airmic

Cyber risk

Understanding your risk and purchasing insurance

Guide 2017

HERBERT SMITH FREEHILLS

LLOYD'S

LOCKTON

RGL Forensics

Herbert Smith Freehills

As one of the world's leading law firms, Herbert Smith Freehills advises many of the biggest and most ambitious organisations across all major regions of the globe. Its insurance and reinsurance lawyers have an outstanding reputation in complex, high profile insurance and reinsurance disputes and for providing strategic legal advice and representation to corporate policyholders. Herbert Smith Freehills is Airmic's Preferred Service Provider on insurance law issues and has assisted Airmic in producing a number of its technical guides over the past few years. These practical tools assist Airmic members, Airmic partner brokers and insurers to promote legal certainty in their insurance contracts.

Lockton

Lockton is a global professional services firm with 6,500 Associates who advise clients on protecting their people, property and reputations.

Lockton has grown to become the world's largest privately held, independent insurance broker by helping clients achieve their business objectives.

Clients across the globe count on Lockton for risk management, insurance and employee benefits. Our experts tailor solutions to the unique needs of each company and individual just about anywhere. Our long-term relationships with underwriters around the world allow us to structure and negotiate comprehensive coverage at the best price possible.

Lloyd's

Lloyd's is the world's specialist insurance and reinsurance market.

With expertise earned over centuries, Lloyd's is the foundation of the insurance industry and the future of it. Led by expert underwriters and brokers in more than 200 territories, the Lloyd's market develops the essential, complex and critical insurance needed to underwrite human progress.

Backed by diverse global capital and excellent financial ratings, Lloyd's works with a global network of over 4000 insurance professionals to grow the insured world – building resilience for businesses and local communities and strengthening economic growth around the world.

The Lloyd's market offers a variety of cyber policies covering everything from financial pay-outs after a cyber-attack and on-the-ground support during the period of crisis, to business interruption, pre- and post-breach risk management, and helping businesses to deal with operational, financial and reputational impacts. For more information visit lloyds.com/cyber

RGL Forensics

RGL Forensics is a multidisciplinary forensic accounting and consulting firm delivering accurate and reliable financial analysis to the insurance, legal, corporate and public sectors. Operating worldwide from offices on five continents, we serve global insurance companies, multinational corporations, leading law firms and government entities.

RGL specialises in the quantification of economic damages and financial analysis in claims of all kinds. We provide comprehensive forensic accounting, fraud investigation, expert testimony and forensic technology services, going beyond the numbers to deliver financial clarity in the most complex situations.

As detectives of the financial world, the professionals at RGL use advanced tools, proven methodologies and sophisticated modeling to deliver sound evidence and reports that meet or exceed global standards for financial evidence. Clients in the insurance, legal, corporate and public sectors rely on RGL to deliver financial analysis that withstands the toughest scrutiny.

Contents

1 Introduction

The rapid digitalisation of all businesses means that the use of technology and the associated cyber risk is now truly a strategic issue. As digitalisation grows, so does vulnerability to the associated risks. Cyber hackers are notoriously opportunistic and continuously create ways to attack new technology and overcome defences. The global 'WannaCry' malware attack that took place in May 2017 has demonstrated the growing scale and impact of cyber events. The effective management of cyber risks can help build stakeholder trust, provide customer assurance and deliver competitive advantage.

Cyber risk continues to feature in the top three risk concerns of Airmic members and two-thirds are concerned that a cyber event resulting in business interruption may affect their business in the next three years (Airmic transformation of the risk profession survey, 2017). However, confidence in cyber risk management is low. Less than a third of members are satisfied with their organisation's ability to manage cyber risks (Airmic transformation of the risk profession survey, 2017).

The cyber insurance market has developed rapidly. Policies with greater limits and an increasing focus on first-party losses are beginning to emerge. There is a sense of developing standardisation of covers across the market, making the purchasing process easier. However, just 38% of organisations are buying relevant cyber insurance cover *(PwC Global State of Information Security Survey, 2017)*.

Airmic members report that the cyber risk is very high on the risk agenda but is often patchily implemented, with little collaboration between the risk, information technology and other related functions. However, the risk manager has a clear role to play. Risk managers should have:

- the understanding of the business at an enterprise level to visualise how a distinct cyber event would be felt across the business and affect internal and external stakeholders
- the internal connections with HR, Audit, the Board, Finance, etc. to develop cyber risk management beyond technical protection into an enterprise-risk management framework
- the understanding of the insurance market and its associated services such as external crisis management support, to provide additional support and risk control beyond internal security.

This paper aims to help risk managers lead the cyber risk conversation. The paper is an update of the 2012 paper, 'Airmic review of recent developments in the cyber insurance market' and provides a framework for Airmic members to assess their cyber risks, before summarising the cover available and the underwriting information required to buy such cover.

2 What is cyber risk?

Airmic members state repeatedly that it is challenging to appreciate fully the cyber risks facing their organisations. Cyber incidents can have several wide-ranging impacts on the business. The possible consequences of a cyber event are summarised in Figure 1.

Figure 1 Business Consequences of cyber risk events

Data and privacy breach costs
- Notification and reporting costs
- Other regualatory fines and costs
- Other third party costs

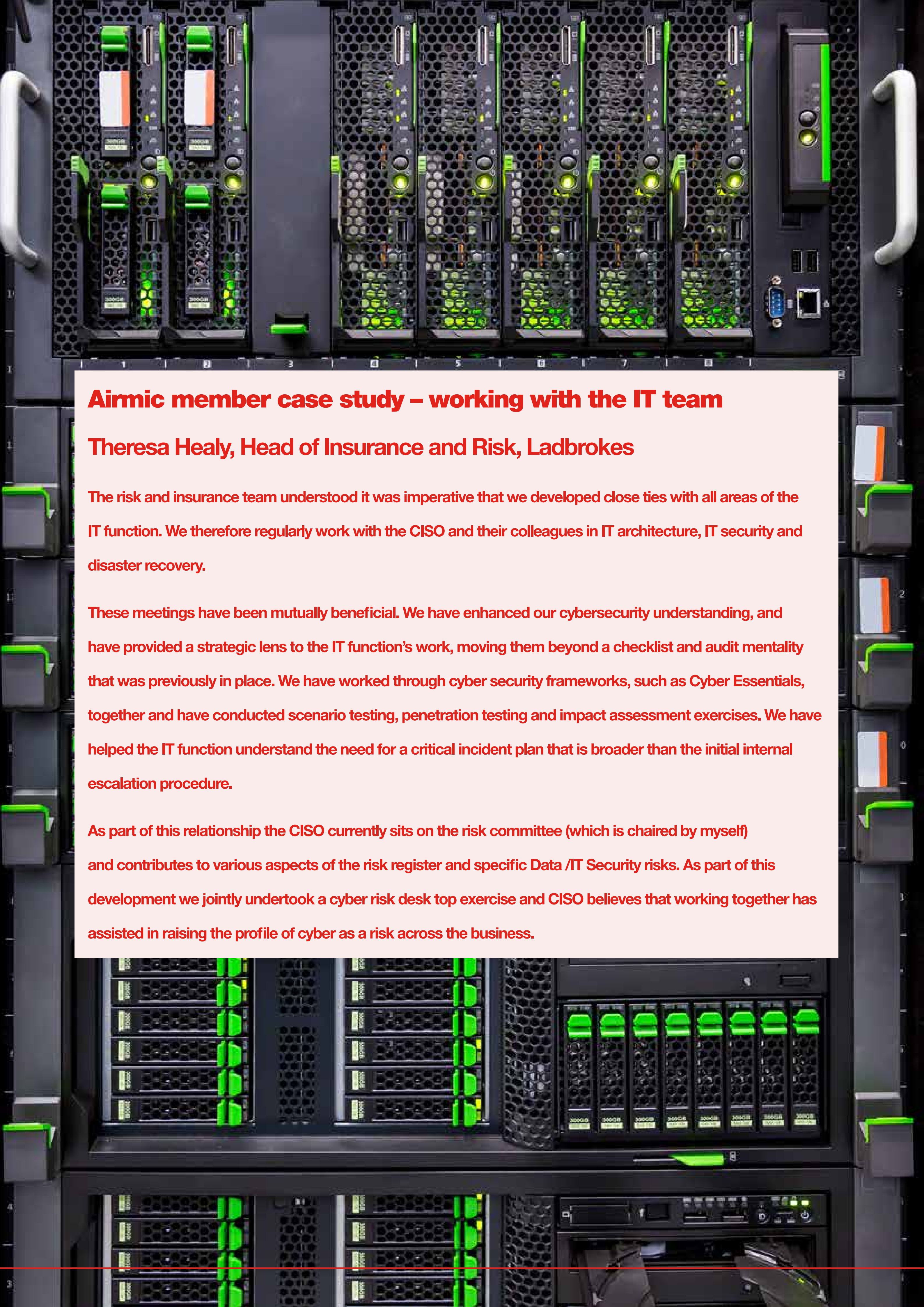
Physical damage and business interruption
- Loss of revenue
- Additinoal costs of working e.g. forensic and crisis managements costs
- Restoration costs to software, systems, data

Fraudulent payments
- Extortion / ransom
- Fraudulent payments
- Fraudulent transactions

Intellectual property breach / theft
- Loss of information costs
- Restoration costs

Reputation and brand damage
- Loss of customers
- Loss of revenue
- Crisis management and PR support costs

Understanding the likelihood of each of these impacts will be hampered if risk managers have limited working relationships with the Chief Information Officer (CIO) and Chief Information Security Officer (CISO), who have the greatest working knowledge of cyber risk controls in the business. Risk managers report that CIOs and CISOs can be reluctant to share details of the cyber threats facing the organisation and may appear overly confident in the security controls in place, with this confidence influencing the Board when considering the risk. However, cyber risk is a strategic risk and it is critical that the Board and relevant senior management understand this risk.



Airmic member case study – working with the IT team

Theresa Healy, Head of Insurance and Risk, Ladbrokes

The risk and insurance team understood it was imperative that we developed close ties with all areas of the IT function. We therefore regularly work with the CISO and their colleagues in IT architecture, IT security and disaster recovery.

These meetings have been mutually beneficial. We have enhanced our cybersecurity understanding, and have provided a strategic lens to the IT function's work, moving them beyond a checklist and audit mentality that was previously in place. We have worked through cyber security frameworks, such as Cyber Essentials, together and have conducted scenario testing, penetration testing and impact assessment exercises. We have helped the IT function understand the need for a critical incident plan that is broader than the initial internal escalation procedure.

As part of this relationship the CISO currently sits on the risk committee (which is chaired by myself) and contributes to various aspects of the risk register and specific Data /IT Security risks. As part of this development we jointly undertook a cyber risk desk top exercise and CISO believes that working together has assisted in raising the profile of cyber as a risk across the business.

2.1 Identifying and understanding an organisation's cyber risks

No two organisations will have the same cyber risk. Some organisations will worry about the loss of the proprietary data they hold, whilst others will be concerned about disruption to the control systems their business relies on. As a starting point, Airmic members should understand what their data and information 'crown jewels' are. What data or processes are most critical to the business?

> **'Businesses need to ask themselves three questions:**
>
> **What are our fundamental cyber assets?**
>
> **Where do they sit within the business?**
>
> **What happens to the business if any of those assets are compromised?'**
>
> **Ben Hobby, Partner, RGL Forensics**

The cyber threat environment explained

The threat environment can be divided into five main categories, and the relevance of each of these to the business must be understood;

- **Criminal**
  With an aim of theft of intellectual property, data, funds, etc.

- **Terrorist or state**
  With an aim of widespread disruption, e.g. disruption to infrastructure or economy

- **Malice**
  With an aim to disrupt or damage a specific company, e.g. an attack from a disgruntled customer or employee

- **Hacktivist**
  With an aim to achieve political or social goals

- **Internal**
  No aim, but cyber event caused by internal employee negligence, error, loss of hardware, etc.

Figure 2: **Six first questions to ask to understand the key cyber threats to the business**

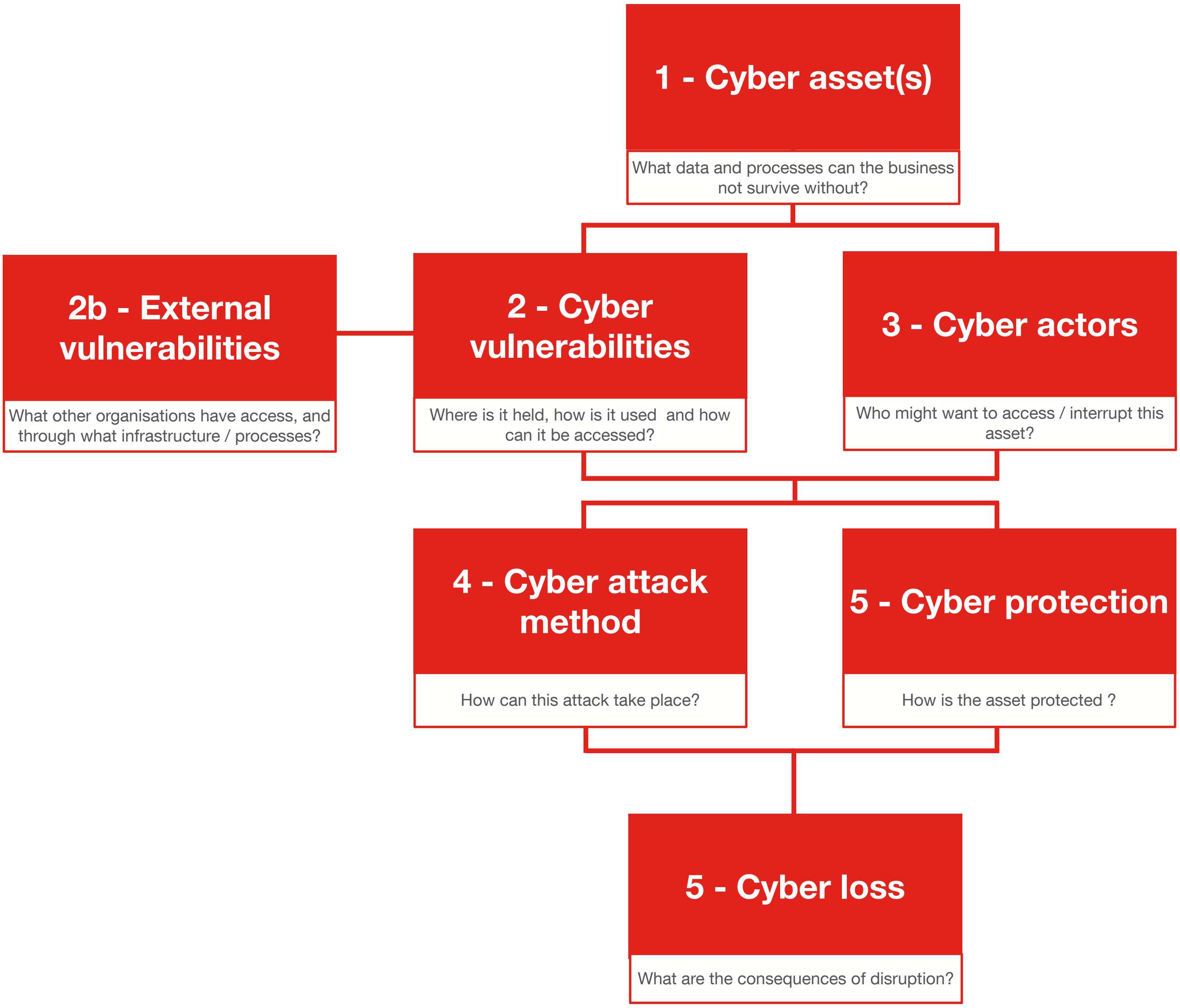

1 - Cyber asset(s)
What data and processes can the business not survive without?
2b - External vulnerabilities
What other organisations have access, and through what infrastructure / processes?
2 - Cyber vulnerabilities
Where is it held, how is it used and how can it be accessed?
3 - Cyber actors
Who might want to access / interrupt this asset?
4 - Cyber attack method
How can this attack take place?
5 - Cyber protection
How is the asset protected ?
5 - Cyber loss
What are the consequences of disruption?

Figure 2 provides a series of questions that organisations can ask themselves to begin understanding their cyber risks.

- The answer to Question 1, identifying the cyber asset(s), will be unique to every business: personal or commercially confidential data, healthcare information, intellectual property, payment processes and control systems are some of the most obvious examples.

- After understanding the cyber assets that are most critical to the business, risk managers will need to answer questions 2 to 6 by identifying the actors, vulnerabilities and outcomes of a cyber-attack that targets these assets. This will help them establish the cyber events that pose a risk to their organisation. Table 1 provides some examples of answers to the other questions, and can be used to help risk managers structure a conversation with their IT teams.

Table 1: Internal cyber risk assessment

Cyber vulnerabilities The points of access (physical and via systems) into the organisation’s system and subsequently to the cyber asset in question	**Cyber actors** The malicious and non-malicious parties and causes of a cyber event. These can be both internal and external
• Own IT infrastructure, e.g. hardware and software • Online communications • Bring your own devices and third-party hardware • Own employees • Own customers • Operational technology affecting plant and equipment Organisations are vulnerable through their connections with other organisations. Identify the processes and infrastructure connecting the two: • Outsourced infrastructure and software • Managed services provider	• Activists / hacktivists • Competitors • Organised criminals • Insider threat, including rogue or vulnerable staff • State sponsored attackers • Terrorists Additionally, the following non-malicious parties and events may lead to a cyber incident: • IT system failure • Power failure • Human error by staff, suppliers, customers
Cyber attack method Cyber actors employ several techniques to access systems. Risk managers will need to familiarise themselves with the techniques below:	**Cyber protection** Organisations must develop control processes and technology to protect again cyber attacks. Training their people to identify and defend against attacks is also important
• Ransomware • Distributed denial of service • Trojan • Email attachments • Phishing • Social engineering, often targeting key staff, e.g. Finance team • Continued attack of known vulnerabilities • Advanced persistent threat • Open source intelligence	• Antivirus solutions • Patching of detected vulnerabilities • Firewalls • Network segregation • User privileges, passwords, etc. • Education and training of staff • Reporting and incident response plans aligned to crisis management plans • Penetration and vulnerability testing Detection measures are equally important: • Data leak protection/prevention systems • Identifying leading and lagging indicators of a breach
Cyber loss Organisations must understand the consequences of each cyber event they identify as a threat (refer to Figure 1 for more information): • Data and privacy breach costs - physical damage and business interruption • Fraudulent payments - intellectual property breach / theft • Reputation and brand damage.	

2.2 Cyber risk governance

The cyber landscape is changing continuously. Organisations can be targeted by organisations with political goals or financial motives, and the tools available to these hackers is growing. Figures vary but a common figure is a 25% increase in cyber-attacks on organisations each year.

Regulation is keeping up with the threat and organisations will need to be aware of relevant regulations such as the EU General Data Protection Regulations. These regulations highlight cyber risks as strategic business risks. Therefore, appropriate governance arrangements must be in place to take advantage of the opportunities available through cyber developments and to evaluate the risk appetite for the organisation.

The British Standard Institution is currently developing a cyber risk resilience standard, that addresses the role of the Board and executive management in cyber risk governance.

Figure 3 summarises an appropriate structure for effective cyber risk governance. Regardless of how the governance framework is structured, it should enable the following:

- Effective oversight by the Board and executive management, ensuring that cyber resilience is considered part of the overall organisational goals, including highlighting an individual, with relevant technical experience on the Board to be responsible for IT security and data protection

- Cross-functional approach to cyber management and communications, including the Board, IT, Legal, Finance, Risk, HR and PR and Communications

- A mature cyber risk culture, where cyber risk management is embedded into the business decision process at all levels of the organisation

- Recognition of cyber regulations across all territories the organisation operates in, relevant cyber standards and frameworks, and industry good practice

- Appropriate resource allocation in terms of cyber risk controls, training and testing

- A structured communication plan with partners and external stakeholders

- Regular reporting to and risk management representation among the Board, enabling an understanding of what cyber risk means to the organisation so that it can answer questions such as:

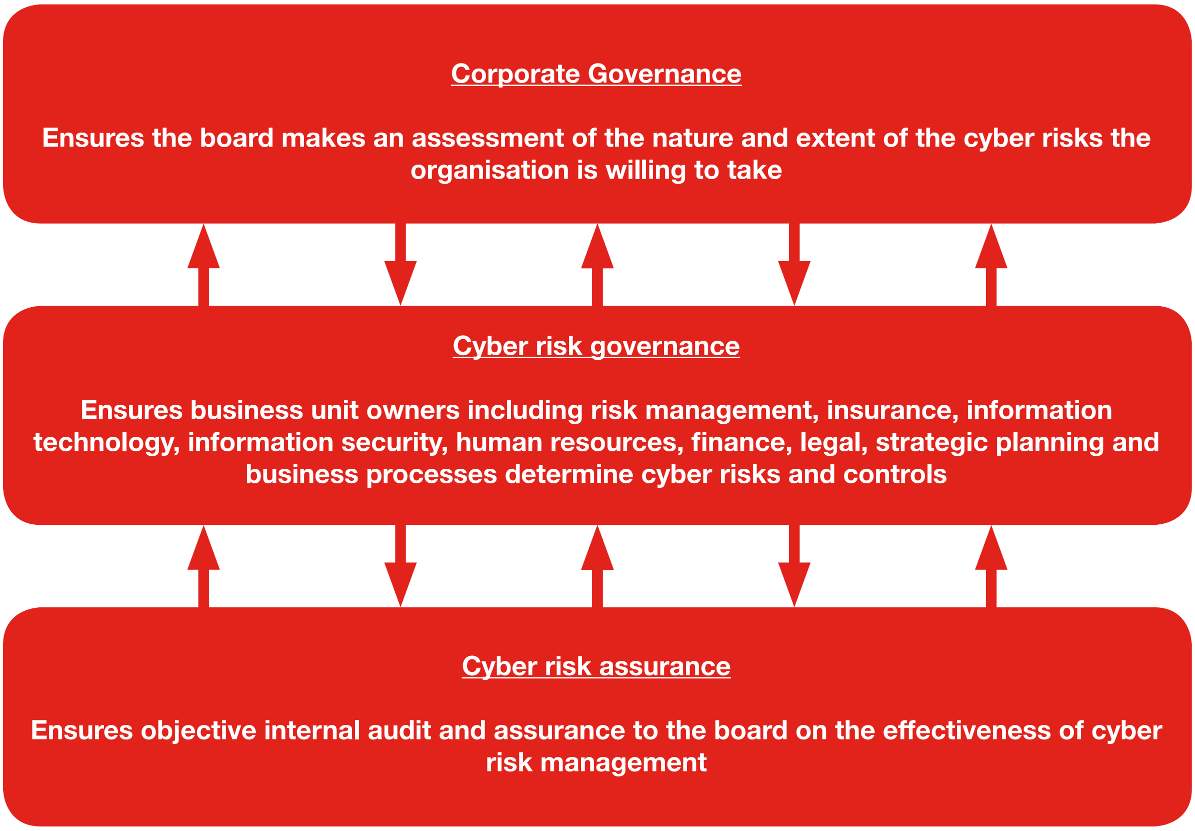
    - What are your organisation’s technological infrastructure, systems and processes?

    - What are your organisation’s vulnerabilities to this infrastructure?

    - What strategies are in place to mitigate those risks?

    - Why were decisions on cyber security and cyber insurance taken?

Figure 3: **An example cyber risk governance framework**



Corporate Governance

Ensures the board makes an assessment of the nature and extent of the cyber risks the organisation is willing to take

Cyber risk governance

Ensures business unit owners including risk management, insurance, information technology, information security, human resources, finance, legal, strategic planning and business processes determine cyber risks and controls

Cyber risk assurance

Ensures objective internal audit and assurance to the board on the effectiveness of cyber risk management

***Cyber risk governance group reports directly to Board if there is no risk committee**

Risk managers report that the Board-level understanding of cyber developments and risk can be limited, unless there is clear evidence of a competitor having suffered an attack or increasing their cyber risk management. Over half of Boards discuss their cyber risk once a quarter *(Lockton UK Cyber Security Survey, 2017)*. However, as the cyber threat is advancing at such a rapid pace, those Boards discussing this less often would be wise to consider doing so more regularly, or to ensure they receive information on the subject regularly, if they meet less than once a quarter. Airmic members who have engaged the Board on cyber risks report that working through cyber standards and carrying out cyber scenario analysis can help develop Board-level understanding. Both techniques are covered within the following sections.

2.3 Cyber risk standards and frameworks

There are a huge number of cyber standards and good practice guides. These standards are used by organisations to benchmark their cyber security and highlight areas of weakness. Additionally, taking the time to work through the standard helps risk managers to improve their own understanding of cyber security and develop the relationship between the risk and IT functions.

Standards typically provide guidance on the full cyber risk assessment, including identifying cyber processes and procedures within the organisation, undertaking gap analysis of controls by benchmarking themselves against the standard, independent testing of controls, effective reporting across the business, and continuous monitoring and improvement.

Organisations will need to select the standard that best reflects the nature, size and complexity of their business and cyber processing. Relevant standards for risk managers to be aware of include;

- **ISO 27001/02 (global)**
  Best practice for implementing an information security management system that complies with the relevant laws and regulations, as well as the UK Cyber Essentials scheme

- **OECD Digital Security Risk Management for Economic and Social Prosperity (global)**
  Summarises key principles of data security and outlines how these can be applied to businesses, with the aim to increase trust and innovation in the digital economy.

- **Cyber Essentials scheme (UK)**
  Structured around ten steps to cyber resilience that focus on five key cyber security controls; boundary firewalls and internet gateways, secure configuration, access control, malware protection and patch management.

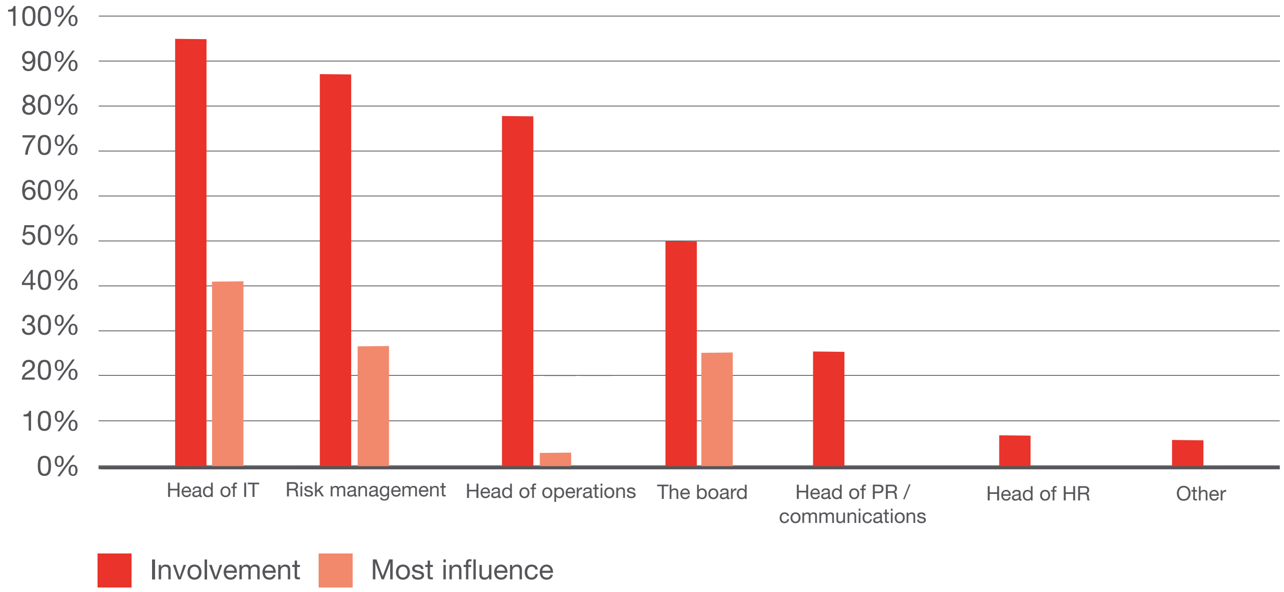
- **NIST cyber security framework (US)**
  A risk-based approach to managing cyber security risk. Businesses can use the framework to identify the most critical infrastructure of the business and develop effective cyber security to protect it.

- **Sans 20 (US)**
  Highlights the top 20 cyber controls that organisations can put in place to manage their cyber risk. Controls range from preparing an inventory of all devices on the network, to security skills assessment and training of staff, to malware defences.

2.4 Making use of cyber scenarios

Like all risk events, scenario planning is one of the most useful techniques for understanding how the business would be affected and respond to a cyber incident. Figure 4 demonstrates the parties typically involved in cyber scenario planning *(Lockton UK Cyber Security Survey, 2017)*: 96% of organisations involve IT in their scenario planning, and 42% advise that the IT function has the most influence on the decisions made during the exercises.

Figure 4: The involvement and influence of business functions in cyber breach scenario planning *(Lockton UK Cyber Security Survey, 2017)*



Airmic believes that risk managers should have greater influence in cyber scenarios. Table 2, based on the seven stages of scenario analysis presented in Airmic's 'Scenario analysis: A practical system for Airmic members' demonstrates where risk managers should be having an influence.

Primarily, risk managers should ensure that the focus of scenarios is not simply on IT systems controls and security, but also looks at the operational impact on the business, and that the output of these scenarios is validated and signed off by key areas of the business and external parties.

'Traditionally, insurers focused on technical cybersecurity information when assessing risks. However, we are now looking to go beyond this and gain a wider understanding on how an organisation would respond to and be affected by a cyber event. Conversations with the IT functions, business continuity, and risk and insurance are useful.'

Paul Bantick, UK Focus Group Leader, Technology, Media and Business Services, Beazley

Table 2: **The role of the risk manager in cyber scenario exercises**

Scenario stage	Aims	Role of the risk manager
Definition and approach	Agree the organisation-wide aims for the exercise	• Ensure that cyber risk concerns reported across the organisation are reflected in the cyber scenario tested
Framework and planning	Agree the specific scenario to be tested and identify participants	• Consider how likely the organisation is to be identified as a cyber attack target, going beyond cyber security weaknesses to consider the organisation's position and role in the wider economy • Identify participants from all functions that can be affected or can affect the cyber scenario
Assessment and measurement	Identify the impact on areas of the business	• Identify the relationships between the cyber scenario and other scenarios that have been considered (across all risk categories) - highlighting the wider business impact
Validation and modelling	Model the financial impact and validate the credibility of the scenario	• Assess the full business cost across the business from moment of attack through to full recovery, using wider business interruption expertise • Map costs against potential insurance solutions and controls beyond technical cyber security • Advocate the added value nature of insurance policies and the experts available as part of coverage • Validate the credibility with other business units
Reporting and sign-off	Present to relevant committees and management	• Integrate scenario output within the overall risk governance and reporting framework incorporating risk and audit committees and the Board
Communicating output	Integrate the lessons and actions from the analysis across the business	• Prepare actions for all staff for identifying, reporting and responding to a cyber risk event • Discuss the key cyber threats identified with insurers, allowing for a more informed conversation
Process review	Review and update scenarios periodically	• Integrate the cyber scenarios into the overall scenario handbook • Initiate reviews of scenarios as internal and external events, relating all risk categories, may indicate a potential change to the cyber risk.

Airmic member case study – validating cyber scenarios

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

We use cyber scenario analysis to identify cyber events that are a strategic risk for the business. We aim to create cyber risk scenarios that are; credible, quantifiable and, most importantly, validated across the business and our cyber experts.

For each type of cyber-attack, where we have identified an exposure, we consider the following:

1. The operational risk management

   The CIO and CISO identify and test the cyber security controls and procedures in place to prevent or mitigate a cyber incident and then identify any vulnerabilities.

2. The compliance assessment

   The legal team, including the data risk officer, assess the impact in terms of our regulatory requirements and obligations

3. The enterprise risk management

   The risk function works with the business owners to identify how each area of the business would be impacted, whilst being aware of how our stakeholders would also be affected.

4. The phasing of consequences

   The scenario also includes phasing of the quantified impact, from crisis to remediation and vigilance since the nature of those impacts and parties may vary.

5. We consider Indicators of Threats and Maturity against the scenario

   When looking at threats we consider the availability of the technical means to operate such attack. When looking at maturity we consider the status of the organisation with respect to its peers allowing to assess how identifiable a target it can appear.

6. Test of controls

   The operational risk managers (IT) would review the cyber security controls currently in place against the complete scenario and propose new measures to address those exposures.

This process produces credible scenarios to present to the Board, for discussion, as well as risk controls and risk transfer options. Decisions on control priorities and allocation of resources can then be made.

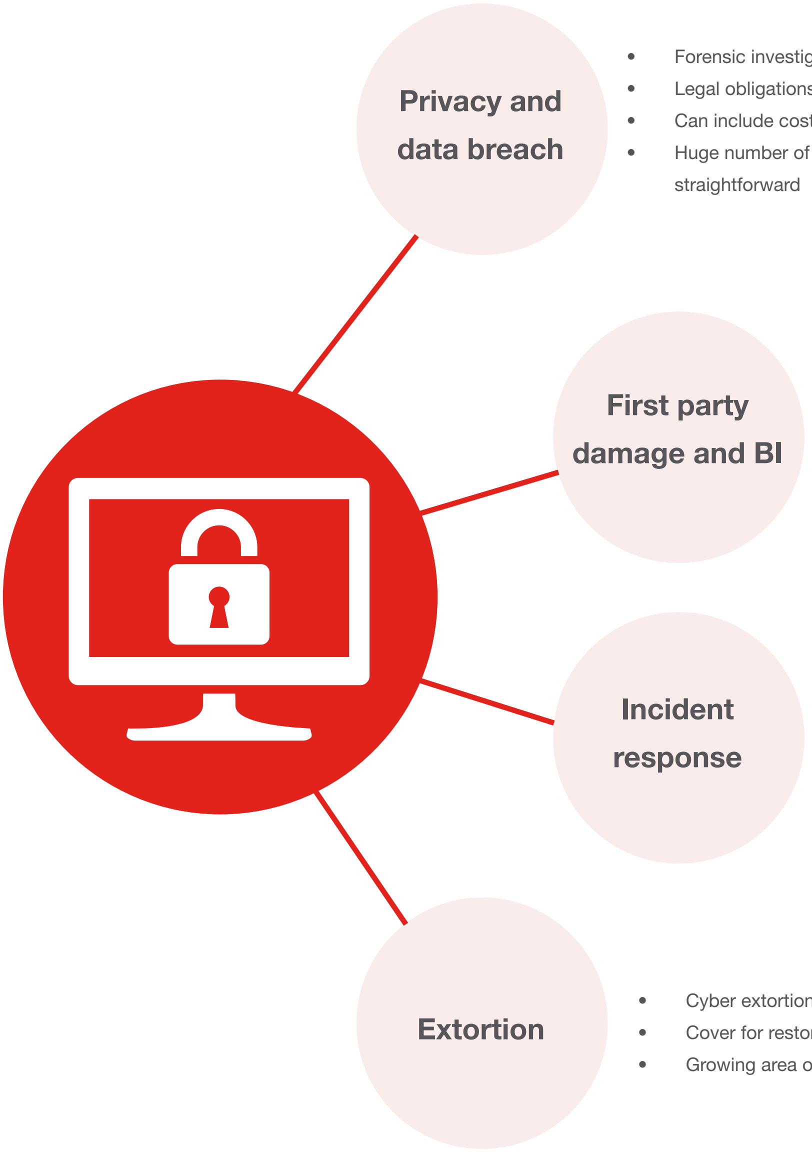
3 Cyber insurance

The uptake of cyber insurance is growing but remains relatively low. More than half of risk and insurance managers (52%) plan to transfer cyber risks causing BI to the market and just under half (48%) plan to transfer data loss and theft arising from a cyber attack (Airmic transformation of the risk profession survey, 2017). . Members cite several reasons for this: their organisation would prefer to spend on internal cyber controls, the absence of meaningful capacity, the high cost of cover and uncertainty over what coverage entails, including whether claims would be paid. However, Airmic members and brokers are beginning to recognise a shift towards relevant cover over the last year. Therefore, Airmic members are encouraged to review the cyber insurance market.

Figure 5 provides a summary of cyber cover currently available. Airmic members should compare the output of their cyber threat assessment (Figure 2 and Table 1) when identifying which portions of cover are relevant to them.

> **'Cyber insurance is the fastest-growing area of the market, and we are seeing a major increase in the relevance of cyber products and the number of companies purchasing cover, with great strides made in the last 12 months particularly. Products are broader than ever before, as insurers attempt to differentiate themselves from one another. As more loss data is available, clients are requesting and achieving the capacity they require too, with towers of up to $500m and growing becoming available.'**
>
> **Carl Moore, Partner, Lockton Companies LLP**

Figure 5: Cyber insurance - key modules



Privacy and data breach

- Forensic investigation costs
- Legal obligations, e.g. notification and reporting
- Can include costs due to third parties, including compensation
- Huge number of carriers, and acheiving high capacity is relatively straightforward

First party damage and BI

- Replacement and restoration costs after damage to data, systems and occasionally physical property
- Loss of profits and additional costs of working following damage
- Limited number of carriers, and some availability through traditional PDBI policies

Incident response

- Support to the organisation following cyber incident
- Forensic costs, crisis management, legal and PR costs
- Provided as standard for a variety of standalone cyber covers

Extortion

- Cyber extortion negotiation and ransom costs
- Cover for restoring data / system access where ransom isn't paid
- Growing area of cover due to proliferation of costs

> **'Given the relative infancy of the UK cyber insurance market and the limited number of paid claims to date, insureds are often dubious that cyber insurance policies will pay against the losses they eventually suffer. It is vital that insurance and risk managers take the time to map the digital assets of their business against the threats they face and the scope of cyber insurance cover within their existing policy suite. Only then will they be able to clearly articulate the cover they require to insurers and increase the contract, coverage and claims certainty.'**
>
> **Greig Anderson, Partner, Herbert Smith Freehills**

3.1.Comparing against other covers

Cyber catastrophes are likely to impact on a huge number of policies, e.g. property damage, liability, D&O, etc. and therefore cyber cover can overlap with many traditional covers. A gap analysis of the cover already in place is essential. The wordings of cyber polices differ widely, and traditional polices are often silent on cyber threats so insurance managers must be clear of where exclusions are in place and how policies will fit together. Specific examples include:

- **Property damage cover**
  Traditional property damage / business interruption cover is one of the greatest areas for overlap. Typical examples include:

  - Insurers not excluding physical property damage as a consequence of a cyber event, e.g. an attack on an industrial control system

  - Recognition of data as ‘property’, providing cover for data restoration after a cyber attack, e.g. a virus corrupting data or malware incident

  - Business interruption coverage extending to ‘cyber type’ events such as denial of service attacks or cloud interruption

  Cyber cover through the property market can be particularly relevant where the organisation is more exposed to attacks that seek to disable industrial control systems rather than tamper with data. Insureds will need to take extra care, and work through claims scenarios with their insurers to understand which cyber consequences are covered.

- **Crime cover**

  It can be difficult for large organisations to achieve meaningful stand-alone cover for cyber crime incidents such as CEO fraud and the scamming of financial staff to make fraudulent payments. Large organisations may be better served through their own separate crime policy.

- **Ransom cover**

  Many insurers report a doubling of cyber extortion incidents between 2015 and 2016, as organisations hold more data which can be used to hold them to ransom. Cyber polices are likely to be more relevant than traditional kidnap and ransom cover, which focuses more on ransom negotiation. Cyber products will take advantage of specialist cyber vendors who can often avoid the ransom by releasing the data themselves.

Insurance managers may find that their traditional polices are silent on the cover available for the variety of cyber events that may impact their organisation. If an organisation seeks to rely on a silent cover for a cyber loss they may face challenges based on non-disclosure or meeting the requirements of the Insurance Act. Insurance managers should therefore consider the benefits of discussing cyber risk underwriting information (see section 3.3) with their insurer and brokers for other covers that may be called upon in the event of a cyber loss.

> **‘We consider the property market to be the natural home for physical loss or damage and resulting business interruption when caused by a cyber-attack. I.e. we think that traditional property policies should cover traditional property losses even when the loss results from cyber-attack. In addition, a few property insurers such as FM Global are now offering much wider first party coverage for non-physical damage losses. This includes the cost to repair, replace and restore damaged data, denial of service events, cloud computing disruption etc. We work closely with our clients to gain a better understanding of their cyber risk, using a series of cyber questions and discussion topics.’**
>
> **Robert Beattie, Senior Underwriter, FM Global**

3.2 Gaining internal support for cyber insurance

Airmic members frequently advise that their organisations are more comfortable in allocating budget to internal cyber security controls, rather than purchasing cyber insurance, which is comparatively less well understood. Insurance managers will often find it challenging to promote the benefits of cyber cover.

Insurance managers who do purchase cover have found that promoting the ‘add-on’ benefits of cover to their CISO, Chief Financial Officer and Board is helpful. Only 16% of organisations alert the crisis response team as their first step following a cyber incident, with the majority focusing on investigating and securing the breach first (Lockton UK Cyber Security Survey, 2017). However, as cyber incidents gain more and more press attention, mitigating the reputational damage of an event becomes increasingly important.

Cyber covers can include the costs for crisis management, legal advice, incident monitoring and developing a PR response through vetted and discounted providers. No organisation can be well versed in every type of cyber incident, so external support from experienced providers can be invaluable. Boards frequently highlight loss of reputation as a key concern, yet only 26% of organisations are involving their PR team in cyber breach scenario planning (Lockton UK Cyber Security Survey, 2017), and therefore the costs for PR support offered from cyber insurers can be very attractive.

Some insurers are now selling these ‘added-value’ services, without the additional traditional insurance cover. Airmic members have found their IT teams to be particularly keen on such support, where they can select the vendors involved themselves, as IT teams will tend to already have vendors that they know and trust. Some insurers are happy to have vendors chosen by the insured names on the policy.

‘As an ex-CISO, I am well aware that not all companies have a full team to cover all areas of crisis management or have all the required skillsets. And even if they do, the sheer size and complexity of a cyber reach can overwhelm teams. Internal/external communications and crisis response can suffer as a result. Having the ability to supplement teams through cyber insurance provides flexibility and reassurance to key decision makers, such as General Counsel and Executive Management.’

Peter Erceg, Senior Vice President, Global Cyber and Technology, Lockton Companies, LLP

3.3 Presenting cyber risk information to insurers

Airmic members frequently comment that cyber insurance underwriting requirements have been onerous in the past and have put the business off purchasing cover at all. In the last year, cyber proposal forms have reduced significantly in length, although where high limits are required, proposal forms with up to 40 questions are common. Additionally, there appears to be no standard question set across different insurers, and many questions appear ‘irrelevant’, making the process even more frustrating and challenging.

Airmic identified ‘buckets’ of information that are required by underwriters to assess the cyber risk. Figure 6 summarises these questions. Even where the organisation isn’t purchasing specific cyber insurance working through these questions can provide a useful structure for discussing cyber risk with the business.

Figure 6: **Cyber insurance underwriting questions**

Background information

Information on geography and industry of the organisation will help insurers identify your most significant cyber threats

- Industry and revenue - identifies the type of data processing undertaken, applicable industry regulations and most probable cyber threats
- Organisation geography - identifies the applicable regulatory requirements and potential cyber threat actors
- Summary of IT infrastructure - identifies what systems the organisation uses and why
- Number and type of data records held, and number and type of records processed

Governance

Cyber risk is a Board-level issue and insurers are increasingly interested in their understanding of the risk

- To what extent are the Board and senior managment engaged in cyber security?
- Who is responsbile for cyber security and cyber risk management?
- To what degree does cyber risk feature in the risk management framework?
- What external and internal audit procedures are in place for cyber risk and cyber security?

Training and awareness

Insider threat, whether malicious or non-malicious, is a significant contributor to cyber risk, and insurers will require evidence of how this is managed

- How are employees vetted and trained before being given system access, and how is this monitored and developed once access is given?
- How are security concerns related to employees away from the orgnisation's premises handled?
- How are security concerns related to employees who have left the orgnisation handled?
- What training programmes are in place to increase cyber attack awareness within the organisation

Technical security

Insurers will require information on physical and system cyber security. It is essential that risk managers work with the IT teams to complete this section

- What physcial security, e.g. data centre access and system security e.g. firewalls methods are routinely adopted?
- How often are user access privileges to sensitive data and systems evaluated and updated?
- How often is data backed up, and how is the integrity of this data tested?
- What systems are in place to detect unauthorised access or abnormal activities?

Business continuity and disaster recovery plans

Most organisations will have suffered a cyber incident of some sort. Insurers need to understand the circumstances and how they were handled

- What cyber breach circumstances (either successful or defended) have occured in the last x years and what was the impact if successful?
- How are cyber incidents detected, monitored and reported?
- How do cyber response plans differ in relation to different types of cyber incidents
- How often are cyber incident plans tested and what changes have been made as a result of this testing?

Vendor management

Organisations may be attacked via the third parties they work with, or vice versa

- What processes are outsourced to third parties and what data hosting providers are used?
- What data, processes and systems are shared with third parties?
- What cyber security contractual requirements are in place with third parties and how are these monitored?

All the insurers spoken to were keen to highlight that presenting a thorough understanding of the risk is more useful than highlighting the effectiveness of the internal controls in place. Insurers are keen to gain an understanding of the IT infrastructure in place and then consider a summary of what controls are in place and why.

> **‘I would not place much confidence in a company that declares itself to have cyber security that is 100% effective. It is impossible to achieve this. We would rather understand what the organisation considers to be its main cyber risks, and what the commercial reality of those risks manifesting would be.’**
>
> **Laila Khudairi, Divisional Head of Enterprise Risk, Tokio Marine Kiln**

The questions in Figure 6 are broad and can be challenging to answer without the support of the IT team and senior management, demonstrating the need for cross-functional collaboration when purchasing cyber insurance. This is the case whether completing an application form or working through the risk face to face with underwriters.

Airmic member case study – presenting cyber risk information

Head of Risk Financing and Corporate Insurance, Financial Institution

Cyber insurance underwriting requirements have traditionally seemed very onerous. The level of detail required can be off-putting for our Information Technology and Information Security teams, who may feel like they are being asked to share information on how to hack the company!

I have found it more effective to work with the IT teams to understand what are the key threats. This has included discussing each type of cyber exposure, and understanding the cost of controls, the likelihood / cost of a loss and, crucially, identifying how that loss would be evidenced. This has helped us understand where insurance would be most beneficial.

Having limited the cover required (rather than just requiring broad cyber insurance), we have requested reduced proposal forms with only appropriate questions included. We have worked with our IT, Legal and Compliance teams to ensure that the questions asked and our responses are relevant, meaning they are less hesitant to provide information.

3.4 The cyber claims landscape

The number of cyber claims made to insurers is growing, e.g. FM Global reported that the number of cyber claims made doubled in 2015 from 2014, and the trend of increasing loss frequency continued over 2016. Insurers report that there has been a clear increase in claims relating to the following:

- **Privacy breach events**

  An organisation's data records are stolen, deleted or amended

- **Ransomware events**

  Access to an organisation's data files or systems is denied, with the hackers making a subsequent ransom demand, often in the form of bitcoins

- **Distributed denial of service events**

  An organisation's website or systems are overwhelmed by hacker traffic, causing an outage.

For the above losses, the main coverage called upon are the first-party losses, e.g. forensic investigation and crisis management costs. Policies will normally have a pre-approved panel of legal, forensic, communications and other experts included in the cover. Airmic members who are buying cyber cover report that developing a relationship with these vendors or having your own choice of vendor named in the policy is vital.

3.4.1 Cyber claims challenges

Airmic members are concerned about the ability of cyber policies to pay claims. Much is made of the limited number of cyber losses and, without substantial loss data and legal precedents, claims worries will continue. Table 3 summarises a number of difficulties that insureds may face when bringing claims for losses suffered as a result of a cyber incident and that they should be aware of and prepare for.

Establishing claims protocols during placement is key to mitigating many of these difficulties. Cyber claims protocols can establish insurer, broker and insured roles and responsibilities, the involvement of third-party experts, communications procedures, data requirements, and payment and settlement timetables. Airmic members report that IT teams can be reluctant to share cyber security incident information, and confidentiality procedures and agreements should be built into these protocols.

Table 3: **Cyber claims difficulties**

Claims difficulties	Insured actions
Difficulty recovering costs incurred when notifying customers of a data breach where the notification was made voluntarily by the insured, rather than through an obligation by law	Be aware of national notification requirements, e.g. General Data Protection Regulations Establish loss protocols covering where insurer consent is required before costs are incurred or settlements agreed
Difficulty proving and calculating the impact of a cyber incident for business interruption cover **This is further complicated as cyber business interruption events are likely to be far shorter than a typical property damage event**	Clarify the data required by insurers to satisfy a cyber business interruption claim Verify whether the data requirements can be supplied by the business within the required timescales
Failure to comply with the insurer's loss notifications provisions, especially where these are conditions precedent to paying the claims	Gain clarity on how cyber incidents are detected internally and clarify with insurers how this can relate to loss notification
Failure to comply with the duty of fair presentation, including the obligation to notify insurers of material changes to the risk. This is particularly challenging due to the technical and evolving nature of cyber risk and security	Seek to discuss the duty of fair presentation with insurers as it relates to cyber, and involve internal stakeholders including IT and Legal to establish a common interpretation

4 Conclusion

The use of technology is rapidly transforming the business models of organisations and the risks they face. The speed of change is beyond that of any other risk, and risk managers will need to work collaboratively across their businesses to assess, monitor and ultimately control these risks.

> **As digitization increases and the digital economy grows businesses are exposed to far more cyber threats. The nature of these threats is changing too. With more and more devices connected to the 'internet of things' (IoT) the opportunities for attack are multiplying. This introduces two main challenges. First, a growing number of devices from which hackers can launch attacks. Second, the increasing vulnerability of IoT connected critical infrastructure. If they wish to keep up, organisations should continue to closely monitor the threat landscape, check they have the right kind of insurance cover and scenario test their defences."**
>
> **Dr Keith Smith, Manager, Emerging Risks & Research, Innovation Team, Lloyd's**

The challenge is clear, but risk managers are uniquely placed to lead the discussion. Their cross-functional role allows for a deeper understanding of how cyber events can impact the business, and their knowledge of risk controls and risk transfer solutions can help protect the business beyond technical security. However, they will need to strengthen their own skills too. An integrated, cross-functional approach and a smarter use of data and analytics streams will be required to monitor and protect against the evolving cyber threat. More information on how businesses can respond to the growing cyber threat can be found in Airmic's Digital Transformation report, 2017.

Airmic will continue to focus on cyber and digital risk to support Airmic members on this journey. Airmic recognises that organisations must be aware of how the digital revolution could transform the way in which businesses build resilience and, crucially, how they approach and manage risk. It will carry out in-depth research to determine what resilience looks like in a digitally transformed business world within in a new study, *Roads to Revolution.*

Notes

airmic

6 Lloyds Avenue
London
EC3N 3AX
Ph. +44 207 680 3088
Fax. +44 20 7702 3752
Email enquiries@airmic.com
Web www.airmic.com