platform-specific security configurations.

To achieve the timely deployment of these configurations, organizations may use images of systems with security configurations or tools already applied and then perform a gap analysis periodically.
An important topic that insurers are concerned about is the exposure of weak or commonly attacked protocols or services to the internet, such as remote desktop protocol (RDP), server message block (SMB), secure shell (SSH), file transfer protocol (FTP), as well as database ports. Organisations need to have a strict hardening process in order to eliminate the usage of these kinds of ports exposed to the internet. If they are needed, as a result of a specific business requirement, organizations should implement compensating controls to mitigate the associated risk.

REMOTE DESKTOP PROTOCOL (RDP) MITIGATION AND OTHER HARDENING TECHNIQUES (CONTINUED)

One of the most common barriers to implementing a hardening process is the absence of a comprehensive asset inventory, providing an organization with detailed knowledge of the technologies in place on the network, which may be supporting critical processes.
Organisations are advised to define a structured change management process to deploy these security baselines. Without a proper process, some of these arrangements may affect the availability of the systems by disabling configurations that are required at the moment of deployment. They may need a deeper analysis in order to find a secure method to function or may even require a change on an application. Today, vendors and cybersecurity organisations are constantly releasing security baselines for the most common systems and services.

EMAIL FILTERING AND WEB SECURITY

WHAT SHOULD A COMPANY CONSIDER TO PUT THIS CONTROL IN PLACE?

Security controls related to malware protection, email security, and web–filtering that could be put in place can encompass the following:

- Using technology to scan and filter incoming emails for malicious attachments and links.
- Preventing macro-enabled files from running by default.
- Evaluating email attachments in a sandbox environment prior to user delivery, in order to determine whether files are malicious.
- Using technology to monitor web content and to block access to malicious websites or web content.

APPENDIX 2

CLAIMS PROTOCOL

The following protocol is the culmination of the joint-efforts of the project. It is stylised to be used as an indicative guide by practitioners.

OVERALL SCHEMA FOR INCIDENT HANDLING –STYLISED CLAIMS PROTOCOL

PREPARATION

- Implementing tools and capabilities allowing a later incident response.
- Defining the incident response teams.
- Creating the incident response plan.
- Testing the incident response plan.

DETECTION AND ANALYSIS

- Identifying the threats: precursors and indicators.
- Analysing security weaknesses.
- Measuring the impact.
- Notifying impacted parties

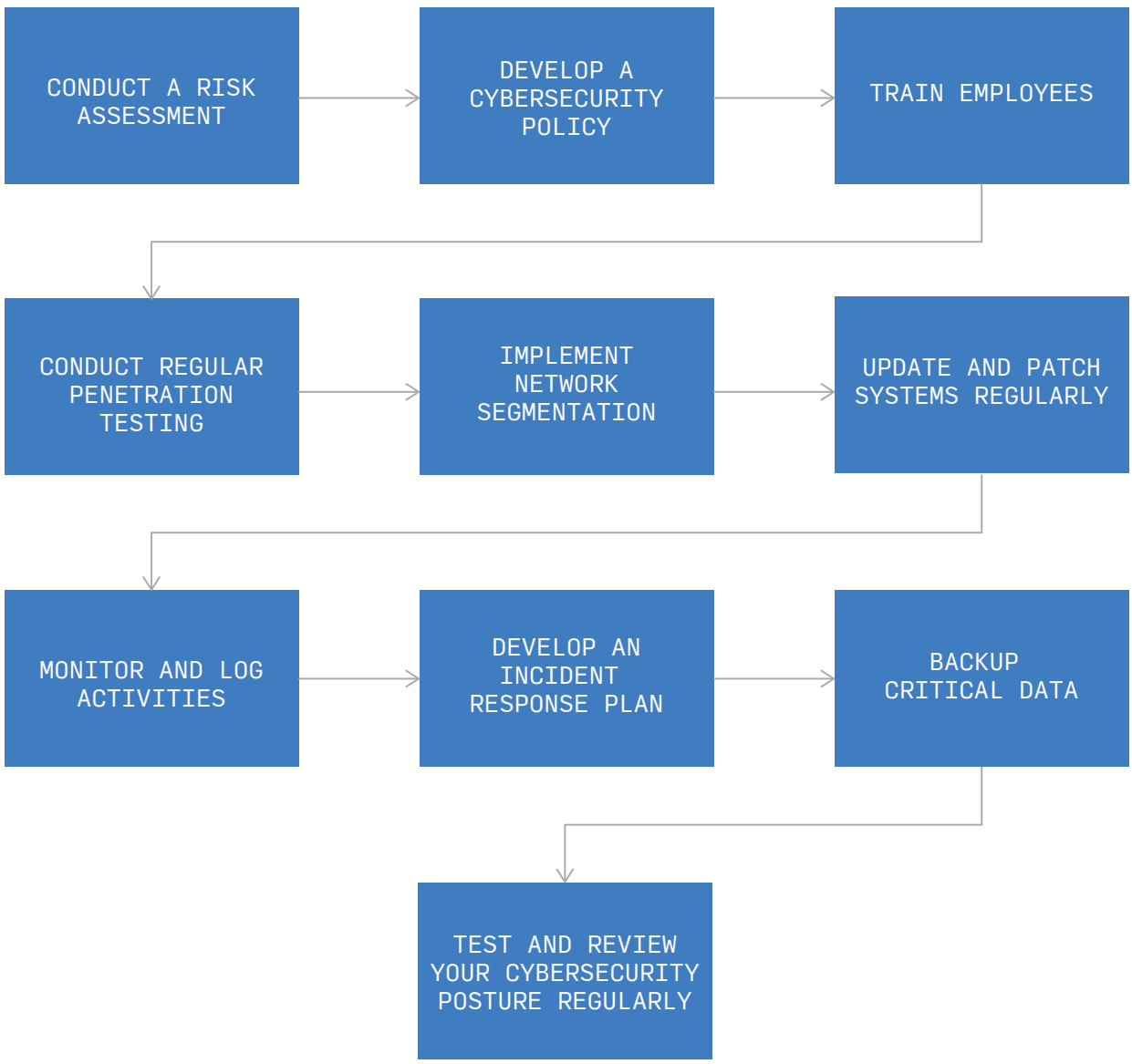
CONTAINMENT, ERADICATION AND RECOVERY

- Isolating the threat and limiting the attack propagation.
- Removing any persistencies, such as malware, and deleting compromised accounts.
- Identifying recovery options (for example availability and quality of backups).
- Improving security controls, removing vulnerabilities via applying latest patches for example.
- Restoring systems from clean backups, changing passwords and such.

POST-INCIDENT ACTIVITY

- 'Lessons Learned'.
- Preparing for future cybersecurity threats and events.
- Incident reporting.

PREPARATION



CLAIMS HANDLING

- Contain the Incident: Quickly isolate and contain the affected systems or devices to prevent further damage or spread of the attack.
- Notify the Relevant Parties: Inform all relevant stakeholders and activate cyber insurance.
- Activate the Incident Response Plan: Activate the organisation's incident response plan.
- Mitigate the Damage: Implement mitigation measures to limit the damage
- Report the Incident: Report the incident to law enforcement or regulatory bodies, if required.
- Restore Normal Operations: Work to restore normal operations as soon as possible and implement measures to prevent a similar incident from occurring in the future.

OPEN DIALOGUE WITH CYBER INSURER, BROKER, AND AUTHORITIES FOR REPORTING

NOTIFYING CLAIM

Insurance
Company / broker / third party /
Notification and regulations
in different jurisdictions

DURING THE CYBER EVENT

IRT / Monitor / Breach coach
Legal / PR / Negociating team

POST EVENT

Forensic accountant
Monitor / Claims department
Broker

KEY POINTS

Time line
Forensic report

NOTES

NOTES

NOTES

For more information, contact:

FERMA - Federation of European Risk Management Associations
Avenue de Tervuren 273 Tervurenlaan
B12 1150 Brussels, Belgium
+32 2 761 94 32
enquiries@ferma.eu
www.ferma.eu
EU Transparency Register N° 018778010447-60

EU Ecolabel
www.ecolabel.eu