Preparing for cyber insurance

bipar

FERMA
Federation of European Risk Management Associations

insurance europe

with the contribution of

AON
Empower Results®

MARSH

October 2018

FOREWORDS

FERMA

This report is the first of its kind, a joint effort by risk managers, insurers and intermediaries to prepare organisations for the exchange of information and prepare for the dialogue on cyber insurance with intermediaries and insurers.

Our ambition is to support insurance buyers in selecting the insurance solutions that are the best adapted to their needs. The fast-evolving legal environment and technological changes are pushing organisations to use cyber insurance products.

The ability of the insurance buyer, notably in medium-sized enterprises, to understand, collect and justify internally the underwriting information required by insurers is one of the greatest challenges for organisations to fully benefit from the potential of cyber insurance.

Jo Willaert,
President of FERMA
(Federation of European Risk Management Associations)

INSURANCE EUROPE

Recent events have demonstrated our economy's exposure to cyber risks. While organisations are becoming increasingly aware of the risks they face — and of the need to implement some kind of risk mitigation solution — many still struggle to translate this into concrete action.

There are various tools available to enhance an organisation's resilience, of which cyber insurance is one. And, while cyber risks are difficult to manage and quantify, the availability of cyber insurance is growing.

To maximise its effectiveness, all parties involved — the insured, the insurer and the intermediary — must have a clear understanding of the risks faced by the potential insured. This helps to ensure that the customer is provided with the most appropriate cover and related services. The aim of this joint report is to help potential buyers better understand their cyber insurance needs and how to go about procuring the protection best suited to them.

Michaela Koller,
Director General of Insurance Europe

BIPAR

Insurance intermediaries (brokers and agents) play a key role in the insurance process. Intermediaries help identify the risks clients face and ensure that clients take informed decisions about the risks they wish to insure. Intermediaries also often design new and innovative solutions.

They assist their clients with claims-related services and policy administration services. Once the risks of the client are identified and the insurance needs are defined, there are a number of factors determining the recommendation that intermediaries make to their clients when advising them on the choice of a particular insurance or solution.

In the cyber risk and cyber insurance market, a new and quickly changing environment, this brochure gives a general indication of the complexity and a starting point for a good dialogue about how insurance intermediaries can assist clients in this specific area.

Ulrich Zander,
Chairman of BIPAR
(European Federation of Insurance Intermediaries)

Special addresses from FERMA strategic partners:

MARSH

Policymakers, businesses and insurance each have a role in helping to find a better way to deal with the many challenges of a rapidly evolving cyber risk landscape. We commend European political leaders for their continued work to develop strategies for cybersecurity. Businesses increasingly treat cyber risk as an enterprise-level governance issue with broad stakeholder engagement. The FERMA cyber governance framework can help achieve that goal.

Within the insurance industry, we have a responsibility to improve information-sharing with key stakeholders and clients about the added value of cyber insurance. Marsh welcomes and strongly supports industry initiatives such as this joint report to contribute to a more cyber-resilient Europe.

Flavio Piccolomini,
President, Marsh International

AON

The growing cyber threat and its potential impact continues to generate concern in boardrooms, with the need for leaders across business functions to take an enterprise-wide approach to cyber risk. Insurance is complementary to a robust cyber resilience risk management programme. Organisations should make an informed decision when considering cyber insurance, and how it responds to their cyber risk scenarios.

The cyber insurance market is continuously evolving and demand for cyber insurance products has extended beyond data breach cover. There has been an increasing demand for products to cover financial losses and property damage resulting from a system failure or cyber incident. Aon is committed to help shape solutions to meet the growing needs of organisations across Europe, so that they can prepare for, and mitigate against a cyber incident.

Onno Janssen,
Chief Executive Officer,
Risk Consulting & Cyber Solutions EMEA, Aon

TABLE OF CONTENTS

GENERAL INTRODUCTION

In its 2018 Global Risks report[1], the World Economic Forum identified cybersecurity as one of the five top risks currently faced by governments, organisations and civil societies across the world. This comes after cyber-attacks and massive data frauds intensified in 2017. Policymakers in the EU are responding to this increased threat by putting forward a battery of proposals to further build Europe's resilience and protect citizens and businesses from cyber threats.

In practice, the recent cyber events have had one positive effect, in that they have made organisations much more aware of the cyber risks they face and more conscious of the need to manage their cybersecurity exposure. However, many companies still struggle to translate their cybersecurity concerns into concrete action.

Cyber insurance is part of a range of tools available to organisations to build up their cybersecurity and resilience. The solutions typically offered by insurers include not only insurance coverage, but also prevention advice and mitigation support in the event of a cyber-related incident.

Despite the increasing importance of cyber risks, the market for cyber insurance in the EU has still to reach its full potential. One reason is that cyber risks can be challenging for insurers to cover due to the difficulty in quantifying risks that are constantly evolving and can rapidly spread worldwide. Similarly, organisations can find it hard to accurately assess their cybersecurity exposures and how best to use insurance to mitigate them. However, these challenges have not prevented insurers and intermediaries from developing solutions, and the market is evolving rapidly.

The insurance solutions proposed reflect an organisation's cyber risks. These are not uniform and depend on the organisation's characteristics, including its size, type, sector and level of digitalisation.

Large organisations tend to rely on tailor-made cyber insurance solutions targeted to their needs. Small organisations, meanwhile, can opt for one of a range of standardised cyber insurance products. Medium-sized organisations, however, tend to be more hesitant about what they need in terms of coverage and services to protect themselves against and mitigate cyber risks. On the other hand, their size and operations might not be adequately addressed by a standardised product targeted at smaller companies. On the other, they may not have the necessary resources within the organisation to undertake a comprehensive cyber risk assessment to gauge whether they need a tailor-made solution.

Whatever the situation, a key component of success in any cyber insurance deal is a good understanding between the potential insured and their insurer.

The authors hope this report can help businesses of all sizes and across all sectors better manage their cyber risks. Cyber insurance is an increasingly valuable part of that risk management.

[1] World Economic Forum (January 2018), Global Risks Report

EXECUTIVE SUMMARY

This report aims to help organisations that are considering buying cyber insurance by providing guidance on some of the important questions they face. It can also help businesses of all sizes and across all sectors better manage their cybersecurity risks.

Part 1 of the report is intended to help organisations prepare for the discussion with their intermediary and insurers. Insurers tend to use their own questionnaires for information-gathering. Nevertheless, there is generally a common thread in the type of information they will ask an organisation to provide. This part of the process is very important for both sides.

The insurer will rely on this information for underwriting purposes, as well as to offer related services. Meanwhile, the potential insurance buyer will be able to assess their cybersecurity needs, and to identify the people to involve in the event of a cyber-related incident. The intermediary will play a crucial role in this dialogue, confirming that the potential buyer has a good understanding of their cyber risks and of the insurance options.

Part 2 of the report provides organisations with tools to help them evaluate cyber insurance offers by giving a general overview of the different coverage available. It also describes potential scenarios that can help an organisation consider how cyber insurance could be useful in their situation.

In summary, this report is for informational purposes only and provides high-level guidance to help organisations assess their cybersecurity and insurance needs. However, the information it contains should not be regarded as providing advice on specific products and the report is not a substitute for the discussion a potential buyer of insurance should have with an intermediary and/or insurer on their specific needs.

PART 1 – PREPARING CYBER UNDERWRITING INFORMATION

Any organisation wishing to implement some form of risk mitigation for its cyber risks —including insurance — must first assess as accurately as possible its exposures and potential vulnerabilities. As a first step, the organisation needs to conduct internal research and build a picture of its cyber risks and how it manages them.

Conducting this research can be challenging, especially for organisations that do not have a dedicated function in charge of risk management or the resources to outsource it. For instance, it may not be obvious which functions within the organisation have relevant information for this exercise. Likewise, knowing which questions to ask can be difficult.

What follows in the next sections represents a broad spectrum of relevant cyber-related information, with an indication of where it is likely to be found within the organisation.

This information-collecting exercise has to take place early in the process of assessing cyber risks. The exercise could lead to improvements in cyber risk management. Indeed, by going through a series of indicators like the ones described below, the organisation may recognise mismatches between the threats it faces and its level of preparation.

The exercise is also likely to be useful for organisations when buying insurance. While insurers tend to rely on their own questionnaires to collect information from potential customers, there is a common thread in the information they will find relevant for underwriting purposes. The sections below are based on this commonality, even though each insurer has to decide which points are the most critical in its own decision-making.

An effective discussion on cyber insurance, based on a high level of understanding between an insurer/intermediary and the prospective insured, is essential to tackle cyber risks effectively. Collecting appropriate internal information can play a huge role in achieving this.

The diagram below shows senior management blocks of information to prepare internally before or in parallel with initiating a discussion with an intermediary or insurer on cyber insurance.

Preparing the dialogue on cyber insurance

Senior Management

Chief Information Security Officer (CISO)/ IT teams/ IT Audit/ Data Protection Officer (DPO)/ Crisis management

- Information system security
- IT suppliers, if applicable
- IT update management
- Ongoing assessment: oversight and audit of cyber risk management plans

Human Resources

Cybersecurity corporate culture: the human component – ability to raise awareness and train teams

Finance/ treasury
Legal
Investor relations
Company secretary
Procurement
Communication
Internal audit
Risk/ Insurance management

- General business information: links between the business profile and the cyber threats
- Ongoing assessment: oversight and audit of cyber risk management plans
- Personal data

1. GENERAL BUSINESS INFORMATION:
LINKS BETWEEN THE BUSINESS PROFILE AND THE CYBER THREATS

This general business information is intended to allow the insurer to understand the extent of the organisation's exposure to cyber threats and to better assess what solution to offer.

WHY IS THIS IMPORTANT?

The list below represents the main general business information that would shape the insurer's profile of an organisation looking for cyber insurance coverage.

Main activities: sector, type of products and services

To help the insurer assess the organisation's exposure to potential claims and third-party losses.

Percentage of activity in consumer (B-to-C) business

B-to-C business can involve the processing of personal data, customer banking details and payment systems. This can generate a greater risk of third-party loss.

Percentage of activity in B-to-B business

To assess the potential for first party loss.

Geographical area (countries, jurisdictions)

Information about multiple or single offices and the location of supply chains, production processes and assets (tangible and intangible) is needed to determine the governing laws and jurisdictions.

To evaluate the political risks.

Turnover, income

Annual turnover is generally the strongest indicator of a policyholder's potential exposure.

IT security budget

Expressed as a value and/or as a percentage of the overall budget or of the IT budget.

For the insurer, this reflects the financial commitment of the organisation to cybersecurity and is a useful indicator of the risk maturity of the client organisation.

WHERE MIGHT YOU FIND THIS INFORMATION?

The following internal functions could help the prospective cyber insurance buyer to build the set of general business information:

- **Finance/ treasury**
- **Legal**
- **Investor relations**
- **Company secretary**
- **Communication**
- **Risk/insurance management**

2. CYBERSECURITY CORPORATE CULTURE:
THE HUMAN COMPONENT – ABILITY TO RAISE AWARENESS AND TRAIN TEAMS

The human component is a critical cybersecurity factor. Since digital transformation affects all the elements of an organisation, the ability of the organisation to raise awareness and train the operational teams, and not only IT people, is an important indicator of the level of development of cybersecurity risk management.

The insurer may therefore want to know more about the training of management and operational teams in information system security and control of outsourced services, including documentation.

WHY IS THIS IMPORTANT?

An insurer could look at whether IT security is a matter for a small group of dedicated persons or a general concern for everyone within the organisation. Each element might indicate the presence of a corporate culture in which IT security is embedded into the training of each user.

These indicators could feed into the insurer's general assessment of the organisation and its capacity to prevent damages/losses incurred by employees.

WHERE MIGHT YOU FIND THIS INFORMATION?

- **Human Resources**
- **Chief Information Security Officer (CISO)**
- **Data Protection Officer (DPO)**

3. INFORMATION SYSTEM SECURITY

A. IDENTIFICATION

Insurers may ask an insurance buying organisation if there is internal capacity to map all the physical systems inside and outside the organisation, as well as the data/information within these systems. Insurers may be interested to know what this data is and its uses. Important indicators include the ability to identify the most sensitive information and servers.

An organisation may not necessarily need to submit to an insurer the detailed information about the types of equipment and data. In most cases, it will simply state if such an exercise is performed or not.

WHY IS THIS IMPORTANT?

For insurers, the organisation's ability to identify sensitive data and critical equipment is a positive sign that the organisation is engaged in IT security.

WHERE MIGHT YOU FIND THIS INFORMATION?

- **CISO**
- **IT internal team**
- **IT suppliers, if applicable**

B. AUTHENTICATION: ROLES AND ACCESS

Insurers may especially value information about:
- Management of critical access to networks, equipment and maintenance;
- Management of all outside access for maintenance purposes with a clear differentiation between access rights.

WHY IS THIS IMPORTANT?

This is where organisations can demonstrate how access points are controlled, showing the relationship between the access points and the criticality of the information and systems.

WHERE MIGHT YOU FIND THIS INFORMATION?

- **CISO**
- **IT internal team**
- **IT suppliers, if applicable**

C. MOBILE WORKING: SECURITY POLICIES

Showing that measures have been taken to physically secure mobile devices can be helpful. This includes the encryption of sensitive data, in particular on hardware that can be lost. The organisation may also have adopted security policies for the network connection of mobile devices used in mobile working.

WHY IS THIS IMPORTANT?

This can be an indicator of how the risk of data leaks is managed.

WHERE MIGHT YOU FIND THIS INFORMATION?

- **CISO**
- **IT internal team**
- **IT suppliers, if applicable**

D. NETWORKS

Having networks accessible within a single space is considered a risk factor for the organisation, so seeing that networks are segmented and partitioned is likely to be a positive indicator for the insurer.

An insurer may ask:

- If and how networks are divided into different zones according to the criticality of the systems to avoid the spread of an attack from a compromised, low-critical system, such as a workstation, to a critical one, such as a server.
- What can be accessed from the outside and/or the internet (for instance, whether the HR and payroll system is accessible from the internet) and whether there is a partition between these areas.
- What security exists for Wi-Fi access networks and whether there are secure network protocols.
- Whether there is a secure access gateway to the internet and if services visible from the internet are segregated from the rest of the information system.
- How secure the dedicated network interconnections with partners are.
- What physical controls protect access to the server rooms and technical areas.
- What levels of redundancy are in place to ensure the availability of information and systems.

WHY IS THIS IMPORTANT?

Information about these elements gives the insurer an indication of how well the organisation can reduce the risk and mitigate an outage of its networks.

WHERE MIGHT YOU FIND THIS INFORMATION?

- **CISO**
- **IT internal team**
- **IT suppliers, if applicable**

E. SECURE ADMINISTRATION

Administration rights are a critical point. If abused, they pose some of the greatest risks. Evidence that these risks are well managed includes:

- Identification of each individual accessing the system by name and distinguishing of the generic user/administrator roles
- Allocation of the correct rights to the information system's sensitive resources
- Setting and verification of rules for the choice and size of passwords and protection of passwords stored on systems
- Changes to the default authentication settings on devices and services and use of a two-factor authentication where possible
- Prohibition of internet access from devices or servers used by the information system administration
- Use of a dedicated and separated network for information system administration and limitation of administration rights on workstations to strictly operational needs

WHY IS THIS IMPORTANT?

Specific treatment of administration rights reduces the risk of abuse.

WHERE MIGHT YOU FIND THIS INFORMATION?

- **CISO**
- **IT internal team**
- **IT suppliers**

F. INDUSTRIAL CONTROL SYSTEMS

Business units that depend on industrial control systems can face high repair costs and large business interruption losses if there is a successful cyber attack. Because of this loss potential, insurers are likely to ask for detailed information on operations and controls.

"Industrial control systems" is a general term used to encompass various types of control systems and related industrial process control instruments.

WHY IS THIS IMPORTANT?

Industrial control systems are a potential source of significant losses.

WHERE MIGHT YOU FIND THIS INFORMATION?

- **CISO**
- **IT internal team**
- **IT suppliers, if applicable**

4. IT SUPPLIERS

Outsourcing IT/cybersecurity-related functions does not remove the responsibility of an organisation for managing the associated risks.

WHY IS THIS IMPORTANT?

The quality and reputation of the IT suppliers could help insurers understand better the risks of accumulation in the case of a cyber attack.

It may also be highly relevant for the insurer to know if the organisation has mapped all outsourced cyber activities, with a list of the most relevant IT suppliers, as well as documentation about how outsourcing contracts are written and managed.

WHERE MIGHT YOU FIND THIS INFORMATION?

- **CISO**
- **IT manager**
- **Procurement**
- **Legal**

5. IT UPDATE MANAGEMENT

Insurers may ask organisations about their policies for updating the components of their information systems and anticipating software and system end of life/maintenance. The presence of some specific software that cannot be updated and the corresponding controls in place to mitigate vulnerabilities are also relevant information.

It might be useful to explain whether this process is centralised and automated or whether it relies on users acting voluntarily, regularly and independently to maintain their systems.

WHY IS THIS IMPORTANT?

The management of updates and obsolescence indicates how well the organisation mitigates threats that exploit vulnerabilities in software and completes the overall picture of the capacity of an organisation to face its cyber risks.

WHERE MIGHT YOU FIND THIS INFORMATION?

- **CISO**
- **IT internal team**
- **IT suppliers, if applicable**

6. ONGOING ASSESSMENT

OVERSIGHT AND AUDIT OF CYBER RISK MANAGEMENT PLANS

As cyber attacks are always possible, the organisation should have a systematic approach to identifying, checking and reviewing its weakest points.

It should inform insurers about the cyber risk management guidelines it is following. Beyond its own internal approach, the organisation may also use baseline guidelines such as those recommended by governments or their agencies, for example the French *"Guidelines for a Healthy Information System in 42 Measures"* or the *"Cyber Essentials +"* scheme in the UK, and international standards for information security management, such as ISO 27001.

Insurers might ask the organisation to explain how it would manage a cyber crisis. Cyber risk management plans can include a crisis management component to prepare the organisation for recovery after an event. As part of this plan, the organisation is likely to be expected to:

- Activate and configure the most important component logs
- Define and apply a backup policy for critical components
- Undertake regular checks and security audits, then apply the associated corrective actions
- Designate a point of contact in information system security and make sure staff are aware of who it is
- Have a defined security incident management procedure

WHY IS THIS IMPORTANT?

Insurers usually want some assurance that there is an internal audit strategy to verify and check that these points are effectively handled with an assessment and measurement of their performance.

Crisis management recovery plans are also important because they can directly affect the magnitude of the losses and the organisation's ability to resume activities after an attack.

WHERE MIGHT YOU FIND THIS INFORMATION?

- **CISO**
- **IT suppliers, if applicable**
- **Crisis management**
- **Internal audit**

7. PERSONAL DATA

Insurers may want to assess the extent of exposure to sensitive personal data, in order to understand:

- How much personal data is managed by the insurance buying organisation (health records, credit card records, other)
- The origin of these records (EU? US? Elsewhere?)
- Where the data is stored and processed
- Who within the organisation has responsibility for handling this issue
- What measures are in place to protect against attacks on these databases (encryption, for instance)
- If processing EU citizens' data, what has been done to comply with the EU General Data Protection Regulation (GDPR)?

WHY IS THIS IMPORTANT?

Personal data loss can be expensive for an organisation if it has to indemnify clients and third parties, particularly in countries with strong privacy regulation, such as the GDPR.

WHERE MIGHT YOU FIND THESE INFORMATION?

- **Legal**
- **Data Protection Officer (DPO)**

PART 1 CONCLUSION

The sections of Part 1 show that cybersecurity is a cross-functional issue whatever the size of an organisation. Senior management will need to involve most functions in preparing for a dialogue on cyber insurance with other market participants.

Compiling the information may be demanding, but also creates a virtuous circle because it also allows the organisation to identify where it can strengthen its policies and procedures.

Cyber insurance is an evolving market. Detailed information about an organisation and a description of how cyber risks are understood and managed can improve the preparation of the dialogue with insurers and intermediaries.

Based on the cyber risk factors described in Part 1 and some scenarios which we will describe in Part 2, the insurance buyer should be able to consider how cyber insurance could translate into their organisation.

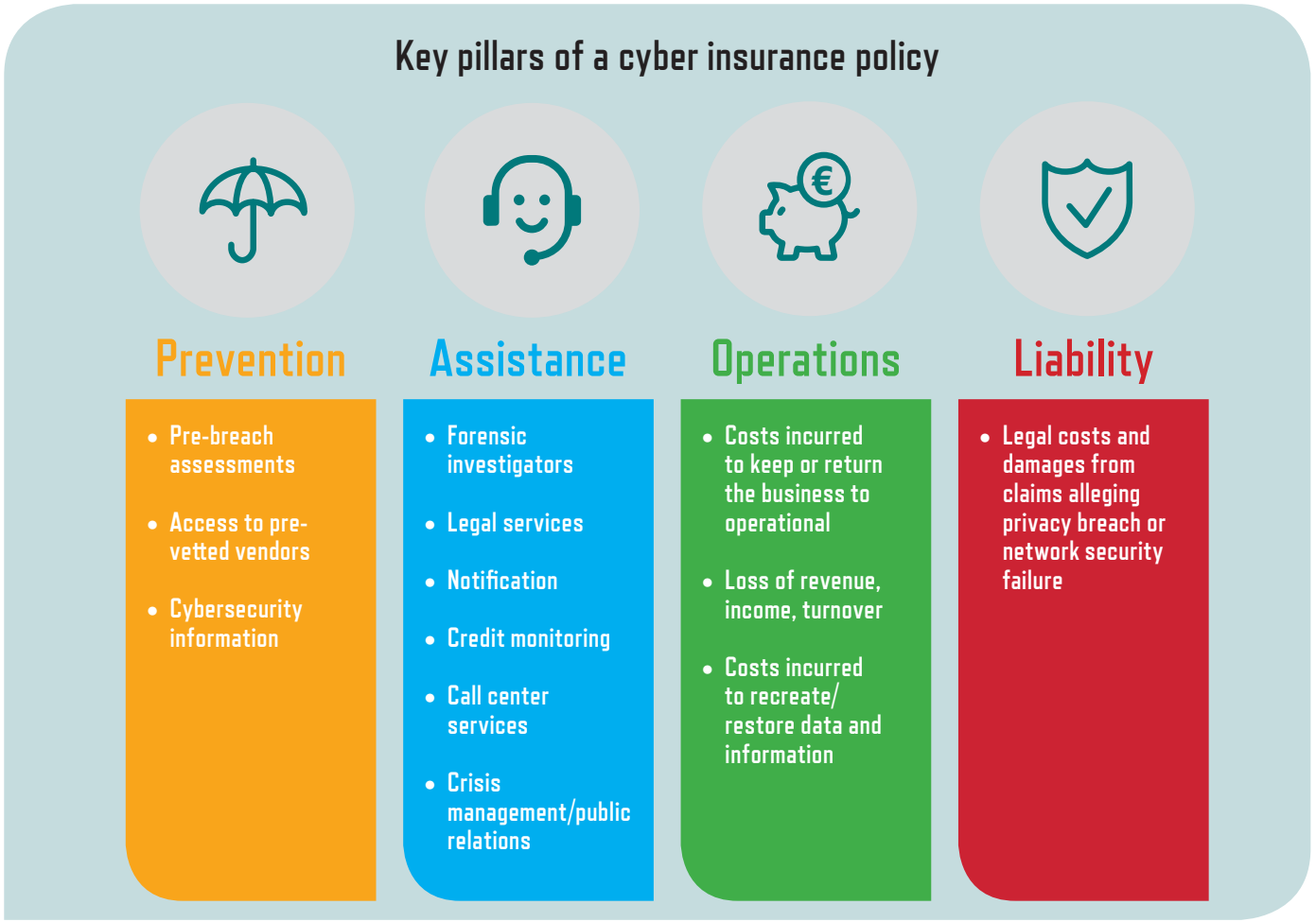
PART 2 – UNDERSTANDING CYBER INSURANCE OFFERS

This section is designed to help insurance buyers better understand the various cyber insurance offers and the different degrees of cover and service levels. This document will not enable an organisation to perform a detailed comparison of offers. It is designed to help the prospective insurance buyer review cyber insurance coverages with their intermediary or insurer to better understand what could make a cyber insurance policy responsive to the organisation's specific needs.

The risk factors described in Part 1 and the scenarios in the following pages should help the insurance buyer consider how cyber insurance could translate into their organisation.

It is crucial for an organisation to look at cyber insurance coverages because they can:
- Vary between offers and may affect how the insurance policy responds in the event of a specific cyber breach
- Help clarify potential gaps and overlaps between the coverage under a cyber insurance policy and other lines of insurance cover

If insurance buyers can evaluate different cyber insurance offers, it should help them explain their purchase decision to internal stakeholders. This way, the value of the cyber insurance policy is understood internally, and it effectively becomes part of the organisation's risk management strategy.



Prevention is one of the key pillars of a cyber insurance policy. Insurance buying organisations may get access to pre-breach assessments, pre-vetted suppliers or cybersecurity information for this purpose.

The organisation may benefit from assistance should there be a cyber incident, including forensic investigations, legal services, notification, credit monitoring, call centre services, crisis management and public relations. Organisations should prepare and test their cyber crisis management and incident response plans as part of their overall cyber risk management strategy, including data security breach notification procedures.

Cyber insurance may also support an organisation's operational recovery and may provide coverage for: costs incurred to keep the business operational or return it to operation; loss of revenue/ income/ turnover; and costs incurred to recreate/restore data and information.

Finally, a cyber insurance policy typically provides liability coverage for legal costs and damages from claims alleging privacy breach or network security failure.

This section contains:

- **Cyber coverage components** — a brief explanation of examples of cyber-related coverages
- **Coverage checklist** — sample questions to ask about cyber coverage
- **Scenarios** — how and when cyber insurance can be relevant following a cyber incident

1. CYBER COVERAGE COMPONENTS

The table below shows how cyber insurance policies may be able to respond at the various stages of a cyber attack or data breach. It displays in chronological order some possible corporate responses to a cyber incident, and when cyber insurance provisions might support the organisation.

Possible actions following a cyber attack or data loss	Examples of cyber coverage components
Investigate what happened	These issues likely require the specialised assistance of forensic investigators. Cyber policies may include coverage for forensic investigation costs following a cyber-attack or data loss.
Deploy technical measures to contain the loss and repair the IT system	
Assess legal/regulatory obligations	Legal services/assistance can be covered by cyber policies for breaches where it is reasonably suspected that confidential information has been compromised, generally in two forms: (i) post incident discovery and assistance in managing a breach (ii) defence costs following a claim alleging a breach of information
Execute a plan to comply with your obligations	
Assess the complaints/legal challenges you receive	
Implement the emergency plan to continue servicing clients	Cyber policies may include coverage for costs incurred as a result of a cybersecurity breach to maintain or restore operations and for income that is lost during the outage period.
Assess the cost of the cyber-attack, including possible loss of turnover	
If you are facing extortion: - Hire a response/threat consultant - Pay ransom, if legally allowed	Cyber policies may include services and costs to investigate and manage an extortion threat, including forensic experts and threat consultants.
If you are facing a regulatory investigation or a legal suit from third parties: - Hire legal advisers; prepare defence strategy - Pay damages	Cyber policies may include coverage for defence costs and damages that are agreed and/or assessed.

2. COVERAGE CHECKLIST

While every component of cyber coverage is important, there are some key terms and/or conditions in cyber insurance policies that can be used to distinguish coverage offerings. Understanding what could make a cyber insurance policy responsive to the organisation's specific needs is essential in deciding the right option for your organisation.

The list below suggests questions that organisations can ask their intermediary or insurers about coverage elements that may help distinguish one offer from another and identify which policy addresses the organisation's concerns. This is not an exhaustive list. Some terms and/or conditions and their importance can vary according to the risk factors of the organisation, such as the industry sector, revenue or contract requirements.

	Your concern	Ask the insurer	Yes/No
1	How can the organisation improve its management and resilience to cyber risks?	Does the policy offer pre-breach/ risk management services?	
2	Is expert help available in the case of a cyber attack or data loss?	Does the policy have a panel of suppliers for post-breach services including, but not limited to forensic firms, public relations firms and legal counsel?	
3	What if the organisation has only just started losing data but the breach was actually months ago?	Does the policy provide full cover for prior acts? A breach of a system can remain dormant for a long period before it causes problems.	
4	Can the organisation recover the full amount from all the elements of coverage?	Does the policy offer full limits for all coverage elements, including property/ casualty, regulatory and business interruption, or are there sub-limits for some elements?	
5	How much of the risk does the organisation have to retain?	Does the policy have a single retention and not separate retentions for each coverage element?	
6	Is it necessary to have a waiting period for business interruption cover even if there is a retention?	Can the business interruption coverage start from the first minute or first euro?	
7	What about the GDPR?	Does the policy specify that it includes GDPR coverage with full policy limits, to the extent insurable by law?	
8	Can the policy reimburse voluntary notification costs?	Are voluntary notification costs included in event management language?	
9	What if an employee is responsible for the breach?	Does the policy specifically include cover against rogue employees?	
10	Can the organisation be sure it is covered against cyber terrorism?	Is terrorism specified in the policy wording? What does it cover?	
11	What if the systems are out of date?	Are there exclusions for wear and tear or outdated software?	
12	Is there cover for extortion attempts?	Does the policy provide access to extortion advisors?	
13	What if suppliers have a network security failure?	Do suppliers have to be listed on the policy for coverage to apply?	
14	Can we decide who handles any cyber-related claims?	Is it possible to have firms added to the pre-agreed panel?	

3. SCENARIOS

The examples in this section show how a large mid-market organisation in Europe can use cyber insurance to optimise its overall cyber risk management, even if it does not have a dedicated risk manager or the internal resources to conduct a full cyber risk analysis. Note that these scenarios are valid at the time of this report, but could change as threats and/or coverages evolve.

Each example describes:

A. Scenario including some of the cyber risks
B. The outcome and possible insurance coverages

EXAMPLE 1. MANUFACTURER

A. Scenario: Manipulation and denial of access to the manufacturer's production database

A disgruntled employee with suitable privileges and knowledge of a manufacturer's information systems abuses their position within the organisation to perform a data manipulation and denial of service attack. Once in control, the employee methodically changes the data feeds, impacting the integrity of the production line and all goods being manufactured. The manufacturer ceases all production until a fix is found.

B. Outcome

The rogue actions would lead to significant interruption and costs. As the data that the organisation relies upon has been altered/manipulated, it may need a forensic investigation to determine how the information was amended and whether the information can be corrected, incurring significant costs. Additional resources may be required to correct or recreate the information.

With the manipulation of the data jeopardising the integrity of the produced goods, the manufacturer is likely to incur costs to purchase additional raw materials, increase production in other locations or source products from other providers to meet contracts, all in an effort to minimise the impact of the temporary outage.

Finally, the organisation could lose income that cannot be recovered during the manufacturing outage.

Interplay between cyber insurance policies and other lines of insurance

A cyber insurance policy in this scenario could potentially cover costs incurred to maintain or return the business to operational and the loss of income and costs incurred to recreate/restore data and information.

The manufacturing organisation may also benefit from assistance of forensic investigation specialists, legal services and crisis management services offered in a cyber insurance policy.

Other insurance policies may respond to elements of this type of incident: for example, a property all-risks policy may provide some coverage for the income loss, the additional costs incurred to minimise the impact of the disruption and the costs incurred to investigate and correct the data.

Coverage considerations of this scenario in the various cyber insurance offers

With respect to indemnity under different cyber insurance policies, some issues could impact potential coverage:

1. **Policies may only cover an outage if it is unintentional or unplanned.** If, in the scenario above, the organisation decided to take the plant offline to prevent further damage and minimise the overall impact, it could affect the indemnification available.

2. **Policies should provide coverage for the entity irrespective of the bad actor.** Whether an employee or an outside actor has gained unauthorised access (or exceeded authorised access) to systems and caused harm to the organisation, the policy should perform no differently.

3. **Policies generally exclude any coverage for improving systems following a data breach, whether the resulting loss of business income and increased cost of working are covered or not.** Some policies allow for some costs to terminate or repair systems that result in superior systems/software or other elements of betterment if the original version is no longer available and to seek to prevent a substantially similar event from occurring.

EXAMPLE 2. RETAIL

A. Scenario: Privacy breach

A spear-phishing attack aimed at employee emails allows hackers to breach systems and gain access to the log-in credentials and commercially sensitive information of a large retail organisation, including the personal information of clients. Records are sold on the dark web and details of the breach become public. Impacted commercial clients commence proceedings against the retail organisation.

B. Outcome

Following the discovery of the breach, the organisation is likely to require an investigation to determine how the breach occurred, what information was released and how to stop the breach, if it is continuing. Often, this requires bringing in forensic investigation specialists.

To manage the public narrative relating to the breach, the organisation may decide to bring in a crisis management/public relations team to help develop and execute a media strategy.

As the breach includes personal information, specialised assistance and legal guidance may be needed when handling all the aspects of the breach (a breach coach), separate from dealing with any claims against the organisation.

The organisation may have an obligation to notify individuals who could be affected by the breach and to offer credit monitoring, or it may decide to do this voluntarily. The organisation could also decide, with the assistance of its crisis management/public relations team, to offer "goodwill vouchers" for use at its stores to individual consumers.

If the organisation is facing legal proceedings brought by its clients, it will require legal representation and could have to pay damages at the conclusion of the proceedings. In addition, given the unauthorised release of consumer data, the organisation could face a regulatory investigation or proceedings, and ultimately may have to pay fines/penalties.

Interplay between cyber insurance policies and other lines of insurance

A cyber insurance policy in this scenario could potentially cover the legal costs and damages from claims alleging privacy breach or network security failure. The retail organisation may in this scenario also benefit from assistance of forensic investigation specialists, legal services, credit monitoring, call centre services, crisis management and public relations services offered in a cyber insurance policy.

Other insurance policies may respond to certain elements: for example, a professional indemnity policy may cover the costs incurred to defend and settle claims against the organisation and may also cover the costs incurred to mitigate the breach if coverage is provided for loss mitigation.

In addition, a directors and officers (D&O) policy may provide coverage for regulatory defence and for fines and penalties levied against a director or officer.

Coverage considerations of this scenario in the various cyber insurance offers

With respect to indemnity under different cyber insurance policies, there are some issues to highlight as they could impact potential coverage:

1. **Some policies require the insured organisation to receive express, written permission from the insurer before incurring any costs in relation to managing/mitigating a breach.** Otherwise, the insurer has the right to decline payment for the costs incurred prior to giving their consent. The organisation's CISO or technical team and their risk management team should coordinate actions. Understanding the requirements of the organisation's insurance policy is critical. Mitigating actions by the technical team in particular — however well intended — could affect the organisation's ability to recover financial loss through insurance.

2. **Policies may be subject to a retroactive date that provides a "hard start" for any breaches/network security failures, irrespective of when the breach/failure was discovered.** The insured should carefully review any proposed retroactive dates, as modules of coverage may be subject to different retroactive dates. As breaches may occur before the policy start date, retroactive coverage is an important issue for the settlement of subsequent claims.

EXAMPLE 3. TELECOMMUNICATIONS

A. Scenario: Cyber extortion, business interruption and privacy breach

The CEO of a telecom organisation receives an email demanding a ransom of €500,000 in bitcoins within 24 hours, or anonymous hackers will release sensitive customer information (a sample of which is provided in the email) and shut down critical business systems. The CISO hires a third-party forensic firm, which determines that the threat is real and that more than 500,000 sensitive customer records have been accessed.

The organisation notifies law enforcement, but before it can make a decision regarding the ransom, the hackers release half of the records obtained. They have also managed to make some critical networks inaccessible, so clients/employees are not able to access critical systems or process orders.

The organisation hires legal counsel to assist with notifications to individuals impacted by the breach. Another vendor is hired to handle the public relations response.

The critical systems remain down for ten days, impacting customer orders and general operations. The organisation suffers loss of income and incurs significant expenses related to the outage and to restore the business to operation. Two weeks after the breach notice was issued, a class action suit is filed alleging failure to properly protect private information.

B. Outcome

As the CISO may reasonably suspect a breach of the system given the anomalies discovered, the organisation may proactively pay for a forensic firm to end the threat and secure the systems. Additional forensic costs may be incurred to determine exactly what information was accessed by the hacker.

Further costs may include:

- Breach coach to assist with notices to affected individuals and to help the organisation determine what obligations it has and which laws (potentially in various jurisdictions) it will need to comply with.
- Credit monitoring and possibly call centre costs to respond to enquiries from concerned clients.
- Crisis management/public relations team to help develop and execute a media strategy and control the public narrative relating to the breach.
- Defence costs and possibly damages as a result of the class action lawsuit; more lawsuits may also follow.
- Coverage of the loss of revenue.

Interplay between cyber insurance policies and other lines of insurance

A cyber insurance policy in this scenario could potentially cover costs incurred to maintain or return the business to operational; loss of revenue and costs incurred to recreate/restore data and information.

A cyber insurance policy could potentially also cover legal costs and damages from claims alleging privacy breach or network security failure. The telecom organisation may benefit from the assistance of forensic investigation specialists, legal services, credit monitoring, call centre services, crisis management and public relations services offered in a cyber insurance policy.

Other insurance policies may respond to elements of this type of incident, for example, a professional indemnity policy might cover the costs incurred to defend/settle claims against the organisation and due to the lack of access to the system that causes clients financial harm. A professional indemnity policy might cover the costs to mitigate the breach, such as credit monitoring, public relations and a breach coach, if coverage includes loss mitigation.

Coverage considerations of this scenario in the various cyber insurance offers

With respect to indemnity under different cyber insurance policies, it is important to understand that some policies require the insured organisation to receive express, written permission from the insurer, before incurring any costs in relation to managing/mitigating a breach. Otherwise, the insurer has the right to decline payment for costs incurred before it gave its consent.

The CISO or technical team and the risk management team should, therefore, coordinate actions. Understanding the requirements of the insurance policy is critical. Mitigating actions by the technical team in particular — however well intended — could impact the organisation's ability to recover financial loss through insurance.

PART 2 CONCLUSION

The scenarios described in this section show that many cyber risks can be insured. Stand-alone cyber insurance policies provide a package of services and coverage that can support an organisation's risk management strategy, as well as provide assistance and financial support in the event of a cyber incident.

The coverage checklist can help organisations to understand the critical cyber coverage components that may help distinguish one offer from another, and to identify a cyber insurance policy addressing the organisation's concerns in dialogue with their intermediary or insurer.

The scenarios show that some elements of coverage could be available under other lines of insurance; buyers need to work with their intermediaries and insurers to understand potential cyber coverages and gaps within their current insurance policies and evaluate the value of a stand-alone cyber insurance policy for their organisation.

CONCLUSION

Today, organisations of all sizes are striving to address their cyber risks and integrate them into their overall risk management programme. In this respect, cyber insurance can be a useful tool, as this report clearly shows.

Preparing the information described in Part 1 may initially seem daunting, but we believe the rewards are worth the effort. This is because the exercise goes beyond helping organisations prepare a discussion with their insurer and intermediary; it serves to gauge the extent to which they are ready to face cyber risks generally, both in terms of preventing them and of reacting appropriately should an event occur.

Similarly, on the basis of this information, the insurer will be able to offer the coverage that is best suited to the organisation's needs, and, equally importantly, access to pre- and post-incident services.

The cyber insurance landscape is likely to evolve as insurers continue to develop solutions and cyber risks become easier to quantify. In practice, this means that there is no unique cyber insurance coverage. However, Part 2 of this guide offers a useful tool to help organisations evaluate cyber insurance offers.

The scenarios described give an overview of some typical coverage features and how they would work in an event, as well as related services that insurers are increasingly offering to their clients. A better understanding of what an organisation can expect from its insurer also helps strengthen its trust in insurance solutions.

Cyber risks will continue to increase and remain a fixture on the risk landscape. Organisations and individuals must prepare themselves to the greatest extent possible, both through preventative actions and mitigation where feasible.

We believe that a good understanding between potential insurance buyers, intermediaries and insurers will be key to the cyber insurance market reaching its full potential and serving the widest number and type of organisations. The authors hope that this report contributes to that understanding.

JOINT EXPERT GROUP

Names	Organisations	Title
Philippe Cotelle (Chairman)	Airbus Defence and Space	Head of Insurance Risk Management
Ramón De la Vega Rodríguez	Telefónica SA	Head of Corporate Risk and Insurance
Tobias Bunz	E.ON Insurance Services GmbH	Legal Counsel
Julia Graham	AIRMIC	Deputy CEO and Technical Director FBCI, FCII, Chartered Insurance Risk Manager
Aldo Cappelletti	UBS AG	Executive Director, Group Insurance Management
Yves Brants	NRB	Risk Manager
Typhaine Beaupérin	FERMA	CEO
Julien Bedhouche	FERMA	European Affairs Adviser
Nic De Maesschalck	BIPAR	Director
Vanessa Leemans	Aon	Chief Commercial Officer, Cyber Solutions EMEA
Shannan Fort	Aon	Cyber Insurance Leader | Global Broking Centre
Jean Bayon de La Tour	Marsh	Cyber Development Leader – Continental Europe
Sara MacArthur	Insurance Europe	Policy Advisor, General Insurance
Nicolas Jeanmart	Insurance Europe	Head of Personal Insurance, General Insurance & Macro-economics
Nils Hellberg	German Insurance Association	Head of Liability, Credit, Marine, Aviation, Accident and Legal Expenses Insurance, Assistance, Statistics
Scott Sayce	Axa	Global Chief Underwriting Officer of Cyber
Santiago Sanchez	Chubb	Head of Sales & Distribution, Spain & Portugal

NOTES

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

Insurance Europe
Rue Montoyer 51
1000 Brussels, Belgium
Tel: +32 2 894 30 00
E-mail: info@insuranceeurope.eu – www.insuranceeurope.eu
EU Transparency Register N° 33213703459-54

BIPAR
Avenue Albert-Elisabeth, 40
1200 Brussels, Belgium
Tel: +32 2 735 60 48
Email: bipar@bipar.eu – www.bipar.eu
EU Transparency Register N° 58041461167-22