Cyber resilience

The cyber risk challenge and the role of insurance

December 2014

CRO FORUM

Table of Contents

1 Executive summary

The continuing evolution of cyber risk

The digital revolution is affecting nearly all aspects of everyday life. Society and business have become increasingly reliant on technology and the internet. As a result, the availability and security of all services we rely on for daily life, particularly financial services, are exposed to cyber threats and cyber risk.

As a term, cyber risk covers the risks of doing business, including managing and controlling data, in a digital or "cyber" environment. Goods and services are being provided at an ever increasing rate by large scale infrastructure and business projects, underpinned by information technology and the internet. As the environment becomes increasingly interconnected and complex, the tools and expertise needed to exploit the increasing vulnerabilities become more widely available. Consequently, it becomes simpler to carry out an attack. Given the many ways that cyber risk can affect the operation of a business, the costs and impact are uncertain and will be increasingly substantial.

Insurance is not exempt from the impact of these changes, as the industry embraces technology to interact with customers. The sensitive data that insurers accumulate and hold about their customers and the variety of privacy laws that relate to the protection of this information make them a target. The threat for insurers falls into three broad areas: unavailability of IT services, data breach and loss of data integrity.

In light of the continuing evolution of cyber risk, this paper explores two key areas:
1) Practical steps for cyber resilience;
2) The role of insurance in strengthening cyber resilience.

Cyber resilience

The increasing complexity, interconnectivity and interdependency of technology make guaranteed protection impossible. No system is impregnable and therefore there is always a risk that something has penetrated or compromised the performance of a company's systems and technology.

The response to this needs to be cross functional, as more frequently cyber risks are caused by human behaviour rather than from system flaws or technological weaknesses. The Chief Risk Officer (CRO) has an important role to play within an organisation in working with internal stakeholders across business functions to promote awareness and understanding that support effective risk management of cyber risk.

Four pillars have been identified as a framework for enhancing existing risk management and establishing a process for cyber resilience:

Prepare Understand your critical assets; develop capabilities to address different levels of risk; establish risk appetite and embed risk management throughout your organisation.

Protect Ensure well-founded and repeatable cyber preparedness; undertake threat and control assessments: ensure appropriate due diligence and vetting processes for third parties; enable and empower incident management and response capabilities; develop and implement an incident response plan, potentially with war gaming and drill exercises; and ongoing education and training.

Detect Develop detection and continuous monitoring capabilities to address anomalies and threats to your company assets.

Improve Build a comprehensive database of security incidents that support continuous learning and finally enable your recovery from an event in a shorter timeframe.

Insuring cyber risk

Insurers also have a key role to play in improving the overall resilience of society to cyber risk by incentivising best practise through risk transfer and premiums, aggregating and interpreting loss data, and providing capabilities as part of their product offering. The new and evolving nature of cyber risk presents a number of issues that need to be addressed, particularly around understanding the costs associated with a cyber event. This necessitates a different approach to the assessment of cyber risk to traditional insurance risks.

There are three elements that need to be in place to support the insurance market for cyber risk and a cyber risk assessment:

1) Common classification and codification of cyber risk

The evolving nature of the risk, changing products and lack of clarity over the scope of cover all contribute to making codification of cyber risk challenging. CROs have a clear role in helping their organisation to take proper steps in codifying cyber risk. This involves promoting consideration of cyber risk in traditional lines of business and exploring the opportunities for a larger pool of good quality loss information (including wider industry sharing of information).

2) Understanding cyber risk exposure accumulation

This is a critical area for a successful insurance market and management of exposure. A key component is the development of cyber risk scenarios to help understand the risk exposure accumulation, bearing in mind the factors that will influence the probability/ severity of losses and accumulation potential.

3) Strong well designed risk management framework

Having developed approaches to codification and cyber risk exposure accumulation, organisations will be better equipped to establish risk tolerance parameters and agree capital allocation, informed by operational risk and underwriting perspectives.

The promotion of cyber resilience requires cross-functional teams. Organisations should leverage their own experience in developing practices for increasing cyber risk resilience to develop cyber insurance products that are in line with the business strategy.

Taking cyber risk management forward

The dynamic nature of cyber risk presents a significant challenge and opportunity for insurers. Risk management and the CRO can help by establishing a common language that supports internal cyber risk management and the development of insurance products for cyber risk. The successful risk management of these external exposures can provide a platform for insurance to promote cyber resilience in conjunction with other stakeholders through the provision of effective cyber risk cover.

The steps outlined in the paper are intended to help CROs enhance cyber resilience. The increased discussion of this topic in various forums, including government initiatives, and wider industry dialogue will be important in promoting a road-map to develop a common understanding of terms throughout the industry and of the potential for cyber risk information sharing.

The availability of data remains a challenge in both understanding the cost and accumulation of cyber risk, and the evolving nature of the threat. The possibility of an industry-wide cyber risk database to enable loss data to be captured and wider public/ private initiatives are areas for further discussion. In this context, and given the developing legislation on data protection, risk management can play an important role in the dialogue.

2 Understanding and managing cyber risk

2.1 Understanding cyber risk

"Cyber risk" is an increasingly common term in boardrooms, publications and mainstream media. In the broadest sense, cyber risk is best understood as the risk of doing business in the cyber environment. However, such a broad term may be unhelpful and so contextualising cyber risk against other types of risk is necessary.

Cyber risk covers any risks that emanate from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks. It also encompasses physical damage that can be caused by cyber attacks, fraud committed by misuse of data, any liability arising from data storage, and the availability, integrity and confidentiality of electronic information – be it related to individuals, companies, or governments.

These risks may emanate from a number of sources, often unforeseen, and the impacts can vary and may affect a business in a number of different ways. Attacks on critical infrastructure, such as industrial control systems, may be particularly severe and could have far-reaching consequences.

The risks and impacts can be due to human or system error, but also due to cyber-crime that is often driven by traditional criminal motives, such as theft, robbery or sabotage, that can be executed without a need for physical proximity.

As such, cyber criminals may be internal or external to an organisation, and their motives and drivers are varied and evolving (see Figure 1). Attacks have stemmed from sabotage and lone hackers, from the use of malware, through to sophisticated networks or state-backed hacking.

Evolution of cyber threats

Figure 1: Evolution of cyber threats (Source BAE Systems Applied Intelligence).

Cyber risk can also emerge from not having proper resilience to failure (either human or non-human) in the cyber environment. The rapidly changing cyber landscape requires increasingly robust change management processes to ensure that cyber services continue to be available and meet the expectations of customers. In today's cyber world, this often means that recovery in hours or days of systems is no longer sufficient; services must now be capable of recovering on almost a real-time basis.

At the same time, organisations are undergoing a huge amount of change. Much of this is driven by the digital revolution which is rapidly increasing the level of connectivity and processing power available to both organisations and individuals.

While such trends have benefits for customers, they increase companies' vulnerability to cyber risk and its evolving threat landscape.

Fierce competition among organisations to reach customers and reduce costs is compounding the threat, as insufficient time is taken to understand and manage cyber risk. There is also the challenge of ensuring that employees observe standard IT hygiene practices on an ongoing basis. This is true in the insurance industry, as with all other industries.

As interconnectedness increases and the threat landscape evolves, the tools and expertise needed to exploit vulnerabilities is becoming more widely available, making it simpler to carry out an attack (see Figure 2).

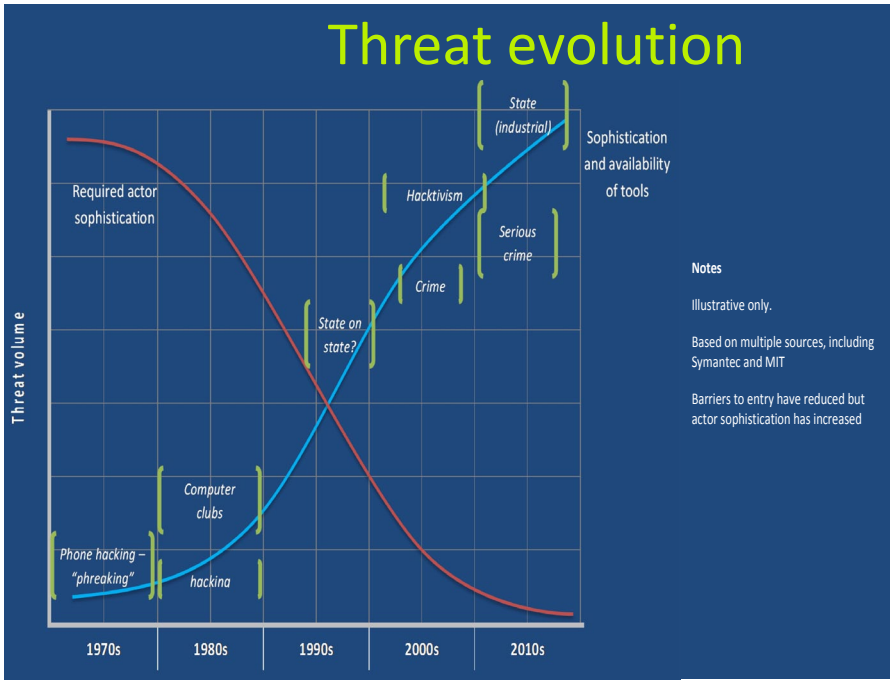


Figure 2: Threat evolution (Source: Richard Bach, Assistant Director for Cyber Security, UK Government's Department for Business, Innovation & Skills).

Factors influencing the threat landscape

The cloud	Businesses are becoming far more complex as they outsource bespoke requirements and large scale infrastructure to external cloud providers.
Shadow IT	The growing use of "shadow IT" – when business functions procure IT solutions without involving the IT department – is eroding organisational boundaries.
Mobile and flexible working	The rush to provide new services on platforms such as mobile devices and through social media is exposing companies to unforeseen risks and new technologies that are less understood.
Bring your own	The traditional boundaries and tight controls enjoyed by IT are being devices eroded as organisations embrace "bring your own device" (BYOD) solutions and web collaboration services to support mobile working and customer engagement.
Internet of things	The growing connectivity of devices via the internet (e.g. smart home appliances) is increasing society's vulnerability to cyber attacks on control and infrastructure systems.

Understanding cyber risk

In light of the evolving threat landscape, there is still a large amount of uncertainty about the scale of cyber risk to businesses and the return on investment of automated detection systems.

Cyber activity has moved from being highly disruptive, as in the early days of malware, to being highly secretive. The most serious breaches remain undetected for considerable amounts of time. For example, current UK government estimates indicate that, on average, 200 days elapse between the occurrence of a security incident and its detection. A victim of an advanced persistent threat (APT) may not even know the kind of damage suffered.

These kinds of attacks are usually very professional and put in place to gain shadow control of an environment. They often last for a long time and undermine confidentiality, integrity and availability. An advanced persistent threat creates opportunities for data manipulation and leakage. More seriously, they also create conditions for a lethal outage of services. These attacks may not be directed at a single company, but rather at an industry sector or even a country's infrastructure.

Determining the effect of cyber breaches and collecting information on incidents for large organisations remains challenging. Many security incidents are often seen as near-misses or not sufficiently material to warrant Group reporting. However, such incidents do impact the business, can accumulate and can often be an indicator for more fundamental vulnerabilities.

As the recent World Economic Forum - Insight Report states "failing to address these issues, typical of an open and interconnected technology environment, means that the risk from major cyber events could materially slow the pace of technological innovation"[1] .

[1] "Risk and Responsibility in a Hyperconnected World", WEF in collaboration with McKinsey, 2014

Connections with external providers require a special focus on controls and vulnerability assessment. This reinforces the need to gain the necessary assurance from service providers in respect of the control environment that provides the respective services. The example of Target[2] highlights the cyber risk associated with supplier connections and how vulnerabilities on internal networks are used to gain further access.

The challenge is whether steps to manage cyber risks are understood. This is prompting governments to improve and support awareness of the steps that need to be taken to manage cyber risk. While prior focus was on near full prevention, there is now a need to focus on resilience which is about better detection and capability to handle events. This is an area where insurance itself can play a role.

Beyond the potential financial impact, cyber attacks also present a reputational risk for organisations, which can be heavily criticised for not having done enough to protect their customers or the organisation itself.

From a risk management perspective, it is therefore important that there is a framework in place that captures all security incidents, that the potential business impact is recorded and the implications understood across the organisation. The CRO has a vital role to play, not only in understanding cyber risk, but also in explaining it to internal and external stakeholders. CROs can help embed good practices for managing and mitigating the risks and improving resilience.

2.1.1 Impacts on insurers

Insurers hold data on their customers for a variety of reasons, e.g. to tailor insurance cover to customers' needs, to price risk and to forecast revenues. The long-term nature of many types of insurance liabilities often means that data on customers is accumulated and held for a long period of time.

On this basis, insurers are likely to be a target because of the sensitive data they hold, for example, on:

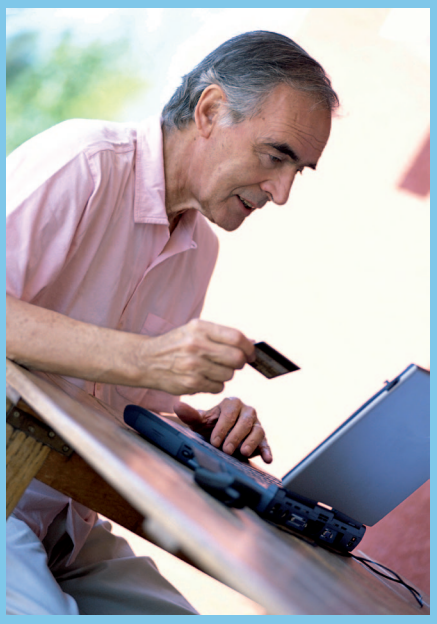
- A customer's Life & Health (L&H) policies;
- A customer's investments (pension plans, life policies and, for bigger groups, because of their accounts in group banks or in asset management firms);
- A customer's bank details; and
- A customer's estates and belongings, or about their business because of Property & Casualty (P&C) and Third Party Liability (TPL) policies.

The goal of cyber risk management is to improve resilience to cyber attacks and to protect customers' data. Safeguarding data availability is mandatory for the ongoing viability of many lines of insurance business and compliance with relevant regulations. There are three broad categories of particular vulnerability for insurers:

- Unavailability of IT services;
- Data breach; and
- Loss of data integrity.

[2] See text box on "Data Breach" on page 9.

Unavailability of IT services



The availability of IT services, both internally and externally, is critical, particularly where sales are made online. Financial costs in the form of lost revenues, lost productivity, regulatory fines, unmanaged financial assets, and even litigation for undelivered service, all add to the amount of money at stake.

The unavailability of IT services may also affect claims management, which can result in fines in some countries. Although operational risk capital may absorb these losses, it is much more difficult to quantify the cost to an insurers' reputation, which is hard earned and easily damaged. It could also pose challenges to assistance services which rely on the interconnectedness of IT systems, from smartphones to specific devices, to medical monitoring equipment.

As a result, unavailability of services poses a significant risk to insurers, with potentially severe financial and reputational consequences.

On 19 June 2012, a major IT incident impacted 6.5 million Royal Bank of Scotland customers who faced disruption to their online banking facilities over several weeks. The incident resulted in a total regulatory fine of GBP 56 million.

Data breach

A loss of data triggers a number of issues for insurers from confidentiality, trust and regulatory perspectives.

Safeguarding confidentiality is a cornerstone of financial services, but is made more challenging by the complexity of networks and systems, the extension of digital services to many people, and exposure to third parties' IT systems and policies.

Highly confidential and sensitive data is no longer strictly kept in a secure environment of the company premises, but maybe stored in a Cloud or at a third party service provider or transmitted through PCs, smartphones and tablets which can be a target for espionage or, for an insider, an easy tool to carry information away or gain access to information stored or transmitted.

A loss of a company's own data can lead to reputational damage, loss of public or customer trust, and economic losses, for example due to fines for non-compliance with data security standards (e.g. the Payment Card Industry Data Security Standard - PCI DSS) and consequent data violation, or by undermining competitive advantage.

Losses of customers' data, which are protected by privacy laws, are likely to have far-reaching legal and regulatory consequences, and may result in fines or in the worst case regarded as criminally negligent. Customers may also seek redress through legal means.

The impact is compounded by the differences in privacy and data protection laws that exist across the globe, and the different reporting/disclosure requirements in the event of a loss of data. These place different values on different types of data and different requirements around where and how data can be stored and who it can be shared with (directly or indirectly).

The challenges in this area continue to evolve and will, no doubt, be magnified by the impending European legislation on data protection. The European Commission's proposal for general data protection regulation proposes new rules on individuals' ability to control their data, for example, through new rules on consent/withdrawal of consent for data use, access to data, rights regarding data portability and information on data handling. It is also likely that it will introduce new requirements on data breach notification and sanctions for data breaches. The proposals, if introduced, will require insurers to change the way that they use and process data. The consequence of data breaches/loss of data will, in particular, increase risk of reputational damage due to notification requirements.

In December 2013, a security breach at Target exposed approximately 45 million credit card numbers and the personal details of 110 million customers, leading to an estimated cost of USD 148 million, offset partially by USD 38 million in insurance coverage.

Loss of data integrity

Maintaining data integrity is a key part of combatting financial crime.

A fraud involving altered information on payments or setting up a fictitious transaction can lead to a loss of data integrity. For example, an attack may change parameters in underwriting or claims systems, leading to policy premiums or claims payments being miscalculated.

The loss of data integrity is likely to result in economic losses and have a negative reputational impact. These will be particularly difficult to quantify when the incident affects the estimation of economic variables like provisions, capital or other balance sheet items, where data quality weaknesses may lead to regulatory action. Furthermore, data integrity incidents are much harder to detect as everything appears to work as normal.

Cross-system integrity checks, reconcilement and audit trails are essential, as is addressing the specific challenges arising from the use of multiple systems and bring your own devices.

In June 2014, there were reports of external attackers being able to wipe company devices by exploiting a well-known vulnerability into companies' mobile infrastructure being managed by outsourced service providers.

2.2 Managing the threat of cyber risk

2.2.1 The role of the CRO

Cyber risk is now a truly cross-functional concern that requires recognition that accountability and responsibility lies with every employee, including members of the board and executives. CROs have a key role to play in encouraging a culture of communication and openness on cyber risk throughout their organisations that helps improve awareness and strengthen resilience.

As a starting point, it is important for CROs to work with internal stakeholders to agree a definition for cyber risk that enables the risk to be understood. Cyber risk should be understood in a way that is consistent with the existing, internal Enterprise Risk Management approach.

Having a clear understanding of cyber risk and the fact that many cyber attacks rely on tactics such as phishing reinforces the importance of educating all employees on cyber risks. However, while many cyber risk management techniques may be common sense, specialist security skills are still needed in order to ensure that subject matter experts across the organisation receive and can analyse the information most relevant to them.

The challenges for CROs are to establish a cyber risk management framework supported by a team with the relevant skills and expertise to engage all business functions to recognise the individual accountability and responsibility of all employees in managing cyber risk.

Given the need to focus on cyber risk resilience, the CRO should consider the following:

- Promoting a culture of open communication and risk awareness;
- Increasing awareness of cyber risks at senior levels;
- Facilitating discussions and understanding of cyber risk at both business and board level;
- Articulating how cyber risk is integrated within the broad risk management landscape;
- Ensuring appropriate ownership of and responsibility for cyber risk management responsibilities;
- Embedding cyber security governance throughout the business; and
- Establishing good assurance.

2.2.2 Practices for increasing cyber risk resilience

Traditional information security protection and risk management strategies need to be augmented by process and technology improvements and employee training programmes which are geared towards the new threat types and sources.

There are a number of industry best practices being developed by several institutions including those by the National Institute of Standards and Technology (NIST), the Informations Security Forum (ISF) and UK Government Communications Headquarters (GCHQ). While the adoption of these types of cyber-defence frameworks are something that insurers should consider, it is important that these do not become mandatory. It should be about establishing a culture of continuous cyber defence improvements as a company value. Prescriptive standards will undermine the effects of good risk management, drive up costs and potentially provide false assurance against evolving threats.

Four pillars can be identified for cyber risk management:

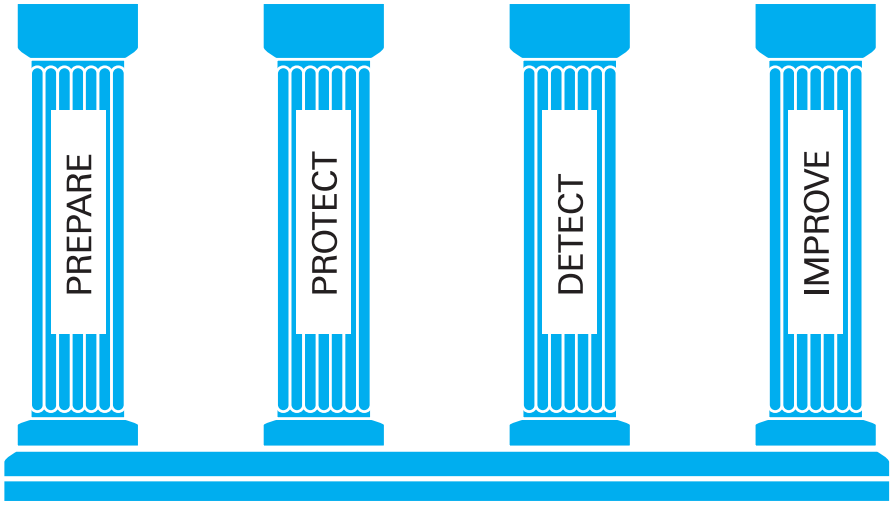


Figure 3: Four pillars for cyber risk management.

Historically, the focus has been largely on the first two pillars of preparing for and protecting against cyber risk and attacks. However, while these pillars are important, the nature of cyber risk means detection and rapid response are now equally, if not more, important. Organisations must be prepared to react and recover from potential failures or breaches.

The CRO has an important role to play in building consensus within their organisation about the equal importance of detection and response when reviewing, and taking steps to increase, resilience to cyber risk.

The following are some practical steps that organisations can consider for increasing their resilience to cyber risk:

Understand your critical assets
An organisation needs to consider what is vital to protect, both in terms of critical data and systems. The identification of critical data and systems enables companies to understand their potential exposure (vulnerability).

Develop capabilities to address different levels of risk
Capabilities to address the different levels of risk should also be developed, including:

i. New approaches to assurance and threat management that adapts to the developing risk environment; and
ii. Good relationships with industry and governmental agencies to help respond to high end threats and advanced attacks.

Establish risk appetite
An organisation should establish overall governance around policies and processes so that its regulatory, environmental and operational requirements are understood. As part of the process of embedding cyber risk management into an organisation, boards should consider the levels of cyber risk that they accept are within the risk tolerance for the organisation. This can then help companies to develop either a separate risk appetite statement for cyber risk or amend existing risk appetite statements (e.g. for IT risk). A separate risk appetite statement has the advantage of facilitating internal and external communication on this issue.

Embed cyber risk management throughout the organisation
The first line of defence in cyber risk or cyber security management is with the frontline employees. Here it is necessary to implement appropriate capabilities for identifying threats. Additionally, this should include the development and implementation of processes to control and monitor its operational effectiveness. The second line, through risk management, should articulate best practices so that it is clear "what good looks like" and should provide thought leadership on cyber risk management and conduct reviews.

Ensure well-founded and repeatable cyber preparedness
There needs to be strong levels of hygiene in the IT environment covering key areas such as robust access control processes that include external parties and leavers, data security controls, tried and tested information protection processes. This will help thwart a large majority of the basic threats.

Undertake threat and control assessments
Undertaking threat, vulnerability and control assessments is a key part of preparing for a cyber attack. It is highly likely that at some point a cyber attack will be successful and hence an organisation needs to have a clear understanding of their critical assets (see above).

Once the identification of critical assets has taken place, insurers should analyse the cyber threat landscape to understand where a likely threat will come from and predict the identity of likely attackers. This can enable a response to be created that is appropriate to the size and complexity of any potential attack.

A Cyber threat observatory could be used for this purpose, incorporating information from the following sources:

- Information Systems Security providers (Antivirus, IPS, SIEM etc)
- Incident Response networks (FIRST, TERENA, FI-SAC, etc.)
- Specialized Cyber Security media (security blogs, cyber security publications etc)
- Specialized "Cyber Intelligence" providers (e.g. FS – ISAC)
- Sector-specific information sharing networks; and
- Results from internal cyber threat analysis

Once a threat is understood, an organisation can review the controls it has in place to protect critical systems and data. On this basis, existing controls can be assessed for their ability to perform appropriately in a stress situation and upgraded or replaced if necessary to increase protection. Including control requirements into the deployment of new projects going forward is a cost-effective way to ensure that systems are built resiliently to begin with.

The protection of identified 'critical' components should create as strong and secure a boundary as possible. The focus of security should move away from generic perimeter protection and become more focused on the areas of real impact (including data endpoints) and their possible linkages.

Some of this can be achieved through the use of penetration testing linked to the threat assessment and critical functions – dependent upon the technical ability of an organisation, this may be carried out by an internal resource. However, it may be more practical for penetration testing to be performed by an external provider. This could be by a specialist organisation or by firms that offer 'ethical hacking' as one of its services. Aside from these practices governments and regulators are now interacting with organisations in proposing threat intelligence led ethical hacking testing (e.g. CBEST in the UK). This is an example of a potentially effective methodology for testing and bolstering resilience to the increase in threats and be a conduit for threat and control assessments.

Ensure appropriate due diligence and vetting of third parties

Any relationship with a third party company involving the outsourcing of services needs to be closely managed and monitored. This is particularly important where third party providers have access to an organisation's key data. In such cases, the third party should be thoroughly vetted both at a technical capability level, but also from a human resource perspective (ie appropriate and vetted employees).

As part of any service agreement with a third party provider where critical systems or data is held, the provider should agree to look through rights and seek approval for any further sub-contracting that they may be contemplating. Additionally, the impact of increased use of cloud services by businesses should be considered. This is especially important because ease of availability often means that these services are engaged without adequate IT involvement or understanding of the cloud provider's legal liability. This potentially increases the organisational attack surface outside of IT's control or monitoring capabilities. In this context, Cloud Security Alliance, amongst others, provides information and suggestions of good practice, including their recently released Cloud Controls Matrix[3].

[3] see https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1

Enable and empower incident management and response capabilities
Companies need sound processes for detecting and responding to cyber attacks. Responsibility for incident management should be clearly defined. A company's incident response capability should be aligned with the threat landscape and company's risk levels and taken into account when developing a Service Level Agreement (SLA), including for example incident response times, for the incident monitoring/response team.

Develop and implement an incident response plan
Companies should develop an incident response plan as this is a crucial part of bolstering resilience to cyber risk and mitigating the risk of reputational impact. Incident response plans should include:

- An escalation procedure;
- A communications plan, including public disclosures for the board or equivalent authoritative body and a plan for responding to press queries;
- An incident response depending on the type of attack experienced, e.g. denial of service, and an associated response time threshold;
- A recovery plan that describes clear recovery protocols to respond to threats, breaches and identified vulnerabilities and clear steps to get back up and running as soon as possible; and
- Details of scenario testing of potential threats to ensure the incident response plan is robust and tested periodically.

War gaming and drill exercises can be used to test and improve communication and incident response plans and report internally.

Education and training
Cyber resilience is not just about technical controls, but also about employees' cyber risk understanding and awareness. Ensuring that all staff are trained on their respective responsibilities with regards to handling the threat of cyber risk will not only help to prevent deliberate actions, but also unintentional actions that might compromise IT security.

Organisations should review internal training for staff at all levels, specifically:

- Awareness programme for high risk individuals (board, system administrators);
- Annual training plan for all employees; and
- Dedicated security training for IT developers.

Develop detection and continuous monitoring capabilities
Building on the previous steps in prepare and protect, having timely detection is a crucial capability for cyber resilience.

Companies should have mechanisms that ensure that infrastructure and information assets are continuously monitored to detect anomalies and threats to its set-up.

Monitoring types can include real-time protective monitoring which will help detect outbreaks of known malware from signatures, monitoring of user behaviour to identify suspicious insider activity, and external monitoring to identify evidence or claims of compromise before these take hold. Improved training will also allow all employees to play a role in monitoring and potentially stopping phishing campaigns at an early stage.

Companies should also provide adequate resources to incident monitoring/response teams, in terms of people, tools and procedures, to ensure that incident response times can be met. Companies may want to establish agreements with third party providers (e.g. cyber intelligence and security companies) and governments to broaden their incident response capabilities.

Finally, detection capabilities should be tested regularly to ensure scope of coverage is adequate for the organisation's infrastructure and its key information assets in order to ensure timely detection is achieved (see Figure 4).

Intelligence key to all risk management layers

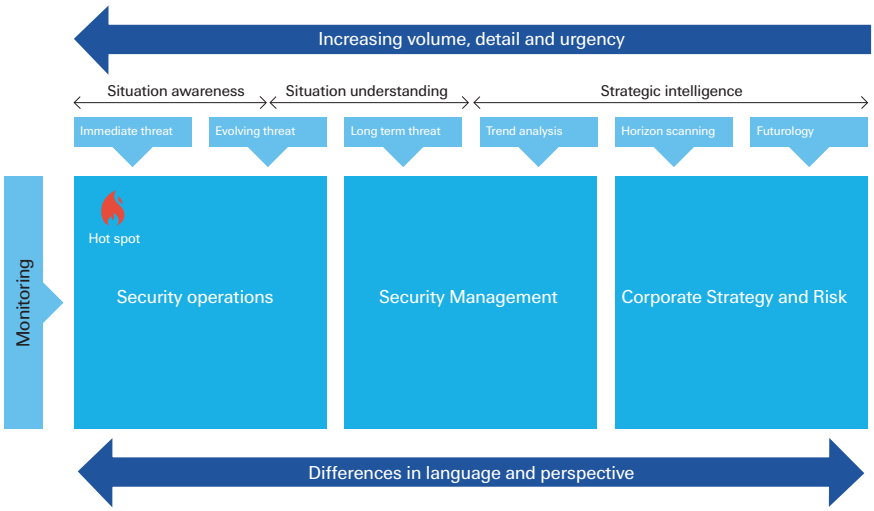


Figure 4: Risk management layers (Source: BAE Systems Applied Intelligence).

Build a comprehensive database of security incidents
Companies should look to build a comprehensive database of cyber incidents, including near-miss and minor events. This should capture lessons learnt in order to provide companies with a broader understanding of possible vulnerabilities and allow security controls and capacities (including business continuity/disaster recovery scenarios, strategies and procedures) to be modified where necessary. This feedback loop will help to strengthen the cyber resilience capability overall. The recorded number of incidents will also be a useful key risk indicator for monitoring the imminence/acuteness of cyber risk.

Recover from an event
If the company does suffer from an event, then the recovery plan should be executed to ensure that normal service is resumed in as short a timeframe as possible. Lessons learnt from such recovery should also be used to improve the overall end-to-end processes and procedures for future handling of such events.

2.3 Looking forward

While it is not possible to predict the future, it is possible to draw a parallel between online and traditional organised crime.

For the most significant threats, governments are likely to become increasingly proficient and may ultimately provide a good level of general national protection – although that position is likely to remain some years away. Meanwhile, technology solutions for general network hygiene will improve and become more attainable for organisations, addressing many of the lower level threats.

It is likely that the mid-tier threats will remain, where attack complexity exceeds basic controls but is low level enough to avoid state level controls. These threats will continue to have a significant, but usually not debilitating impact on organisations.

Regulators should work together with the industry to raise awareness of cyber risks and to provide a platform for information sharing about cyber risks and best practices to increase cyber security. Mandatory, prescriptive regulation is unlikely to be effective, since the evolving threat means that it will quickly become obsolete and will divert resources away from more effective risk management practices. Flexible measures are needed to provide a sustainable high standard of security.

As the major trends in technology begin to settle and become more understood, so, too, will the emerging best practices for gaining assurance and security. Both these aspects will still be fuelled by continued change in the specific technology products and their unique vulnerabilities.

For now, most businesses are working to establish best practice that keeps pace with the evolving threats and associated risks and will continue to develop and adapt their approaches. Business should continue to focus on securing what matters the most. And while it is possible that the cyber risk landscape will stabilise over time, for the foreseeable future, it those organisations that continue to invest and adapt their approaches that are likely to be the most resilient should the worst occur.

It is also important to recognise the significance of the insider threat from an expert who gains access to many systems, processes or exploits loopholes over time. This highlights the cross disciplinary impact of cyber threat from purely technological to human behaviour aspects as confidence around the culture and behaviour of internal staff becomes increasingly important beyond just their technological capabilities.

The pace and scope of change means that resilience practices will need to be revisited on a frequent basis by resources capable of appreciating both risk management techniques and the new ways of conducting business.

3 The role of insurance in strengthening resilience to cyber risk

3.1 An insurance market in cyber

Cyber attacks may stem from a wide array of actors, affect all industries and result in varying levels of damage to data, critical systems, physical property, and even disrupt business continuity. For this reason, cyber risks can trigger a variety of insurance solutions. For example, the expenses to restore damage caused by malicious hacker attacks on personal or financial data and the compensation of related liability claims may be covered by a tailor-made cyber liability insurance policy. Equally the physical damage to a power plant caused by a fire or the machinery breakdown of a power generator or transformer following a cyber attack may trigger the coverage of a fire or machinery breakdown insurance; damage to company assets along with a decrease of shareholder value may trigger Directors & Officers insurance; the power plant operator may claim against the product manufacturer (defective product, product liability) or the service provider (programming error or maintenance failure, professional indemnity); the power blackout may cause business interruption of third party industries, triggering contingent business interruption covers; the lack of power potentially to large areas may result in property damage or bodily injuries; or the lack of business continuity planning may lead to severe financial losses, potentially even the bankruptcy of affected companies.

Insuring cyber risk comes with a myriad of challenges – continually shifting threats, sparse loss data, multi-layered levels of interconnectivity – the list goes on. In order to be able to assess which policies may be triggered under different cyber attack scenarios, the CRO needs to create a strong and well-designed risk management framework. This will help organisations make sense of the cyber risk they have assumed and actively discuss, manage and monitor this risk, while providing assurance and expertise to clients.

This section of the paper will discuss the challenges that CROs face in this environment and aims to provide some practical solutions that can help in designing a risk management framework. The right risk management principles will support insurers assuming cyber risk and facilitate an expansion of the cyber insurance market.

Challenges for an insurance market in cyber from a risk management perspective:

Insufficient or poor quality loss information	The rapidly changing cyber landscape means that historical data often does not reflect the current environment. Hence it is not possible for insurers to use traditional approaches to model loss distribution.
Uncertain value of loss information	There are few established methods to quantify the economic value of the insured's loss information and a general unwillingness on the part of companies to share such information.
Highly interconnected IT systems	The interconnectivity of IT systems hinders the ability to measure and monitor an insurer's cyber risk exposure accumulation because a cyber attack can trigger several insurance products and independent policies in a chain mechanism, similar to contingent business interruption. This challenge is further exacerbated by second and third order linkages which are particularly difficult to identify and analyse.
Continually evolving attack strategies, perpetrators, and motives	Whether a cyber attack is covered by an insurance policy may depend on the motive for the attack and its perpetrator (e.g. cyber crime vs. cyber war vs. hack-tivism vs. espionage vs. national security) as this will affect whether clauses and exclusions for cyber insurance can be considered.

Market developments

As already outlined in section 2.2, cross-functional communication on cyber risk is essential to improve awareness and strengthen resilience. Risk management frameworks that promote communication will improve insurers' ability to actively measure and monitor cyber risk exposure.

Insurance is increasingly part of the strategy to manage cyber risk. The acceptance that companies cannot fully protect themselves against cyber attacks reinforces this point and further strengthens the need for clear risk management measures to support the growth of a comprehensive cyber insurance market.

Against this background, the market for insurance products which are specifically designed to cover cyber risk has evolved as companies respond to the changing regulatory environment and the commercial impact of high profile cyber attacks. Notwithstanding this, market development has been partially constrained by the perceived high cost of policies, confusion about the scope of cover and uncertainty regarding the likelihood of an attack[4].

There are several factors that are likely to trigger a growth in the cyber insurance market in the short to medium term.

[4] United States Department of Homeland Security: http://www.dhs.gov/publication/cybersecurity-insurance.

Firstly, increased publicity around breaches which reinforces the potential economic impact of a cyber attack and demonstrates the way that losses can escalate. Other examples include high profile court rulings such as Zurich American Insurance Co. vs. Sony Corp of America et al.[5] and Federal Trade Commission vs. Wyndham Worldwide Corp et al[6].

Secondly, regulatory shifts in both the US, e.g. Securities and Exchange Commission guidance on cyber event disclosure, and Europe, e.g. ongoing discussions on a European General Data Protection regulation, which increase the cost of data breach through notification requirements and sanctions.

Thirdly, standard policy language changes, for example, the Insurance Services Office (ISO) standard exclusion for cyber risk under the commercial general liability policy, which increases the need for tailor-made cyber liability insurance.

Government initiatives are also having an effect. In February 2014, the US government released a first version of its Framework for Improving Critical Infrastructure Cybersecurity ("the framework"). The framework principles were developed in collaboration with industry and represent a "set of standards, guidelines and practices to promote the protection of critical infrastructure." The UK government is taking a similar approach and released its Cyber Essentials Scheme in June 2014 to promote cyber best practices and has made it a mandatory scheme for suppliers bidding for certain UK government and large business contracts that handle personal information.

3.2 Risk management of cyber risk exposure

The challenges set out in section 3.1 provide an important context for understanding and managing the risks arising from underwriting cyber risk. For the CRO, this is crucial to enable:

1) Classification and codification of cyber risks;
2) An assessment of cyber risk exposure accumulation; and
3) Development of an appropriate risk management framework to manage cyber risk exposure.

3.2.1 Codification

Understanding and managing the underwriting exposure of an insurer begins with accurate classification and coding of risks. Codification is fundamental to pricing, measuring profitability, managing aggregations and allocating capital, as well as allowing insurers to link underwriting exposures to their own operational risks.

However, the rapidly changing nature of cyber risk and the broad array of products being offered by carriers make accurate coding of cyber policies challenging for the industry. Cyber coverage is not currently coded in a consistent way, which complicates risk measurement.

The implementation of specific codes for cyber risks would help insurers capture and monitor cyber exposures in a consistent and transparent way. Consequently, CROs should work with Chief Underwriting Officers to establish a robust system of control around cyber codification both within the Underwriting and Claims functions.

[5] Case number 651982/ 2011
[6] Case number 2:2013cv01887

Codification

The challenges for a consistent coding of cyber policies include:

An evolving threat

The use of the internet for commercial purposes has exposed companies to the risk of operating in a cyber environment which is continuously evolving.

The potential for operational disruption in the wake of a cyber attack was recognised, and the insurance industry responded by providing the first cyber insurance cover, which focused on the loss caused by early computer viruses or hackers.

As companies increasingly created, collected and stored data across networked systems, the nature of the risk posed by cyber threats widened to include the loss or manipulation of confidential customer and commercial information. Changes in the regulatory environment, in particular US data breach notification laws, significantly increased the potential cost of a data event to companies.

Today the threat has evolved still further. A sophisticated cyber attack can cause physical damage to assets (see "Stuxnet" virus[7]). Even though the target in this case was highly specific and potentially not insurable, the implication for commercial industries of this type of attacks and the need to protect against business interruption, property damage and other operational risks was profound.

A changing product

Cyber insurance has evolved in response to the primary source of loss, namely business interruption and liability for data breach.

While there remains limited consistency in codification across the industry, the risks that are typically classified as cyber fall into the following broad categories, covering financial damages caused by interruption of services, corruption of data, breaches of security or privacy of data.

While 'traditional' cyber policies are relatively easy to codify, the challenge from an insurance perspective is to ensure that codification practices keep pace with the evolving cyber threat.

[7] en.wikipedia.org/wiki/Stuxnet – This malware affected Siemens' SCADA system, used to monitor and control technical processes, with the aim of sabotaging industrial plants. The malware was spread in several ways, including via USB sticks and security vulnerabilities in Microsoft programs.

Area	Risk categories	Example cover
First party costs	1 Business interruption	A computer system failure or breach of network security leading to income loss and expenses incurred during the period of interruption.
	2 Restoration costs	Expenses to restore information/data after a failure of the computer system or network leading to destruction, corruption or loss of electronic information assets and/or data.
	3 Regulatory defence costs	Defence costs of regulatory action due to breach of privacy regulation. Cover may include fines and penalties due to breach of privacy regulation.
	4 Security and privacy	Investigation costs to determine cause and extent of security failure. Cover may include fines and penalties due to breach of privacy regulation.
	5 Cyber extortion	Costs and expenses related to threats or extortion after the release of confidential information or breach of computer security.
	6 Intellectual property	Value of trade secrets stolen through a cyber attack.
Third party costs	7 Data breach	Compensation of third party liability claims related to the disclosure of confidential commercial and/or personal information (privacy), as well as economic harm suffered by others from a failure of network security.
	8 Crisis management	Costs and expenses associated with managing a cyber event (e.g. a privacy breach), which may include forensic investigation expenses, call centre costs, credit monitoring costs and public relations costs.

Unclear cover

The final major challenge in the codification of cyber is the inherent interaction and overlap with standard products. As cyber threats change, the extent to which property, liability and speciality cover responds to cyber events becomes increasingly blurred. This is relevant for general liability cover, but even more so for property cover and all-risk policies.

Policy wordings are currently inconsistent, with evidence of some clear cyber exclusions, some explicit inclusion (though in some cases merely through write-backs to remove exclusions) and many policies which are not explicit either way. For the purposes of codification, it is this final group which is clearly the most challenging.

Cyber threats generate uncertainty in coverage under standard exclusions on war and terrorism. The nature of a cyber attack means tracing (and proving) the event to a perpetrator is difficult. The fact that many attacks, although generated by nation states, are unlikely to be classified as an "act of war" means some coverage could be expected. How cyber terrorism is categorised has an impact on the management of aggregate exposures across underwriting and operational risk.

As demands for cyber cover increase and insurers begin to offer amalgamated or modular products, there may be a need to proportionally codify policies based on coverage, i.e. stand-alone cyber vs. liability vs. property.

Effective coding is a prerequisite to appropriately understanding and managing insurers' exposures to the accumulation of cyber risks. Therefore, correct codification of the risk is central to the ability of insurers to meet increased demand for insurance solutions for cyber risk in the long term.

How should CROs ensure that firms are taking steps to properly code exposure to cyber risk in the short term?

As insurers' internal systems and controls have developed to keep pace with progression in the cyber market, there is no single approach that will fit all companies and no clearly defined 'best practice'. However, a set of core principles have emerged across the industry which CROs can consider when working with underwriting colleagues to develop or evaluate the approach for coding exposure to cyber risk within their business.

In developing an approach to coding exposure to cyber risk, CROs should draw on their experience in increasing cyber risk resilience and the practices in section 2.2.2.

1) Keep the scope of cyber as broad as possible
In order to deal with the increase in the scope of losses caused by cyber attacks, a general best practice would be to code any policy involving cyber in either the initial event or the outcome as cyber. Coding an event which would be considered cyber terrorism as cyber and terrorism as opposed to just terrorism alone, as is often the case, is an example of how this would be achieved in practice. This small change in practice would provide insurers with a more detailed understanding of their true cyber exposure and would support effective pricing of risk.

This does present some practical challenges since casting the net too wide could lead to everything being classified as cyber. However, on balance, this is outweighed by the benefits of improved scrutiny and consistency in policy wordings and an understanding of accumulation potential.

2) Keep codification under review
The continuously evolving cyber threat requires the constant monitoring of the nature of the risk. Companies should acknowledge that any definitions created to understand the scope of cyber risk may become obsolete in a matter of months. Ongoing effort is required, but has the added benefit of placing insurers at an advantage in understanding and pricing risks.

A more granular approach to codification may become necessary over time in order to provide a richer and more comprehensive understanding of losses and exposures.

At present, cyber is generally described as one category which covers a range of different constituents. Property on the other hand, for example, has a range of codes to cover the different aspects involved such as flooding or fire. This may be replicated with cyber, for example distinct classification for technology Erorrs & Omissions (E&O) / professional indemnity, business interruption and cyber terrorism as distinct classes, rather than under a universal cyber categorisation.

3) Ensure underwriters in traditional lines consider cyber exposures
It is crucial to ensure that all exposure to cyber risk is coded in some way and that the potential for insurers to be exposed to cyber risk through more traditional lines of insurance is not overlooked. In addition to the physical damage that could be caused by an IT failure or cyber attack, insurers' portfolios may also be exposed to non-traditional cyber losses.

Developing a set of questions such as those included in Figure 5 can allow for a more accurate and replicable assessment of what constitutes cyber risk and allow for premiums to be apportioned accordingly. This approach would lead to a more consistent approach to coding and allow for improved communication of cyber risk exposures throughout companies.

Figure 5: Questions to determine what constitutes cyber risk.

4) Utilise industry loss data

There are a variety of third party initiatives which have gone live over the last 12 to 18 months which act as loss database services. For example, DataLossDB[8] collects information on data losses as a third party, and is publicly accessible for free. It is an Open Security Foundation project which scans news feeds, blogs and other sources for any data breaches. Contributions in the form of news articles or other information from external sources are appreciated, with more of this participation naturally leading to a more complete database. The information is then broken down and analysed, presented graphically for ease of understanding, and allows useful conclusions to be drawn on the trends of cyber threats.

Organisations whose practices for increasing cyber risk resilience include a comprehensive database of security incidents (see section 2.2.2) will be able to draw on their own experiences of cyber attacks to build loss databases. This will promote cross-functional communication between underwriters, risk management and information security.

[8] http://datalossdb.org/

How should efforts to promote industry-wide consistency be encouraged in the long term?

In the longer term, greater sharing of threat intelligence information will increase the insurance industry's understanding of and resilience to cyber risk.

Recently the Cyber Security Information Sharing Partnership has been launched to support the wider objectives of the UK National Cyber Security Strategy. This is "a joint, collaborative initiative between industry and government to share cyber threat and vulnerability information in order to increase overall situational awareness of the cyber threat and therefore reduce the impact upon UK business."

In other words, this operates like a cyber risk social network for companies, supported by the government. This voluntary, subscription-like model for sharing loss information on an industry scale is an example of the type of initiative which would greatly improve the industry's understanding and awareness of cyber risk.

Collecting a large amount of information on various incidents will allow for trend analysis of the types of attacks and losses. This has the potential to facilitate the codification of cyber risk. As insurers move towards utilising a more consistent taxonomy, there may be a need to clarify or modify some aspects of cyber policies.

One obstacle to the emergence of industry loss databases is the willingness of participants, particularly smaller companies, to include sensitive issues. Establishing a mechanism to share anonymised data is likely to be necessary to overcome this hurdle and should be part of a longer term roadmap for addressing this issue.

A cyber-risk database could be modelled on existing loss databases (e.g. those that exist for operational risks). The anonymity of such databases encourages reporting of events. However, it is acknowledged that databases which use publicly available information will almost never include full data sets.

3.2.2 Cyber risk exposure accumulation

Managing the accumulation of an insurer's cyber risk exposure in insurance portfolios is critically important to the success of an insurance market in cyber.

The simplest way to manage accumulation risk is to ensure cyber risk exposures are diversified by industry, counterparty and geography. However, the challenges presented by the interconnectedness of IT systems and the fact that the cyber insurance market is still developing mean that this approach is often not straightforward. As a result, insurers should extend their risk management frameworks that facilitate the identification and assessment of areas of potential accumulation.

How should CROs ensure that insurers understand how cyber risk exposure accumulates within insurance portfolios?

Considering the ubiquity and complexity of cyber risks, a scenario-based approach can provide a good solution for measuring and monitoring cyber risk exposure accumulation. The following sets out a process that can be used to establish and maintain a cyber risk exposure accumulation framework.

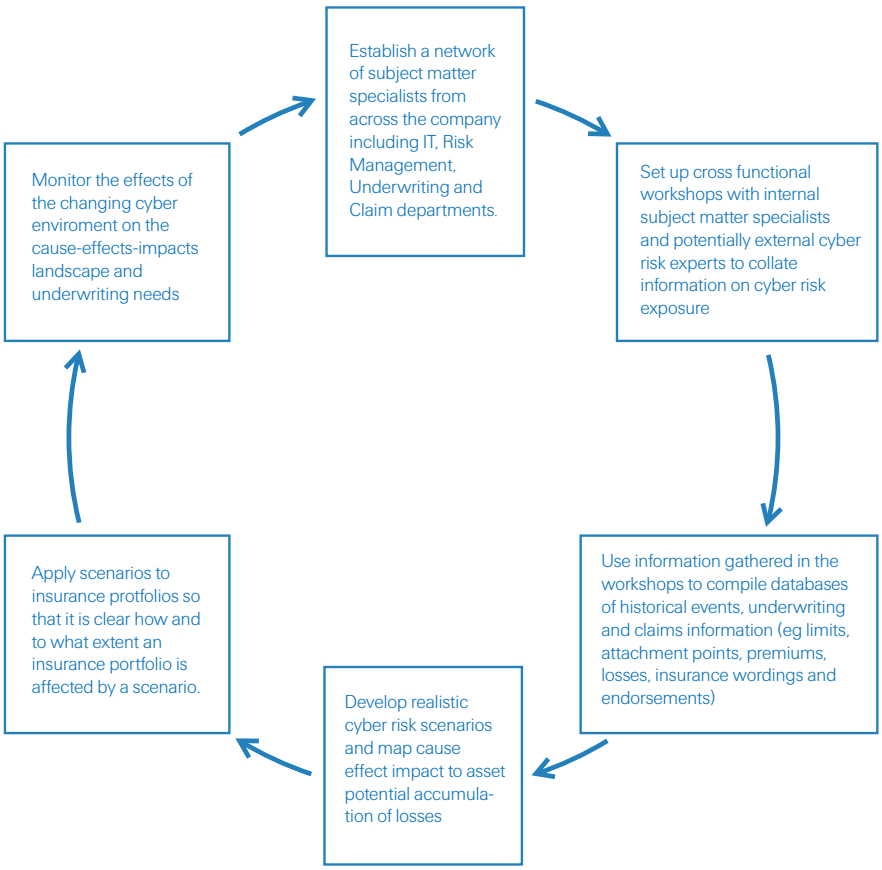


Figure 6: Example of potentially exposed insurance products.

Key steps in this process involve:

- The development of realistic cyber risk scenarios.
- An analysis of which insurance products are affected by a scenario and to what extent.
- A catalogue of cause effect impact maps[9] to allow insurers to visualise the types of cyber risks to which they are exposed and the damage that can be caused.

It is important to remember that the cyber risk landscape is not static and developments in IT, dependency on IT services, the development of instruments and tools to identify and use system vulnerabilities, motivation of hackers, legislation/ litigation may all change the results of the exposure accumulation assessment. Therefore, it is important that the framework is sufficiently dynamic to allow for scenarios to be regularly updated and cyber risk exposure accumulation to be monitored on an ongoing basis.

Developing of realistic cyber risk scenarios

For the development of realistic cyber risk scenarios, it is useful to consider the following categories:

Category 1: Cyber attack affecting cyber policies

Sectors which deal with sensitive data, which are protected under Data Protection laws, are particularly exposed to the types of cyber events set out in this scenario. Examples of affected sectors include retail, financial services and health.

For insurance companies, a critical loss accumulation can arise where a cyber attack causes many customers to lose data at the same time, for example as a result of malware quickly spreading (e.g. the "I love you" virus[10]).

The growing popularity of quickly available, inexpensive cloud services is exacerbating the problem and intensifying the interconnectivity of IT infrastructure, software and data. The outage of a large cloud service provider is likely to cause an uncontrollable and opaque chain reaction of losses.

A virus similar to the "I love you" virus, which spread explosively around the world in May 2000, today could affect many more devices and have a large accumulation loss potential.

[9] See "Summary of cause – effects – impacts" on page 37.

[10] en.wikipedia.org/wiki/ILOVEYOU – this was a computer worm that damaged local machines by overwriting image files and spread by sending a copy of itself to all addresses in the Windows Address Book used by Microsoft Outlook.

Category 2: Cyber attack affecting traditional lines
Cyber attacks can also lead to losses in the traditional classes of insurance business, for example when physical damage is caused (e.g. the "Stuxnet" virus). Such attacks can lead to heavy losses and are generally not sufficiently taken into account in risk assessments.

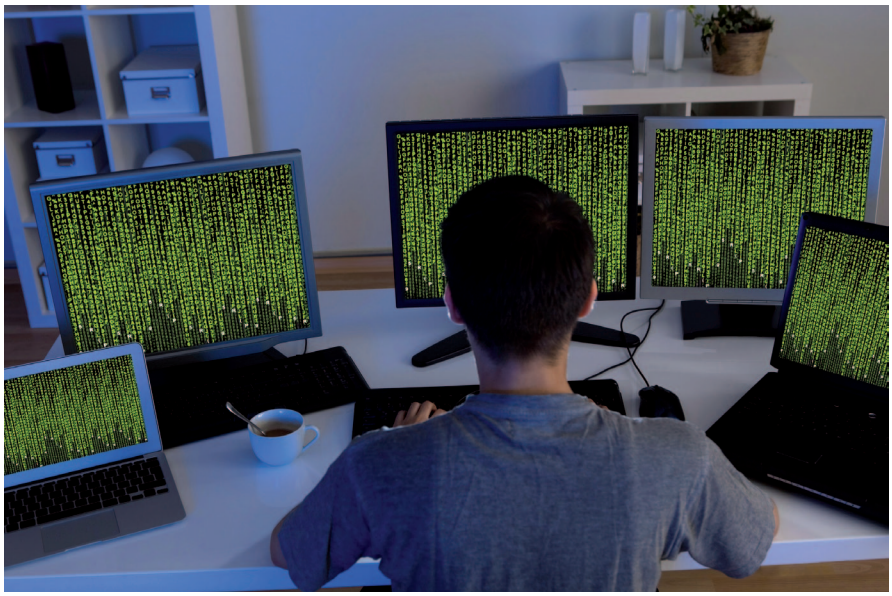
The costs could be particularly severe for critical infrastructure, including control of the water supply, transport systems (road, air, rail, and shipping), production facilities and factories (chemical plant, nuclear) or care of people (hospitals, backup systems). The increasing establishment of flexible remote access capabilities is making the problem worse as they can be exploited by cyber attackers.

The Stuxnet virus exposed the potential for cyber attacks to result in physical damage. Similar attacks which sabotage the facilities of a globally operating supplier and lead to physical damage have a large (accumulation) loss potential and are limited or excluded from the market.

Sources of accumulation losses in category 2 scenario:

The failure of the internet

The internet counts as critical infrastructure since most companies depend heavily on internet availability to run their business. The failure of the internet – or of a major part of it – could result in a high accumulation loss. This makes it very challenging to insure the failure of the internet to any significant extent[11]. This is especially true of reinsurance, which would be seriously hit by such a scenario.



Failure of the internet could lead to uncontrollable accumulation losses across all sectors and is generally excluded.

Power failure

High accumulation losses can be triggered by a power failure because of possible widespread chain reactions. Targeted cyber attacks on elements of the power grid could cause a power interruption. For example, a cyber attack on the Distributed Energy Resource Management System (DERMS) could result in damage to transformers, which are expensive and often difficult to replace.

"I am most concerned about coordinated physical and cyber attacks intended to disable elements of the power grid or deny electricity to specific targets, such as government or business centers, military installations, or other infrastructures." Mr Cauley, President of the North America Electric Reliability Corp.[12]

"Prolonged failures of the power supply are particularly critical, as they can have a lasting adverse effect on the economy and society."[13]

[11] One possible scenario leading to the failure of the internet would be an attack on the internet's DNS (Domain Name Service) server, which is responsible for converting domain names into IP (Internet Protocol) addresses. Any major disruption of its operation could not be absorbed by network redundancies.

[12] http://www.washingtontimes.com/news/2014/apr/16/inside-the-ring-us-power-grid-defenseless-from-att/?page=all

[13] See CRO-ERI Position Paper entitled "Power Blackout Risks"

Open source code

The increasing use of inexpensive and freely-available open-source code can cause accumulation losses for insurers. Where widely-used software modules are defective, extensive security vulnerabilities arise across many sectors. This was shown by the Heartbleed[14] security bug and, very recently, by the Bash Bug/ Shellshock[15]. The security vulnerabilities in the case of Heartbleed have still not been resolved months later and could still be misused today. In the case of the Bash Bug, the situation is still evolving.

Category 3: Non-cyber event affecting cyber policies

While traditional classes of insurance primarily cover physical damage, cyber policies mainly focus on losses arising from data security breaches that are (strictly) regulated in many jurisdictions. As described above, cyber insurance policies can be triggered by cyber incidents (see category 1), however, also by non-cyber events. Possible scenarios leading to such an occurrence are:

- Data media (laptop, USB stick, memory cards etc.) holding sensitive data that is either lost inadvertently or stolen with intent (e.g. by a disgruntled employee or during looting following a flood or earthquake); and
- Paper files holding personal data that could be stolen after improper disposal or destruction following a fire or a flood.

Companies from the health and commerce sectors are particularly exposed, as their business activity requires a great deal of sensitive information to be processed and stored.

Category 4: Cyber attack affecting insurers from both an operational and commercial perspective

Scenarios that affect both an insurers' insurance portfolio and restrict its business activity are particularly critical as they can cause extremely high (accumulation) losses. For example, a cyber attack could lead to physical damage with interruption of the power supply (see category 2), and affect the insurer and its insured customers. Carrying out cyber attacks of this nature requires considerable effort and is generally motivated by terrorism or war, with the aim of adversely affecting one or more countries in a significant way. Such attacks are usually executed through an attack on critical infrastructure.

Insurers regularly exclude such risks, because it is not possible to calculate the cyber risk exposure accumulation. However, the application of terrorism and war exclusion clauses is often ambiguous. A country with appropriate financial resources and the necessary team of attackers can launch a large-scale attack covertly, giving more potential for deniability. This distinguishes cyber terrorism from other acts of terrorism or warfare, making it more likely that cyber methods will be employed, and increasing the relevance of exclusion clauses. This has been demonstrated by historical cases such as the attacks on Georgia[16]. In this case, even though IP addresses from Russia were found, the government denied any participation and a declaration of war was never made. Therefore, it is uncertain whether an insurer's terrorism/war exclusion clauses would have been recognised in this case.

[14] HeartBleed – This was a critical vulnerability found in Open Source software called OpenSSL that provides encryption and is used by about two thirds of all websites globally. The vulnerability allowed anyone exploiting it to read random data blocks from anywhere in a web server's memory, including highly sensitive data such as user IDs, passwords and encryption keys.

[15] Shellshock is a nickname for a bug in the Bash command-line interpreter, known as a shell. This is widely distributed as the default interpreter in many operating systems that support back end infrastructure. Users of Bash that are connected to the internet are exposed to remote exploitation. The bug allows an attacker to perform the same commands as a legitimate user, giving the attacker the ability to do nearly anything that a user can do.

[16] http://en.wikipedia.org/wiki/Cyberattacks_during_the_Russo-Georgian_War

Factors influencing probability/severity of losses and accumulation potential

Building on realistic cyber risk scenarios, it is then necessary to analyse how and to what extent an insurers' insurance portfolio is affected by a scenario.
There are three broad factors influencing the cyber risk exposure accumulation – the type of industry, scope of cover and geography.

Type of industry

The main factors affecting the accumulation potential are industry related and encompass:

1) Dependency on IT and third party services e.g. data storage (cloud), transaction processing (stock exchange, credit card payments), automation (software) etc.
2) Types of data held e.g. financial (credit card, bank account numbers), private individual (social security, addresses, phone numbers, health), government (military, procurement), business (trade secrets, sales information) etc.
3) Vulnerability of the IT infrastructure.
4) Preparedness for IT failures e.g. business contingency planning.

Industry sector exposure rating

The industry factor reflects the vulnerability of the industry to cyber attacks and IT failures. An exposure rating (low-medium-considerable-high) can be allocated to the specific vulnerability in order to derive a factor for each industry sector:

Industry: Hotel sector	
Vulnerability	**Exposure Rating (Low – Medium – Considerable – High)**
Dependency on IT services (e.g. business interruption)	High
Dependency on the third party IT services (e.g. clouds, telecom, power supply)	High
Industry standards regarding preparedness against scenarios	Medium
Ability to restore information and if so the resources and time to restore	Medium
Legal requirements (e.g. disclosure/information requrements)	High
Likelihood of being targeted (e.g. the potential reason for the incident/motivation for malicious attacks)	Low
...	...
Total Industry Rating	**Medium**

Depending on the scenario, the factor sets range from highly exposed industries (e.g. financial institutions) to industries that have low exposure (e.g. construction), to data breaches as illustrated by Figure 7.

Figure 7: Example of types of industry exposed to loss (liability) of financial or personally identifiable information.

Scope of cover

The scope of cover provided by the insurance products – either explicitly or potentially unintentionally – is a key factor in analysing the accumulation exposure of the insurer (see Figure 8).

This reflects the fact that some lines are likely to be more at risk than others for specific scenarios. Products explicitly covering cyber risks (e.g. cyber liability, non-physical damage business interruption or technology E&O) are more exposed than other types of cover (e.g. data restoration endorsements provided in engineering or property/fire policies), which will contribute to the overall accumulation potential to a much lower degree.

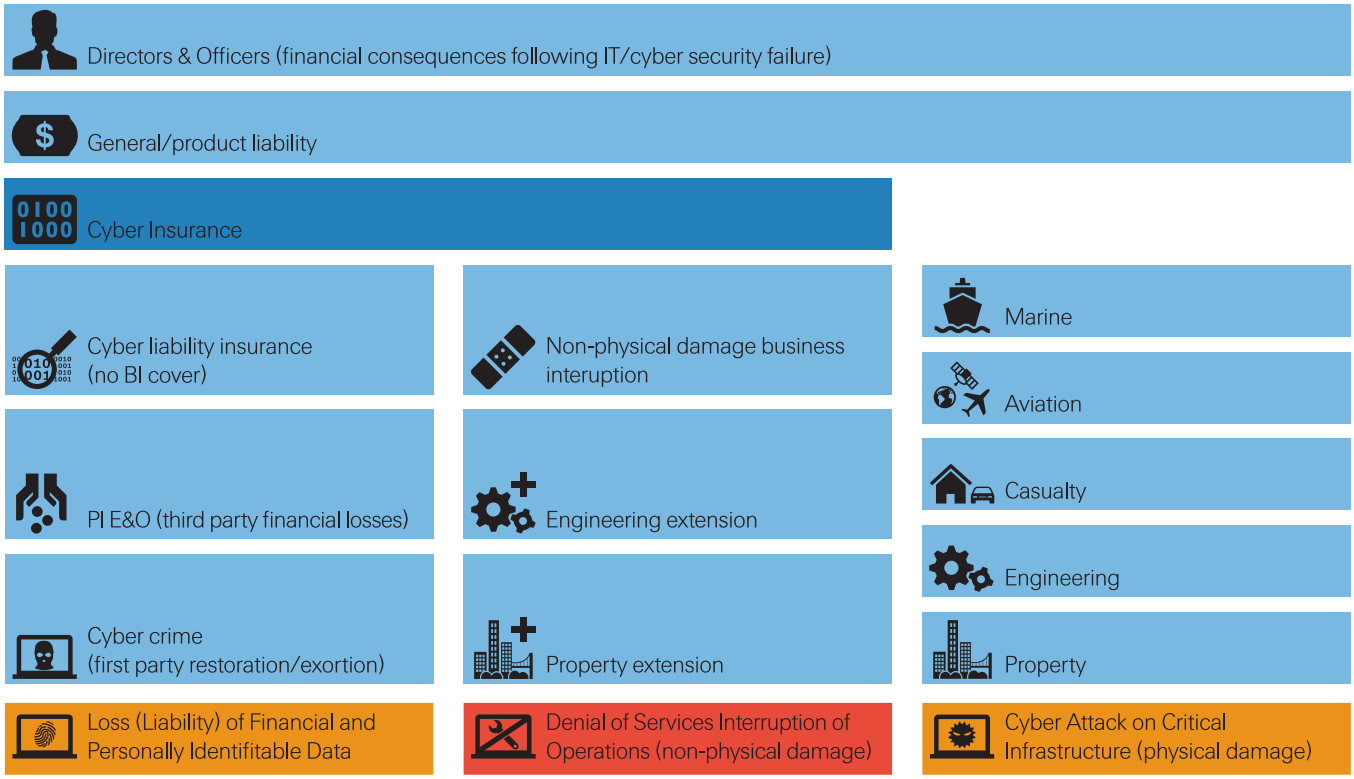


Figure 8: Example of potentially exposed insurance products.

Factors on the overall man-made event exposed portfolio (e.g. property, including material fire, damage, business interruption, or liability, including general liability, product liability, professional indemnity) may help to capture the cyber risk exposure, even if the identified scenarios would reflect a small portion of the overall portfolio. The exposure of the latter depends on the wording used. Many policies already contain exclusions[17]. For example, some energy risks are subject to a cyber attack exclusion[18], which excludes also physical loss or damage after a cyber attack. This may not remove all exposures, but can help to reduce the accumulation potential. Critical infrastructure is the most exposed to a SCADA[19] devices failure/attack.

[17] NMA 2912, 2914, 2915 or equivalent clause excludes loss due to computer programs, except a loss due to a named peril incl. fire and explosion.
[18] Institute Cyber Attack Exclusion Clause CL 380
[19] Supervisory Control and Data Acquisition (SCADA) – computer system which gathers and analyses real time data.

A wording check may help to identify the exposed insurance products and their potential contribution to the overall cyber exposure of a given insurance portfolio (see Figure 9).

As long as only a small number of plants could be simultaneously affected by cyber attacks, it is likely the insurer will be able to cope with the accumulation loss. If a large number of power plants were affected simultaneously, other exclusions like terrorism or war exclusions may apply.

The sophistication and motivation of the perpetrators of a cyber attack are key determinants of the cyber risk accumulation exposure. The discovery of governmental sponsored cyber attacks or the increasing use of the internet for terrorism or war-type attacks are new dimensions to the analysis, in addition to criminal organisations using the internet for economic profit. Insurers should consider whether it is appropriate to provide protection against cyber attacks that are more politically, than criminally, motivated. Terrorism and war-type attacks are traditionally on the cusp of insurability and any limitation or restriction, such as those used in traditional insurance products, could help to control cyber risk exposure.

Policy wording

Policy	Exposure to physical damage from the data malfunction
Policies without data clarification or data exclusion clauses.	Fire, explosion or other physical damage to tangible property resulting from data malfunction is covered.
Policies with limited data clarification or data exclusion clauses.	Exclusion clause does not mention fire, explosion damage as a consequence of data malfunction.
Policies with absolute data clarification or data exclusion clauses.	Fire, explosion etc. damage resulting from data malfunction are excluded.

Figure 9: Scopes of cover.

Geography

Depending on the cyber scenario, which may be rather first party or third party loss exposed, the use of different country/ regional (e.g. Americas, EMEA, Asia Pacific) factors seems reasonable. This is needed to reflect the different technical developments and standards, IT dependency, production costs/loss of profit in the various countries (mainly reflecting property exposures), or the legal and litigation environment (e.g. personal data protection), propensity to sue, compensation (liability exposures).

Developing a catalogue of cause effect impact maps

As noted above, a catalogue of cause effect impact maps can allow insurers to visualise the types of cyber risks to which they are exposed and the damage that can be caused. Below is an example of such a map, and illustrates how this type of analysis can help identify and quantify the accumulation risk factors. Such an analysis can also be used as a basis for internal discussions on cyber risk exposure accumulation.

Cause

A malicious hacker launches an attack on a power plant by embedding a set of code in email attachment masked as IT service tickets.

The attachment in such emails are opened by employees resulting in the installation of code on the plant's IT system, which then gives the hacker the ability to run a process to overload plant capacity resulting in transformer surge leading to power failure over a period of two weeks.

Effect

This results in damages to the plant's residential and business customers (power failure, food spoilage, climate control/burst pipes), as well as damage to the plant's transformer and physical assets.

The parent company of the plant experiences a stock price decline due to lost revenue given that this location was a significant contributor to its quarterly revenue.

The event also causes the parent company to hire a team of specialists to help with the recovery / investigation effort (forensics, IT security specialists, public relations firms, etc.) and restore the system to its pre-breach state.

Impact

Claims were made against the power plant for third-party property damage liability. Contingent business interruption claims were filed under property policies for businesses sourcing power from the power plant.

The power plant files claims against its IT security software provider for Errors & Omissions associated with software design, property damage claims with its property insurer to repair/replace the transformer and claims under its cyber liability policy for forensics, public relations, network restoration, etc. Investors in the parent company file a shareholder class action lawsuit against the company.

Summary of cause – effects – impacts

Cyber attack incident

All industries, in particular critical infrastructure like power generation & distribution
Industries relying on services provided by critical infrastructures like oil/gas, chemical/pharma

Effects
Machinery breakdown
Business interruption
Contingent business interruption
Bodily injury & third party property damage
Loss of profits/bankruptcy leading to shareholder claims

Geography
Worldwide, in particular countries vulnerable to cyber war or companies exposed to politically motivated cyber attacks (e.g. NGO's, cyber terrorisms) or revenge of former employees

Impact on lines of business
Property/Engineering
Property damage & business interruption
Contingent business interruption

Casualty
Worker's Compensation & Employers' Liability
General/product Liability (incl. pollution)
D&O Insurance

Stuxnet attack 2010
Costs unknown
(damage to installation only)

Aurora vulnerability experiment
Remote access & self-destruction of power generator by cyber attack

3.2.3 Risk management

The challenges of writing cyber insurance make determining a company's risk profile, setting risk tolerance limits and agreeing capital allocation complicated and unreliable. As a result, it is essential that risk management is involved in the development of an insurer's business strategy for covering cyber risks.

For organisations that introduce a Cyber Risk Appetite Framework as one of their practices for increasing resilience to cyber risk, it will be easier to ensure that the development of cyber insurance products is in line with the business strategy.

Consistent with the CRO Forum and North American CRO Council's joint paper "Establishing and Embedding Risk Appetite: Practitioners' view"[20] risk appetite encompasses the following three components:

1) Quantitative and qualitative measurement of risk

CROs can facilitate the development of risk measures in two ways. Firstly, by fostering cross-functional collaboration, bringing together specialists from across the business to improve the understanding of cyber risk and strengthen resilience. Secondly, by supporting the development of an approach to identifying, measuring and monitoring cyber risk exposure accumulation.

2) Setting limits and budget around the chosen risk measures

Once cyber risk exposure accumulation is understood, companies can establish boundaries according to the company's objectives and strategy to allow them to maintain their cyber risk exposure at a sustainable level. Boundaries may include risk tolerance limits based on the factors influencing probability/ severity of losses and accumulation potential e.g. maximum exposure to an industry.

3) Allocating risk budget and limits across sources of return in the business

Understanding cyber risk exposure accumulation is central to being able to allocate risk budget and limits across sources of return in the business.

The network of cross-functional, subject matter specialists should be consulted when establishing a Risk Appetite Framework. This should ensure that the risk limits and risk tolerance, both from an underwriting and operational risk perspective, are actually applied to the relevant risk.

Once developed, the Risk Appetite Framework for cyber risks should be integrated into key business processes across the enterprise. In this way, the Board will ensure through strengthened communication that Business functions – underwriting, IT, claims – are aligned with the strategy that they would like to implement and that there are adequate indicators to monitor risk limits and risk tolerance.

Insurers own practices for managing cyber risk should also help to inform the approach to underwriting cyber risk. Insurance can provide a lever to speed up companies' adoption of standard risk management practices such as the UK's Cyber Essentials Scheme by taking into account companies' cyber hygiene practices in the underwriting process.

Insurance plays a wider role in improving society's overall resilience to cyber risks by ensuring that premiums accurately reflect companies' cyber risk profiles. In a similar way, reinsurance can provide a lever for ensuring that insurers identify, measure and monitor cyber risk exposure accumulation.

[20] http://www.crocouncil.org/images/CRO_Forum-Council_Risk_Appetite_FINAL.pdf

3.3 Alternative solutions

Alternative cyber risk transfer mechanisms
The increasing importance of insurance as a component of companies' strategies for managing cyber risk has led to preliminary discussions on alternative cyber risk transfer mechanisms in order to supplement reinsurance capacity. For example, the possibility of cyber bonds and collateralised reinsurance is starting to be discussed.

Some market participants have suggested that there is appetite in the Insurance Linked Security (ILS) market for non-property risks. While casualty catastrophe bonds have been slow to develop, given long latency and uncertain emergence patterns, cyber bonds represent "event-driven" risks with binary outcomes over a defined time period. These risks could provide ILS fund managers with diversified returns on efficiently managed collateral.

Not surprisingly, other risk transfer mechanisms face similar challenges to an insurance market in cyber. Investors are looking for a loss distribution showing expected loss at various return periods based on empirical loss data, so that they can hedge their risks. However, for the reasons mentioned above, historical loss data can be insufficient or of poor quality. Pricing will therefore need to reflect a significant margin for uncertainty. Some market participants have suggested that the risk premium on a cyber bond must be able to survive an increase in the modelled loss result by a factor of two. Although a cyber bond has yet to be issued, estimates suggest that pricing could be much higher than for the primary cyber insurance market.

Despite the challenges, some believe that cyber presents an attractive opportunity for capital markets. Diversified income, collateral efficiency and binary outcomes may attract some niche ILS funds, who could allocate 5% - 10% of total funds for these deals. Capital markets may ultimately act as a complement to reinsurance, allowing insurers that face capacity constraints to top up their programmes.

Limits to insurance
Two areas are being actively discussed with regard to the government's role in cyber insurance – cyber war and terrorism. A proper assessment of these risks requires one to distinguish between asymmetric terrorist attacks (e.g., Al Qaeda, Inter-Services Intelligence, etc.) and more traditional warfare. It is theoretically possible to have a terrorist cyber attack on critical infrastructure, but less likely given a lack of sophistication and solid defences against such attacks. It is more likely for terrorists to use attack modes that allow for attribution which has been a critical driver of past events (e.g. 11 September 2001).

Nonetheless, questions remain about the availability of insurance cover for a terrorist-driven cyber attack. Some insurers suggest that the US Government's Terrorism Risk Insurance Program Reauthorization Act (formerly "TRIA") would apply to a cyber-driven attack on critical infrastructure. Others suggest that TRIA, as originally written, is explicit about attack modes and cyber is not mentioned in the act. Further, the act was written in 2001 to respond to a very different type of event than a cyber attack.

Cyber warfare is also a topic of discussion and is an active part of the military strategies of most major industrialised countries. That said, many industry observers suggest that the threat of a large scale global cyber war is overblown as the fate of most prominent economies (e.g., US, Europe, China, Russia, etc.) are tightly linked. Clearly, a cyber attack on the United States or Europe would cripple the economic growth trajectories of the fast growing economies. What's most concerning is not cyber warfare, but the growing practice of nation states stealing corporate trade secret and confidential information to improve their economies. Insurance is not the right instrument to manage these types of risk and clearly, this is an area where governments should aggressively manage the risk.

3.4 In summary

In summary, the cyber insurance market should continue to grow as a result of high-profile breaches, shifting regulatory policies and major cases. Companies can significantly improve their risk practices by adopting common cyber risk management practices. Insurers and reinsurers are actively learning more about these risks and the underwriting process is getting better as a result. As the market matures, capital markets may lend a hand in the expansion of capacity for cyber reinsurance as deals become more economically attractive. However, it should be recognised that there are limits to the role that insurance can play for managing the threat of cyber attacks. Sole reliance on insurance as a solution can create moral hazards[21] by reducing incentives to actively manage the threat of cyber attacks. In the case of cyber warfare, cyber terrorism and government sponsored cyber attacks, public solutions may be needed, with governments assuming responsibility as the reinsurer of last resort.

[21] ENISA 'Incentives and Barriers of the Cyber Insurance Market in Europe', June 2012 http://www.enisa.europa.eu/media/press-releases/enisa-report-calls-for-kick-start-for-kick-start-in-cyber-insurance-market

4 Conclusion

In today's interconnected world the reality of doing business in a cyber environment means that traditional approaches to IT security are no longer sufficient. Organisations underestimate the sophistication of cyber criminals at their peril and must remain vigilant to the evolving threat to ensure that they can detect cyber incidents and respond quickly and effectively.

While organisations cannot eliminate the cyber risk entirely, introducing practices that increase cyber risk resilience can help limit the economic loss and reputational impact in the event that an attack occurs.

CROs play an important role in improving understanding and cyber risk awareness throughout their organisations, including at board level. This is particularly important since vulnerability to cyber attacks stems more frequently from human error than from system flaws or technological weaknesses.

CROs can help foster open communication on cyber risks within their organisations, by pooling cross-functional knowledge and expertise to adapt the risk management framework to the specificities of cyber risk. For insurers in particular, the ability to draw on the experiences of underwriters, claim handlers, IT security experts and risk management will offer a broad range of perspectives on the issue. This will not only help insurers to bolster their own resilience to cyber risk, but also to develop insurance solutions for their clients and price the risk more effectively.

The fact that complete protection from cyber attack is unachievable strengthens the role that insurance can play in removing residual risk and increasing society's overall resilience. However, a well-functioning cyber insurance market requires appropriate risk management, including the codification of cyber risks and an understanding of cyber risk exposure accumulation, which are pre-requisites to a risk management framework. While, individually, organisations can, in the short term, take steps to improve understanding and cyber risk awareness internally, in the longer term greater collaboration within the sector is needed in the form of sharing cyber threat intelligence. Although organisations are reluctant to share information about their vulnerabilities and cyber risk incidents, pooling information will allow for trend analysis of the types of attacks and losses and enable companies to better monitor the imminence/acuteness of cyber risk.

Having supported CROs in their reviews of where relevant improvements to risk management practices exist and in light of the new emphasis on cyber risk resilience, this paper can provide a platform for a broader industry dialogue on a roadmap towards the development of a cyber-risk database.

5 References

Websites correct as at 19 December 2014.

"Risk and Responsibility in a Hyperconnected World", WEF in collaboration with McKinsey, 2014 http://www.mckinsey.com/insights/business_technology/risk_and_responsibility_in_a_hyperconnected_world_implications_for_enterprises

"Framework for Improving Critical Infrastructure Cybersecurity", National Institute of Standards and Technology, 2014
http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

"Evolving Cyber Threats – Can the Insurance Market Respond?", Ben Beeson, Lockton Companies LLC, July 2014
http://www.cyberrisknetwork.com/2014/07/11/can-insurance-market-respond-evolving-cyber-threats/

"Risk Index", Lloyd's, 2013
http://www.lloyds.com/~/media/Files/News%20and%20Insight/Risk%20Insight/Risk%20Index%202013/Report/Lloyds%20Risk%20Index%202013report100713.pdf

"Risk Codes – Guidance and Mappings", Lloyd's, May 2013
http://www.lloyds.com/~/media/Files/The%20Market/Operating%20at%20Lloyds/Resources/Risk%20codes/Y4694%20%20Risk%20code%20guidance%20notes.pdf

"Data Breach Investigations Report", Verizon, 2013, 2014
http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf
http://www.verizonenterprise.com/DBIR/2014/

"Establishing and Embedding Risk Appetite: Practitioners' view", CRO Forum and North American CRO Council joint paper, 2013
http://www.crocouncil.org/images/CRO_Forum-Council_Risk_Appetite_FINAL.pdf

"Inside the Ring: U.S. power grid defenseless from physical and cyber attacks", Bill Gertz, 2014
http://www.washingtontimes.com/news/2014/apr/16/inside-the-ring-us-power-grid-defense-less-from-att/?page=all

"Will Third-Party Reinsurance Capacity Permanently Shift Market Dynamics?", Barclays, 2014

"EU Cybersecurity plan to protect open internet and online freedom and opportunity - Cyber Security strategy and Proposal for a Directive", European Commission, 2013
http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

'Ahead of the Curve: Understanding Emerging Risks' Guy Carpenter, Emerging Risks Report September 2014
http://www.guycarp.com/content/dam/guycarp/en/documents/dynamic-content/AheadoftheCurve-UnderstandingEmergingRisks.pdf

"Cyber/Privacy Insurance Market Survey", The Betterley Report, 2013
http://betterley.com/samples/cpims13_nt.pdf

"Power Blackout Risks", the CRO Forum – Emerging risk working group, 2011
www.thecroforum.org/cro-forum-positioning-on-power-blackout-risks/

"Incentives and Barriers of the Cyber Insurance Market in Europe", ENISA, June 2012
www.enisa.europa.eu/media/press-releases/enisa-report-calls-for-kick-start-for-kick-start-in-cyber-insurance-market

Resilience Management Model, CERT, version 1.0, 2010
http://www.sei.cmu.edu/reports/10tr012.pdf

ISF: Information Security Forum
www.securityforum.org/

"ILOVEYOU", Wikipedia
http://en.wikipedia.org/wiki/ILOVEYOU

"Stuxnet", Wikipedia
http://en.wikipedia.org/wiki/Stuxnet

"Cyber attacks during the Russo-Georgian War", Wikipedia
http://en.wikipedia.org/wiki/Cyberattacks_during_the_Russo-Georgian_War

United States Department of Homeland Security,
http://www.dhs.gov/publication/cybersecurity-insurance

Title:
Cyber Resilience – The cyber risk challenge and the role of insurance

Working Group Members:
Swiss Re (Nick Kitching*, Neil Arklie, Juerg Busenhart, Charlotte Paterson, Dinesh Shah), ACE Group (Christopher Yaure), Achmea (Gerda van den Brink-Heikamp), Aegon (Walter Hansen), AIG (Anthony Shapella), Allianz (Claudia Meyer), Aviva (Dave Canham), Axa (Sara Albert, Pauline Briaud, Hélène Chauveau), Generali (Carlo Coggiola Pittoni), Groupama (Patrick Prosper), Legal & General (Jeremy Goodger), Lloyd's (Alexander Lucas, Avril Renehan), Lloyds Banking Group (Mark Goree), MAPFRE(Daniel Largacha Lamela, Jacinto Muñoz Muñoz), Munich Re (Heidi Strauß, Andreas Schlayer), NN (Aico Has), Old Mutual (Maurice Lee), Prudential (Ross McNay), RSA (Algy Booker), SCOR (Rémy Bague), Unipol (Stefano Nanni, Pietro Ranieri), Zurich (Carin Gantenbein)
* Working Group chair

Secretariat
KPMG (Michiel Mulder)

Cover Picture
iStock

Photographs
Swiss Re (p9, 29, 30)
Lloyd's (p10, 28)
iStock (p11)

Infographics:
Annie Wu, Swiss Re

Proofreading:
Orla Hare, Swiss Re

Editing:
Charlotte Paterson, Swiss Re

Layout and printing:
Corporate Real Estate & Logistics/Media Production, Zurich

Order no: 1506045_14_EN

The CRO Forum is supported by a Secretariat that is run by:

KPMG Advisory N.V.
Laan van Langerhuize 1, 1186 DS Amstelveen, or
PO Box 74500, 1070 DB Amsterdam
The Netherlands
www.thecroforum.org