Chapter 4

Cyber insurance market challenges

This chapter provides an overview of the main challenges to the development of the cyber insurance market in terms of both insurers' willingness to provide coverage and the demand from companies to acquire insurance coverage. The lack of historical experience and evolving nature of cyber risk create significant challenges for quantifying cyber risk. These challenges, along with concerns about the potential for accumulation risk, lead to higher prices and limited coverage levels. At the same time, the complexity of stand-alone cyber insurance policies, as well as the potential for coverage of cyber risk in traditional policies, leads to significant misunderstanding about the insurance coverage available for cyber risk. There are also concerns about whether cyber insurance policies are responding to the most pressing needs of policyholders.

The insurability of a given risk is usually economically viable only where certain criteria (or "principles of insurability") are generally met (Insurance Europe, 2012).[1] These criteria include:

- Risks must be quantifiable: the probability of occurrence of a given peril, its severity and its impact in terms of damages and losses must be assessable.
- A sufficiently large community with assets at risk can be established to share the risk (mutuality), allowing for sufficient diversification of the risk based on differences across the community in terms of risk exposure (i.e. a limited amount of correlation across the risks covered).
- Risks must occur randomly: the time and location of an insured event must be unpredictable and the occurrence must be independent of the will of the insured.

The extent to which the characteristics of a given risk exposure meets these criteria (among other factors) will impact whether insurance companies can collect the amount of premiums necessary to cover the total losses of a community of insureds (along with administrative costs and returns to investors, where provided by private insurance companies). For insurance to be economically viable, the actuarially-sound premium rates charged to policyholders must be both within their willingness-to-pay for protection and provide sufficient funds in aggregate to cover losses and other costs. The following sections will outline: (i) factors that drive up prices for cyber insurance coverage; and (ii) factors that lower the willingness-to-pay of consumers.

Factors affecting the price of cyber insurance

There are several factors that affect the price at which insurance companies are willing to offer coverage for a given risk, including the level of uncertainty in estimating expected losses (quantifiability), the size of expected losses (economic viability) and the diversity of the pool of risks covered (limited correlation). In the case of cyber insurance, the difficulties in quantifying a relatively new (and evolving) risk, and the potential for significant correlation across insureds (accumulation risk), are the most critical challenges in underwriting cyber risk. This uncertainty is reflected in lower limits offered, higher deductibles and the higher cost of coverage of cyber insurance relative to other types of insurance coverage (where there is more confidence in exposure quantification and a lower probability of correlated exposures). Limited availability (or uncertainty in the availability) of reinsurance coverage may also be a factor leading to a higher cost for coverage as primary insurers may face limits on their ability to transfer risk to reinsurance markets (reinsurance companies face the same challenges in underwriting coverage).

Quantifiability of cyber risk

Of the 36 insurance sector respondents to the OECD questionnaire that commented on challenges to extending coverage for cyber risks, almost two-thirds identified the ability to quantify cyber exposure as a concern (in general or in terms of certain elements required for quantification). There are three main challenges to the quantification of cyber risk: (i) lack of historical data on cyber incidents; (ii) changing nature of cyber risk (and the relevant legal framework); and (iii) access to corporate security information that is necessary for underwriting individual risks.

- *Limited availability of historical data*: As outlined in Chapter 2 (and in the section on underwriting in Chapter 3), the relatively recent emergence of cyber risk as a peril means that there is insufficient historical data to allow for accurate pricing of insurance premiums (Insurance Information Institute, 2015; A.M. Best, 2014; Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, 2016). This lack of data is exacerbated by the general unwillingness of the victims of cyber incidents to share information on these events and their impacts (unless required) out of concern for potential reputational impacts (CRO Forum, 2014; Young et al., 2016). For example, one estimate suggests that only 250 000 of the 5 million fraud and 2.5 million cyber-related crimes that occur annually in the United Kingdom are reported (White, 2016). Others have suggested that anywhere from 60% to 89% of all cyber incident go unreported (Edwards et al., 2014).

  Many insurance companies have entered into partnerships with information technology security firms to improve their access to information on incidents although, so far, few have reported that these partnerships have provided sufficient data and expertise to quantify cyber risk (although the value of these partnerships appears to be improving over time) (Council of Insurance Agents and Brokers, 2016a; Council of Insurance Agents and Brokers, 2017). While more data is becoming available as a result of increasing claims experience, the limited amount of cyber insurance coverage underwritten (partly as a result of the limited data for underwriting) reduces the utility of past claims data, leading to a vicious circle that hinders the ability to address data challenges (Deloitte, 2017). There were only 176 claims with an aggregate value of USD 114 million reported in the most recent NetDiligence (2016) study on US cyber insurance

claims experience (relative to the more than USD 1 trillion in gross claims payments made by US non-life insurers in 2015 (OECD, 2017)). Information sharing initiatives have also been established, although the lack of a shared taxonomy (as well as the different objectives for collecting information) are limiting the potential contribution that these initiatives could make to improving quantification (see Chapter 5).

- *Changing nature of cyber risk*: A potentially more significant challenge is that - even if more data were available - that data may become quickly out-of-date as a result of the fast-evolving nature of cyber risk (CRO Forum, 2014; Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, 2016; Eling and Wirfs, 2016). The perpetrators of cyber attacks can be expected to continue to improve their methods of attack (e.g. new data exfiltration methods, increased denial-of-service capacity or new technologies to support financial fraud and extortion (Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, 2016; Deloitte, 2017)) and find new ways to evade cyber security defences - which will have impacts on any estimates of frequency and severity based on historical cyber attacks. There are inherent challenges to estimating with any significant level of confidence the probability/frequency of incidents caused by human behaviour which can change based on learning from past experience. In the context of cyber risk, this is exacerbated by the involvement of state-sponsored actors whose motivations may be more difficult to understand. Technology and security practices developed to protect against cyber incidents are also constantly evolving, making it extremely difficult to quantify the effectiveness of different protective measures.

  In addition to changing tactics, increasing dependence on digital technologies for new applications and the resulting pervasiveness of connected devices is leading to new exposures (as well as providing additional capacity for malware transmission and DDoS traffic (Howard, 2017) - see Box 2.5). Some estimate that 3 trillion devices could be connected to the internet by 2020 (Allianz Global Corporate & Specialty, 2015), of which an estimated 70% are vulnerable to being compromised as a result of security weaknesses (Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, 2017). The increasing application of connected technologies in areas such as vehicles, medical devices and building (including residential) control systems, such as thermostats, creates potential for future exposure to physical damages and bodily injury (JLT Re, 2017). Almost all of the insurance sector respondents to the OECD questionnaire rated the emergence of the "Internet of Things" as a significant driver of the changing nature of cyber security risk (97% rated it as a moderate or important driver of the overall level of risk). The increasing use of bring-your-own-device as well as the increasing effort to provide new service platforms, such as mobile applications, could also increase the number of targets (CRO Forum, 2014). There is also an increasing amount of confidential data available to be compromised - one report suggests that the cost of data confidentiality breaches could increase by a factor of four by 2019 (relative to 2015) as a result of the continued "digitisation" of personal information (Cullina, 2017).

  Regulatory developments, such as the proliferation of notification and disclosure requirements will have an impact on the costs (and related penalties) involved in responding to data confidentiality breaches (see Box 2.2). In addition, compensation practices in the context of litigation (i.e. amounts due to injured

parties) continue to evolve (Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, 2016). For example, litigation in the US state of Florida created a precedent in 2013 for injury (and rights to damages) from the theft of personally-identifiable information without evidence that the losses were due to an identity theft (in this case, the opening of trading and banking accounts) that directly resulted from the breach - a significant departure from the previous practice of dismissing class action suits where no injury could be proven (Chalmers, 2013). A number of insurance sector respondents to the OECD questionnaire identified uncertainty (or evolutions) in the legal framework as a challenge to providing insurance coverage for cyber incidents, particularly in countries with no existing legislation on data confidentiality breach notification (and also as a result of differences in notification requirements across - and sometimes within - different countries).

- *Access to corporate security information*: A number of insurance companies identified the lack of transparency about security practices and past incidents as a significant obstacle to underwriting coverage (while brokers and risk managers raised concerns about the volume of information required and inconsistencies in the information required by different insurance companies). In particular, the results of penetration tests, as well as complete findings from forensic investigations were identified as information that insureds are reluctant to share with their insurers. For insurance companies, this creates a risk of asymmetric information and adverse selection (i.e., where the insured has a better understanding of the risk being underwritten than the insurance company). For the insured, sharing such information could create disclosure risks, should the insurance company be unable to protect against unauthorised access to the sensitive information or in the event of legal proceedings resulting from a cyber incident.

Accumulation risk

Building a large pool of diversified risks (independent and randomly-occurring losses) allows insurers to spread losses over a large number of insureds and mitigates the potential for a large share of the pool to be affected by losses simultaneously. All things being equal, a smaller pool, or a pool with higher dependencies across the risks covered, will lead insurers to require higher premiums (Schwarze and Wagner, 2007). In the case of cyber risk, there is significant potential for losses to be correlated across insureds and across different types of coverages provided to a single insured ("accumulation risk"). Unlike other perils, it is also more difficult to build a diversified pool of risks based on geography or even industry sector given dependencies on the same infrastructure, software and services (Fitch Ratings, 2017). According to some reports, the potential for accumulation risk across policyholders is the primary reason that insurers limit the coverage available for cyber risk (Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, 2016; Z/Yen Group, 2015; Lloyd's, 2015). Respondents to the OECD questionnaire (particularly those from the public sector) identified accumulation risk as one of the most important drivers of cyber risk and it was identified as a concern by more than 60% of the insurance sector respondents that provided information on challenges to providing cyber insurance coverage. Some respondents suggested that a catastrophic event (i.e. an event involving losses to many policyholders, such as the simultaneous exploitation of a vulnerability in a commonly-used software or system, or a disruptive incident at a major cloud services provider) could be beyond the market's

capacity and lead to numerous exits from the market (similar to what occurred after Hurricane Andrew in 1992 or the September 11 terrorist attacks in the United States). Others suggested that accumulation risk exists across many insurance lines (i.e. it is not unique to cyber) and that the early recognition of this issue in the case of cyber risk is a positive in terms of the sector's ability to manage it.

The most commonly cited sources of accumulation risk (Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, 2016; Allianz Global Corporate & Specialty, 2015; Insurance Information Institute, 2015) include:

- *Common software vulnerability*: A vulnerability in a commonly-used software that, if exploited, could result in widespread data corruption (see the loss scenario described in Box 2.7), encryption (as in the May 2017 "WannaCry" attacks, see Box 2.8) or data confidentiality breach (for example, what could have occurred as a result of the "Heartbleed"[2] vulnerability disclosed in 2014). This risk is exacerbated by what one analyst has described as the "monoculture" apparent in the use of similar software, security programmes and information technology infrastructure (Z/Yen Group, 2015). A scenario analysis by Lloyd's and Cyence (2017) of a vulnerability in a commonly-used operating system that led to exfiltration of first and third party confidential data estimated potential losses ranging from USD 9.68 billion to USD 28.72 billion, including notification and breach of privacy compensation costs and business interruption losses (among other costs).

- *Information technology services disruption*: Attacks on common information technology service providers, such as a cloud service provider (see Box 4.1), the domain name system (DNS) that underpins the functioning of the internet (see Box 2.5), or even the physical infrastructure on which digital technologies rely (such as undersea cables[3] or power supply) that could lead to disruptions in the operations of many insureds simultaneously. One analysis of an insured portfolio found that policyholders had a high-level of shared dependence on certain service providers, including two DNS providers (77% and 50% of policyholders used their services), a cloud service provider (55%) and two verification services providers (64% and 59%) (BitSight, 2016).

- *Critical infrastructure provider*: A cyber incident leading to the disruption of critical infrastructure services that are reliant on digital technologies (power supplies, payment systems, satellites or air traffic control systems) could lead to a broad range of losses across many business lines (see, for example, the blackout scenario described in Box 4.1).

- Given the levels of potential cyber risk in different types of policies (as discussed above), accumulation risk is also possible across policies covering a single customer (Z/Yen Group, 2015). For example, a cyber incident that leads to the malfunction of a critical component of a manufacturing process could cause property and business interruption as well as liability claims by shareholders (directors and officers) and customers if the malfunction leads to defective intermediate or final products (errors and omissions/professional indemnity, product liability). It is also possible that an investigation into a cyber incident could lead to the discovery of past attacks with implications for multiple insurers (depending on the terms and conditions of past policies and assuming the insured had placed cover with different companies over time) (Z/Yen Group, 2015).

Box 4.1. **Accumulation risk in cloud service providers**

Cloud service providers supply an increasing number of services to an increasing number of companies (Risk Management Solutions Inc. and Cambridge Centre for Risk Studies, 2016), including:

- software-as-a-service (SaaS) which provides companies with software accessible through cloud service and accounts for approximately half of cloud-related business volume;
- platform-as-a-service (PaaS) which provides companies with an environment for developing and managing their web applications and accounts for around 25% of cloud-related business; and
- infrastructure-as-a-service (IaaS) which provides companies computing power and resources such as servers and back-up services and accounts for around 20% of cloud-related business.

There are over 100 companies that provide various types of cloud services although the commercial market is dominated by Amazon Web Services, Microsoft, IBM and Google which account for approximately half of the overall market (Risk Management Solutions Inc. and Cambridge Centre for Risk Studies, 2016). Since 2011, the market for public cloud services has grown by almost 18% annually (Gartner, 2016) to over USD 100 billion (Statista, 2016) and by a further 53% in 2016 (Risk Management Solutions Inc. and Cambridge Centre for Risk Studies, 2017). A 2015 survey of information technology specialists worldwide found that 37% of companies depend on cloud services to provide over 25% of their information technology services (including 11% that depend on the cloud for over 50% of their services) and this is expected to grow to over 80% in the next 2-3 years (Spiceworks, 2015) (a more recent survey found that 63% of companies run information technology operations in the cloud (PwC, 2016b)).

While there are some risk management benefits related to the increasing use of cloud-based services (as the level of security provided by cloud service providers can be better than at individual companies), there is also a significant accumulation risk should the services provided by one of the main cloud service providers be disrupted or should the data that they hold be breached (Allianz Global Corporate & Specialty, 2015). The increasing use of cloud services was identified as being a moderate to important driver of the level of cyber risk by 95% of the insurance sector respondents to the OECD questionnaire. A survey of cyber security and risk experts in late 2016 identified a distributed denial-of-service attack on a cloud service provider as the "systemic cyber event" most likely to occur in the near future (i.e. a single event impacting 500 or more companies) (AIG, 2017). A key concern for insurance companies is the level of responsibility that cloud providers will accept in the case of a data confidentiality breach. Some have suggested that cloud service providers will bear only limited liability and that much of the costs of a data confidentiality breach could be borne by its clients (and their insurers) (Deloitte, 2017; Tsangaris, 2016).

This risk has so far been avoided on a large-scale (the four large cloud service providers generally achieve a 99.9% rating for reliability of service from third party rating services) although disruptions have occurred, including an 8-hour disruption to Amazon Web Services in 2011 (along with a 5-hour disruption in 2015 and a 5-hour disruption in 2017), a 4-day disruption to Google Cloud Gmail services in 2010, a 36-hour disruption to the Intuit cloud service (a provider of SaaS services for tax forms) in 2011 and a 24-hour disruption to Symantec's cloud-based security services (Risk Management Solutions Inc. and Cambridge Centre for Risk Studies, 2016; Risk Management Solutions Inc. and Cambridge Centre for Risk Studies, 2017). A similar accumulation risk is present in managed service providers that manage the applications, networks and/or systems infrastructure of other companies. In 2017, security researchers announced that managed service companies had been targeted by a particular hacking group in order to gain access to their clients' networks. While no information was available on the impact of the resulting data confidentiality breaches, the attacks reportedly affected organisations across 15 countries in Europe, North America, South America, Africa and Asia (Trend Micro, 2017).

In 2017, Lloyd's and Cyence (2017) released a scenario based on the inclusion of malicious code in open-source generated "hypervisor"[1] software commonly-used in operating cloud services. Under the scenario, sophisticated companies using "Tier 1" cloud service providers face an outage of at least 55 hours while less sophisticated organisations dependent on "Tier 2" cloud service providers face an outage of up to 5 days and 19 hours. Based on the scenario and estimates of dependence on cloud service providers across different sectors (as well as the availability of alternative business processes), they estimate that losses in terms of lost income and extra expense (i.e. losses that could normally be insured under cyber insurance policies with coverage for cloud service disruptions) would range from USD 4.6 billion ("large loss") to USD 53.05 billion ("extreme loss") depending on the ultimate duration of the outage. When levels of cyber insurance penetration, as well as the sub-limits commonly applied to contingent business interruption coverage, are taken into account, the report estimates insured losses ranging from USD 620 million under the large loss scenario to USD 8.14 billion under the extreme loss scenario.

1. A hypervisor is a type of software that provides a virtual machine platform for executing and monitoring multiple operating systems. In the context of cloud services, hypervisors are used to separate and maintain the privacy of separate virtual machines and are therefore a critical component of the cloud services infrastructure (Lloyd's and Cyence, 2017).

Reinsurance availability

The lack of historical experience, a changing risk landscape - and particularly the potential for accumulation risk - will also impact the availability of reinsurance coverage for cyber risk. Some reports have suggested that there is limited reinsurance availability for cyber risks, that this may be an impediment to the capacity of primary insurers to provide cover, and that a catastrophic cyber event might require a government backstop (Z/Yen Group, 2015; Insurance Information Institute, 2015; Lloyd's as reported by Mitchell, 2015; Swiss Re as reported by Faulkner, 2017). However, very few OECD questionnaire respondents (4 of the 28 insurance sector respondents (excluding reinsurers)) identified availability of reinsurance capacity as an impediment to providing coverage. A number of recent reports have also suggested that there is significant capacity (and appetite) in the reinsurance market for cyber risks (JLT Re, 2017), evident in the growing range of coverage structures available, including both proportional (quota share) and non-proportional (aggregate stop-loss, per risk excess-of-loss and per event excess-of-loss (Swiss Re, 2016b; Aon Benfield, 2016; JLT Re, 2017)).

The offering of reinsurance coverage for cyber risk does face some structural challenges given the mix of first party (property) and third party (liability) coverage that is usually included in stand-alone policies (Parsoire, 2014). As a result, most reinsurance coverage for US cyber risk has been embedded into other treaties such as specialty casualty, errors and omissions and directors and officers (S&P Global Market Intelligence, 2015). Reinsurers may also be providing significant amounts of implicit (silent) coverage through their traditional lines as exclusions are not commonly applied in casualty (liability) reinsurance programmes, while the cyber exclusions that are sometimes applied by reinsurers on property reinsurance coverage are generally untested (JLT Re, 2017; Prudential Regulation Authority, 2016).

Stand-alone reinsurance coverage has begun to emerge. Five reinsurance companies provided responses to the OECD questionnaire and two provided some details on the types of losses that they would cover. Coverage is available from both reinsurers for crisis management, data restoration and the major types of liability (breach of privacy compensation, network security failure and communication and media), although only one reinsurer provided coverage for extortion and fraud. One of the two reinsurers noted that their reinsurance coverage was provided both on a stand-alone basis and in combination with other perils.

There are some reports that reinsurance coverage is being provided cautiously through the use of sub-limits and event limits (i.e. placing limits on payouts linked to a particular "event") in order to manage the potential for accumulation risk (S&P Global Market Intelligence, 2015; Deloitte, 2017). Much of the coverage that has been made available, especially in terms of stand-alone coverage, has been provided as quota share (proportional reinsurance) (Risk Management Solutions Inc. and Cambridge Centre for Risk Studies, 2017; Héon and Parsoire, 2017). As noted, non-proportional stop-loss and per event/occurrence excess-of-loss coverage (which may be better positioned to address accumulation risk) is becoming increasingly available (although excess-of-loss structures must overcome the challenge of defining the event for which the coverage applies).

According to some estimates, there are 20 reinsurers offering some coverage for cyber risk (S&P Global Market Intelligence, 2015). One estimate suggested that there was approximately USD 500 million in reinsurance premiums collected for cyber risk in 2015 (Héon and Parsoire, 2017). The market is generally stable, with few new large entrants, and a significant share of overall capacity provided by three large reinsurers.

Similar to the primary market, reinsurance pricing appears to be generally defying the soft pricing in other business lines with reports of a hardening market in 2015 and 2016 (particularly for sectors such as retail and healthcare) (Swiss Re, 2016b) and some continued price increases in loss-affected programmes in 2017 (although with some loss-free programmes renewed at a discount (JLT Re, 2016)). There are some reports suggesting significant potential for transfer of peak cyber risks to capital markets through insurance-linked security structures (Artemis, 2017; Yoder and Nocera, 2016). One bank's transfer of operational risk (including cyber risk) to capital markets in 2016 provides relevant experience (see Box 5.5).

Box 4.2. **Coverage of cyber-related losses by terrorism insurance programmes**

A number of countries have established terrorism insurance programmes to provide coverage for losses resulting from terrorist attacks. These programmes are generally structured to include some level of retention by the insurance industry supported by a layer of re/insurance coverage provided by a publicly-backed pool. In many cases, the coverage is triggered based on a statutory definition of a terrorism event (often tied to a government declaration that a given event was a terrorist attack). In some countries, the definition of a terrorism event might include attacks using information technology or attacks on information technology.

In 2016, the OECD undertook an informal survey among its contacts at terrorism insurance programmes to determine the extent to which losses from a cyber terrorism attack might be covered by the insurance offered by these programmes - focused on denial-of-service attacks and malicious system malfunctions affecting industrial control systems (see Table 4.1). In some countries, including Australia, Germany and the United Kingdom, cyber attacks are specifically excluded from the definition of an event that would trigger programme coverage. In Russia, the underlying policies reinsured by the terrorism insurance programme consistently exclude cyber as an eligible peril for coverage. Coverage from the Terrorism Risk Insurance Program (TRIP) in the United States also depends on the nature of the underlying coverage provided which, in some cases (e.g. property, liability and worker's compensation), may provide some coverage of losses resulting from cyber attack. The US Treasury published guidance in December 2016 on the inclusion of cyber liability as a class of insurance that could be eligible for TRIP coverage (US Department of the Treasury, 2016). In France and Spain, there is some potential for coverage for physical (material) damage (including intangible assets in Spain) resulting from a cyber attack as well as, in the case of Spain, for business interruption arising from direct damages (where business interruption is explicitly included in the underlying policy). In France, the terrorism reinsurance pool (*Gestion de l'Assurance et de la Réassurance des Risques Attentats et Actes de Terrorisme* (GAREAT)) modified its internal regulations in 2017 to clarify that non-material damages resulting from an act of cyber terrorism are excluded from its coverage. Bodily injury resulting from a cyber attack would also be covered in Spain. A number of countries are examining the appropriateness of the coverage currently provided by terrorism insurance programmes for cyber terrorism (see for example: Australian Reinsurance Pool Corporation, 2016).

Table 4.1. **Terrorism insurance programme coverage of cyber-related losses (DDoS, system malfunction): selected countries**

	Physical damage	Business interruption (without material damage)	Data and software loss	Bodily injury
Australia	*----------cyber attacks are specifically excluded from the definition of terrorism event---------*			
France				
Germany	*----------cyber attacks are specifically excluded from the definition of terrorism event---------*			
Russia	*----------cyber attacks are excluded from coverage in underlying policies----------*			
Spain				
United Kingdom	*----------cyber attacks are specifically excluded from the definition of terrorism event---------*			
United States				

Likely covered Potentially covered Not covered

In the case of cyber attacks related to terrorism, some re/insurance coverage may be available through terrorism insurance programmes (see Box 4.2), although a significant challenge lies in (openly) attributing a cyber attack to a terrorist organisation (or otherwise defining it as a terrorism event) (CRO Forum, 2014). Lloyd's has indicated an interest in examining the extent to which existing war and terrorism exclusions have been - and should be - extended to cover cyber terrorism (Lloyd's, 2016). The terrorism pool in the United Kingdom (Pool Re) has reportedly had discussions with the government and industry about extending the coverage it provides to cyber terrorism (Cohn, 2017). Some reports have suggested that the US insurance industry is also asking the US Congress to consider a government backstop for major cyber attacks similar to the Terrorism Risk Insurance Program (Basak, 2015).

Factors affecting the willingness-to-pay for cyber insurance coverage

While the level of uncertainty in quantifying cyber risk and the high potential for accumulation risk will lead to higher prices for cyber insurance coverage, a number of factors are likely to reduce the demand/willingness-to-pay for coverage, including a lack of awareness of potential losses from cyber risk, misunderstandings about the need for coverage as well as a potential mismatch between the coverage offered and what companies are seeking.

Lack of awareness of potential cyber losses

While cyber risk has often been identified as an underestimated risk with limited attention from senior executives and directors, many more recent surveys have suggested that this is changing even outside of the United States where awareness levels have already been generally high for many years.[4] In the United Kingdom, annual surveys of cyber risk perceptions and incident experience found a substantial increase in the number of companies that considered cyber to be a top-10 risk between 2015 and 2016 (from 45.8% to 71.8%) and the share of companies' whose senior management consider cyber security as high or very high priority (from 68% in 2016 to 74% in 2017) (Department for Culture, Media and Sport, 2017; Department for Culture, Media and Sport, 2016). In continental Europe, the share of companies that included cyber as a top-5 risk on their risk registers increased from 19% in 2015 to 32% in 2016 (while the share of companies not including cyber on their risk survey declined from 23% to 9%) (Marsh, 2016a). Similarly, another recent survey of European business executives found a significant shift in responsibility for issues such as cyber protection and data breach plans from the Chief Information Officer to the Chief Executive Officer as shareholders increasingly expect CEOs to take responsibility mitigating cyber as risk to financial performance (Lloyd's, 2016).

Although the level of awareness of cyber risk and senior management attention to cyber security appear to be increasing, there appears to be a gap in terms of translating cyber risk into estimates of potential losses which would normally be a prerequisite to any decision on the purchase of insurance coverage. In continental Europe, a recent survey found that just over half of companies had identified potential loss scenarios, although only 40% had evaluated potential financial impacts and strategies for funding those losses (Marsh, 2016a). A survey in the United Kingdom found that the share of companies that had estimated the potential financial impact of a cyber incident actually declined from 39.9% in 2015 to 35.4% in 2016 (Department for Culture, Media and Sport, 2016). This is consistent with a survey by Advisen (2014) which found that, for

73% of insurance broker respondents, insureds' lack of understanding about the potential financial impact of cyber incidents was the biggest impediment to purchase. It might also be a factor in the relatively low proportion of companies that evaluate the adequacy of their insurance coverage on the basis of internally-generated risk assessments (13% based on a survey of global companies (Ponemon, 2017)) and that use return-on-investment analysis in decisions on security investments (6% based on a survey of UK companies (Department for Culture, Media and Sport, 2017)). This lack of understanding of financial exposure has led many companies to make insurance purchase decisions based on industry benchmarking (i.e. *how much insurance has my competitor bought?*) rather than an assessment of actual needs.

Misunderstandings about coverage

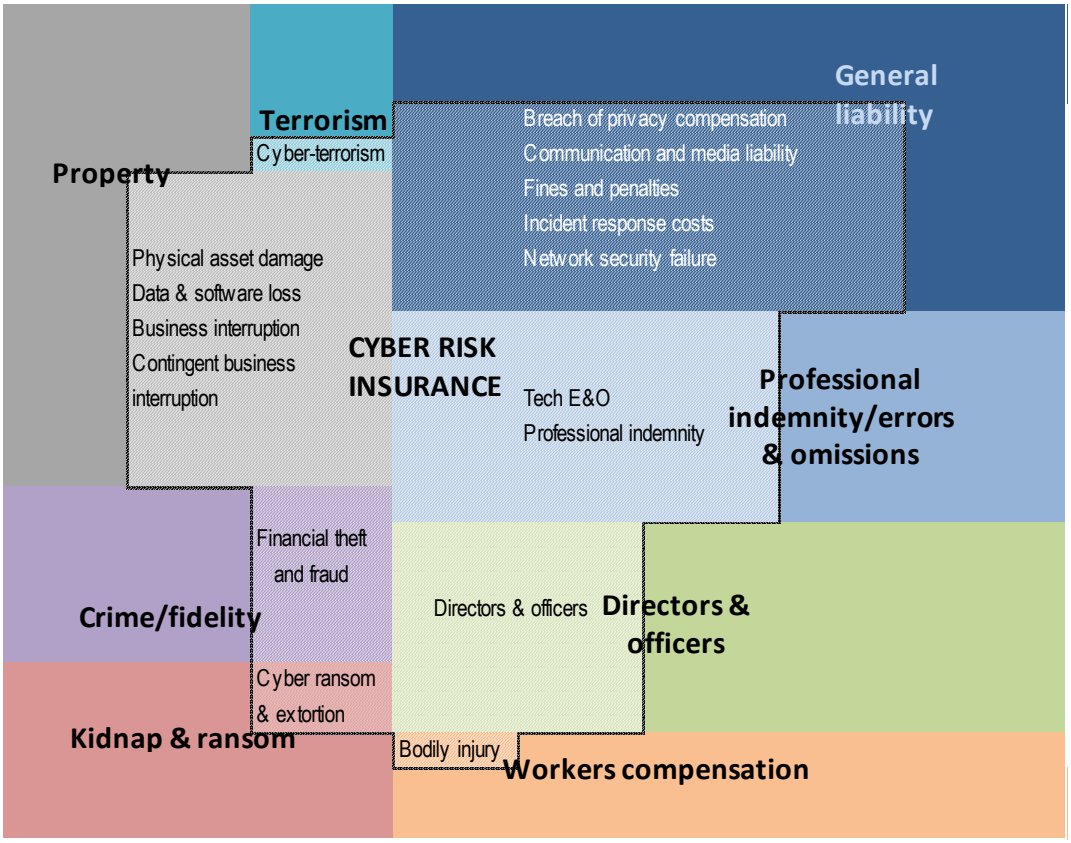
Misunderstandings about insurance coverage for cyber risk, beginning with a lack of awareness about the availability of specific coverage for cyber risks, are widespread. For example, a 2016 survey of European businesses found that 50% were unaware that cyber coverage for data confidentiality breaches was available (Lloyd's, 2016). There are also significant misunderstandings about the level of coverage provided by traditional policies for cyber risks as well as challenges in understanding the specific conditions and coverage limitations in different cyber insurance policies.

As noted in Chapter 3, depending on the exclusions applied, a number of traditional policies could provide some coverage for losses related to cyber incidents, including property, general liability, directors and officers, errors and omissions/professional indemnity, crime and kidnap and ransom. The expectation of coverage (or misunderstanding about the level of coverage) in traditional lines is often cited as a major reason for low levels of cyber insurance take-up (Deloitte, 2017; ENISA, 2012; Swiss Re, 2016a). A recent global survey found that 30% of respondents perceived that their existing property and casualty policies provided sufficient coverage for cyber risks (Ponemon Institute, 2017). This makes it difficult for companies to determine what coverage gaps they may face as a result of cyber risks and how best to address these gaps. Even companies that seek the assistance of brokers may receive different advice. There are conflicting reports, for example, on whether brokers are increasingly advising their clients to purchase stand-alone cyber insurance policies (Council of Insurance Agents and Brokers, 2016a) or seek endorsements on existing policies (Z/Yen, 2015).

These challenges are unlikely to be addressed in the near-term, as some insurers are expanding the scope of stand-alone cyber insurance to cover a broader range of risk while others are expanding the scope of traditional coverage to include cyber risk (Moynihan, 2017). Figure 4.1 provides an illustration of the potential for overlapping coverage between stand-alone cyber policies and various traditional policies (i.e. the centre of the illustration shows the component parts of stand-alone cyber insurance policies and where that coverage might be (or have been) provided in traditional policies).

There are also significant differences in the types of coverage, exclusions and conditions applied in different stand-alone cyber insurance policies (ENISA, 2012; Deloitte, 2017) - and rapid changes as policy language evolves to respond to claims experience, legal interpretations and competitive imperatives (Carbone and Ryan, 2016). Among the stand-alone policies recently reviewed by the Risk Management Solutions and the Cambridge Centre for Risk Studies (2017), only two were found to offer the same set of coverages.

Figure 4.1. **The potential for overlapping coverage for cyber risk in stand-alone and traditional policies**



Source: OECD based on JLT Re (2017).

There are also a number of differences in the specific terms and conditions of stand-alone cyber insurance policies. For example, the triggers for payment among policies offered by the respondents to the OECD questionnaire vary significantly in terms of the time basis for payment (i.e. date that a claim is made ("claims-made basis"), date that the attack took place ("occurrence basis") and date that the attack was discovered ("discovery basis")), as well as whether or not retroactive coverage was offered (a critical issue given that it took an average of 191 days in 2016 for a company to identify that a malicious privacy breach had occurred on its network (Ponemon Institute, 2017)). Some respondents provided retroactive coverage for liability claims made while others provided retroactive coverage relative to the occurrence date and only for first party losses - with varying levels of retroactivity offered (usually 1-3 years). There are also important differences in terms of: (i) coverage of non-malicious acts, including human error (as noted specifically in the case of fraudulent fund transfers); (ii) coverage for voluntary (vs. mandatory) notification costs; and (iii) scope of coverage provided in the definition of "computer system" (i.e. whether outsourced systems are included) (Lloyd's and Cyence, 2017).

Various surveys of brokers, who play a critical role in helping companies understand the coverage being offered, have identified frustrations due to the lack of harmonisation across policy offerings (definitions, terminology, limits, endorsements, exclusions, etc.) and the resulting difficulty in comparing offers without a detailed review of terms and

conditions (Advisen, 2014; Council of Insurance Agents and Brokers, 2015a). As a result, some brokers have reportedly reduced the number of insurance companies that they work with on cyber insurance (Council of Insurance Agents and Brokers, 2016a), with potential implications for the competitiveness of the market.

While these differences in coverage may provide more choice for the insureds, the lack of harmonisation of policy language and conditions also seems to reduce the attractiveness of cyber insurance policies. A recent survey found that, for 27% of respondents, too many exclusions, restrictions and/or uninsurable risks were driving factors in their decision not to purchase cyber insurance coverage (Ponemon Institute, 2017). Policy complexity and lack of harmonisation may also be creating trust issues among policyholders - surveys by KPMG of information technology professionals in the United Kingdom found that close to 50% did not believe that their cyber insurance policies would pay out in the event of a cyber attack (Reeve, 2015; Z/Yen, 2015).

However, there are some signs that the situation is improving – including reports of increasing harmonisation in the US market (Harrington, 2017) as well as a declining share of brokers that feel there is insufficient clarity on what is covered and what is excluded (55%, down from 71% in 2015) (Council of Insurance Agents and Brokers, 2016b).

Coverage that is not suited to the needs of policyholders

A third factor impeding the willingness-to-pay for cyber insurance coverage is the perception that the products being offered do not provide sufficient coverage for the most important costs that result from a cyber incident. In a survey of UK firms, 77% of companies that provided an opinion on whether insurance coverage for cyber incidents met their coverage needs indicated that it only partially met (or did not meet) their needs (Marsh, 2016b). A global survey of companies found that inadequate coverage relative to exposure was an important driver of the decision not to purchase cyber insurance for 36% of respondents (Ponemon Institute, 2017).

Although the specific reasons why insurance is not meeting all the needs of companies were not identified, limited coverage for reputational damages (i.e. loss of profits due to customer churn) and own intellectual property theft are likely important reasons. Surveys regularly find that the reputational damage resulting from cyber incidents is a key concern for companies (only behind business interruption) while recent surveys of European and UK companies have found reputational damage to be a growing concern (Allianz Global Corporate & Specialty, 2017; Marsh, 2016a; Marsh, 2016b). As noted in Chapter 3, the gap in coverage for reputational damage and intellectual property theft is not specific to cyber insurance. In addition, actual reputational damage from cyber incidents may be less significant than perceived (as outlined in Chapter 2), particularly as more and more companies are affected by serious incidents.

Notes

1. The discussion of insurability in the cited report is undertaken in the context of natural catastrophes although the principles are transferrable to other types of risks.
2. The "Heartbleed" vulnerability was publicly disclosed in April 2014 as a serious vulnerability in the commonly-used OpenSSL cryptographic software library which,

if exploited, would allow for the stealing of information that is normally protected by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs) (heartbleed.com, 2014).

3. In 2013, damage to several undersea cables led to a disruption of the internet in Africa that lasted almost one day and had a broad range of impacts including, for example, an interruption to the communications necessary for processing foreign payment card transactions (The Geneva Association, 2016).

4. For example, PwC's annual survey on economic crime (2016a) consistently finds more experience with cyber crime and particularly losses from cyber crime in North America relative to other regions. The 2016 survey found that 46% of North America respondents had experienced cyber crime within the last 24 months, relative to 42% in Western Europe and 32% globally. In addition, 31% of surveyed companies in North America had experienced losses over the previous 24 months of more than USD 100 000 (including 14% that had experienced a loss of more than USD 1 million) relative to 13% of Western European respondents and 16% of global respondents that had experienced losses in excess of USD 100 000.

References

Advisen (2014), *Cyber Liability Insurance Market Trends: Survey*, Advisen Ltd. (October).

AIG (2017), *Is Cyber Risk Systemic?*, American International Group, www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/aig-cyber-risk-systemic-final.pdf.

Allianz Global Corporate & Specialty (2017), *Allianz Risk Barometer: Top Business Risks 2017*, Allianz Global Corporate & Specialty SE, Munich.

Allianz Global Corporate & Specialty (2015), *Guide to Cyber Risk: Managing the Impact of Increasing Interconnectivity*, Allianz Global Corporate & Specialty SE, Munich, www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf.

A.M. Best (2014), "Cyber Security Presents Challenging Landscape for Insurers and Insureds", *Best's Special Report, Issue Review*, 5 December.

Aon Benfield (2016), *Reinsurance Market Outlook: Capacity Gap Narrows as Demand Picks Up*, September, Aon plc.

Artemis (2017), "Cyber risks and government pools. Too soon?", *Artemis news articles*, 30 March, www.artemis.bm/blog/2017/03/30/cyber-risks-and-government-pools-too-soon/.

Australian Reinsurance Pool Corporation (2016), Cyber Terrorism and Australia's Terrorism Insurance Scheme: Physically destructive cyber terrorism is a gap in current insurance coverage (March), Australian Reinsurance Pool Corporation, http://arpc.gov.au/files/2016/03/ARPC-Cyber-Terrorism-Discussion-Paper-FINAL.pdf.

Basak, S. (2015), "Worried About a Cyber-Apocalypse? AIG Wants to Sell You a Policy", *Bloomberg*, 22 July, www.bloomberg.com/news/articles/2015-07-22/worried-about-a-cyber-apocalypse-aig-wants-to-sell-you-a-policy, accessed 4 November 2016.

BitSight (2016), *Risk Degrees of Separation: The Impact of Fourth party Networks on Organizations*, BitSight, Cambridge (Massachusetts)

Carbone, W. and T. Ryan (2016), "Cyber liability insurance: As the market heats up, is it time to cool off in a pool?", *Milliman Insight*, 23 May, http://us.milliman.com/insight/2016/Cyber-liability-insurance-As-the-market-heats-up--is-it-time-to-cool-off-in-a-pool/.

Chalmers, H. (2013), "Recent Ruling Could Prove Costly for Hacked Businesses", *The Privacy Advisor*, 1 April, https://iapp.org/news/a/2013-04-01-recent-ruling-could-prove-costly-for-hacked-businesses/, accessed 9 November 2016.

Cohn, C. (2017), "Terrorism Reinsurance Fund in UK Wants to Add Cyber Cover", *Carrier Management*, 10 March, www.carriermanagement.com/news/2017/01/12/163026.htm.

Council of Insurance Agents & Brokers (2016a), *Cyber Insurance Market Watch Survey: Executive Summary*, Council of Insurance Agents & Brokers (April).

Council of Insurance Agents & Brokers (2016b), Q2 Commercial P/C rates continued decline, according to CIAB Market Survey", *News Release*, 4 August, Council of Insurance Agents & Brokers.

Council of Insurance Agents & Brokers (2015a), *Cyber Insurance Market Watch Survey: Executive Summary*, Council of Insurance Agents & Brokers (October).

Council of Insurance Agents & Brokers (2015b), Pricing continued gradual decline in Q2, while interest in Cyber Liability grew", *News Release*, 29 July, Council of Insurance Agents & Brokers.

CRO Forum (2014), *Cyber resilience: The cyber risk challenge and the role of insurance*, CRO Forum, Amsterdam, www.thecroforum.org/wp-content/uploads/2014/12/Cyber-Risk-Paper-version-24.pdf.

Cullina, M. (2017), "Evolving cyber concerns create gaps in homeowners' coverage", *Property Casualty 360°*, 11 January, www.propertycasualty360.com/2017/01/11/evolving-cyber-concerns-create-gaps-in-homeowners?.

Deloitte (2017), *Demystifying cyber insurance coverage: Clearing obstacles in a problematic but promising growth market*, Deloitte University Press.

Department for Culture, Media and Sport (2017), *Cyber Security Breaches Survey 2017*, Department for Culture, Media and Sport, London.

Department for Culture, Media and Sport (2016), *Cyber Security Breaches Survey 2016*, Department for Culture, Media and Sport, London.

Edwards et al. (2014), "Hype and Heavy Tails: A Closer Look at Data Breaches", Workshop on the Economics of Information Security.

ENISA (2012), *Incentives and barriers of the cyber insurance market in Europe*, European Network and Information Security Agency, Heraklion (Greece).

Faulkner, M. (2017), "Swiss Re calls for government cyber backstop ", *Insurance Day*, 2 March.

Fitch Ratings (2017), "Cyber Insurance - Risks and Opportunities", *Fitch Ratings Report*, September, www.fitchratings.com/site/re/903074.

Gartner (2016), *Market growth forecast for public IT cloud services worldwide from 2011 to 2016*, accessed from Statista, www.statista.com/statistics/203578/global-forecast-of-cloud-computing-services-growth/ on 10 November 2016.

Harrington, J. (2017), "Cyber Insurance: Many Choices Now That There Is No Choice", *MyNewMarkets.com*, 27 April, www.mynewmarkets.com/articles/182994/cyber-insurance-many-choices-now-no-choice.

Heartbleed.com (2014), *The Heartbleed Bug (website)*, http://heartbleed.com/, accessed 21 November 2016.

Héon, S. and D. Parsoire (2017), "La couverture du cyber-risque", *Revue trimestriellle de l'association d'économie financière*, No. 126 (2e trimestre), pp. 169-182.

Howard, L.S. (2017), "Hackers Will Become More Cunning in 2017 as Cyber Risks Intensify: Report", *Carrier Management*, 11 January, www.carriermanagement.com/news/2017/01/11/162963.htm.

Insurance Europe (2012), *Insurance Europe key points for insurers regarding natural catastrophes in Europe*, Insurance Europe, 27 November.

Insurance Information Institute (2015), *Cyber risk: threat and opportunity*, Insurance Information Institute, New York.

JLT Re (2017), *Unlocking the potential of the cyber market: JLT Re Viewpoint*, JLT Re, London.

JLT Re (2016), *Renewal Retrospective: In the balance*, JLT Re, London.

Lloyd's (2016), *Facing the cyber risk challenge: A report by Lloyd's*, Lloyd's, London.

Lloyd's (2015), *Business Blackout: The insurance implications of a cyber attack on the US power grid*, Lloyd's, London.

Lloyd's and Cyence (2017), *Counting the cost: Cyber exposure decoded*, Lloyd's, London.

Marsh (2016a), *Continental European Cyber Risk Survey: 2016 Report*, Marsh LLC, October.

Marsh (2016b), *UK Cyber Risk Survey Report: 2016*, Marsh LLC, September.

Mitchell, S. (2015), "Lloyd's Calling For Government Cyber Backstops", *Cyber Roundup by the Council*, Council of Insurance Agents & Brokers, 16 July, https://cyber.ciab.com/2015/07/16/lloyds-calling-for-government-cyber-backstops/, accessed 10 November 2016.

Moynihan, S. (2017), "Cyber (in)security: Can insurance solutions keep pace with threats?", *PropertyCasualty360°*, 18 January, www.propertycasualty360.com/2017/01/18/cyber-insecurity-can-insurance-solutions-keep-pace.

NetDiligence (2016), *2016 Cyber Claims Study*, NetDiligence.

OECD (2017), "Gross claims payments", *OECD Insurance Statistics (database)*, http://stats.oecd.org/Index.aspx?DatasetCode=INSIND, accessed 19 May 2017.

Parsoire, D. (2014), "Cyberassurance: offres et solutions", *Risques: Les cahiers de l'assurance*, No. 101, pp. 61-65, Paris, http://revue-risques.fr/revue/PDF/revue-risques-101.pdf.

Ponemon Institute (2017), *2017 Global Cyber Risk Transfer Comparison Report*, Ponemon Institute LLC, Traverse City (Michigan).

Ponemon Institute (2017), *2017 Cost of Data Breach Study: Global Analysis*, Ponemon Institute LLC, Traverse City (Michigan).

Prudential Regulation Authority (2016), *Cyber insurance underwriting risk: Consultation Paper CP39/16 (November)*, Bank of England, London, www.bankofengland.co.uk/pra/Documents/publications/cp/2016/cp3916.pdf.

PwC (2016a), *Global Economic Crime Survey 2016 - Adjusting the Lens on Economic Crime: Preparation brings opportunity back into focus*, PwC. www.pwc.com/gx/en/services/advisory/consulting/forensics/economic-crime-survey/data-explorer1.html.

PwC (2016b), *Moving forward with cybersecurity and privacy: Key findings from The Global State of Information Security® Survey 2017*, PwC.

Reeve, T. (2015), "Cyber insurance not trusted by business, KPMG claims", SC Magazine UK, 1 May, www.scmagazineuk.com/cyber-insurance-not-trusted-by-business-kpmg-claims/article/412535/.

Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies (2017), *2017 Cyber Risk Landscape*, Risk Management Solutions, Inc. and Centre for Risk Studies, Cambridge University.

Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies (2016), *Managing Cyber Insurance Accumulation Risk*, Risk Management Solutions, Inc. and Centre for Risk Studies, Cambridge University, http://cambridgeriskframework.com/getdocument/39.

Schwarze, R. and G. Wagner (2007), "The Political Economy of Natural Disaster Insurance: Lessons from the Failure of a Proposed Compulsory Insurance Scheme in Germany", *European Environment*, Vol. 17, pp. 403–415.

S&P Global Market Intelligence (2015), *Looking Before They Leap: U.S. Insurers Dip Their Toes In The Cyber-Risk Pool*, Standard & Poor's, www.globalcreditportal.com/ratingsdirect/renderArticle.do?articleId=1403078&SctArtId=320678&from=CM&nsl_code=LIME&sourceObjectId=9194506&sourceRevId=12&fee_ind=N&exp_date=20250609-19:35:11.

Spiceworks (2015), *Diving into IT Cloud Services*, accessed from Statista, www.statista.com/statistics/541975/north-america-emea-cloud-based-it-services-usage-current-and-planned/ on 10 November 2016.

Statista (2016), *Total size of the public cloud computing market from 2008 to 2020 (in billion U.S. dollars)*, Statista, www.statista.com/statistics/510350/worldwide-public-cloud-computing/, accessed 10 November 2016.

Swiss Re (2016a), *Cyber: in search of resilience in an interconnected world*, Swiss Re, Zurich.

Swiss Re (2016b), *Global insurance review 2016 and outlook 2017/18*, Swiss Re, Zurich.

The Geneva Association (2016), *Ten Key Questions on Cyber Risk and Cyber Risk Insurance*, The Geneva Association, Zurich.

Trend Micro (2017), "Operation Cloud Hopper: What You Need to Know", *Tend Micro Cyber Attacks*, 10 April, www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-cloud-hopper-what-you-need-to-know, accessed 13 April 2017.

Tsangaris, H. (2016), "4 tips to sell more cyber liability policies to small businesses", *Property Casualty 360°*, 4 November, www.propertycasualty360.com/2016/11/04/4-tips-to-sell-more-cyber-liability-policies-to-sm.

US Department of the Treasury (2016), "Guidance Concerning Stand-Alone Cyber Liability Insurance Policies Under the Terrorism Risk Insurance Program", *Federal Register*, Vol. 81, No. 248 (27 December), https://www.gpo.gov/fdsys/pkg/FR-2016-12-27/pdf/2016-31244.pdf.

White, L. (2016), "British Banks Underplay Cyber Attacks, Fearing Bad Publicity or Punishment", *Carrier Management*, 26 October, www.carriermanagement.com/news/2016/10/16/159980.htm.

Yoder, J. and J. Nocera (2016), "8 ways to improve cyber insurance", *Property Casualty 360°*, 30 November, www.propertycasualty360.com/2016/11/30/8-ways-to-improve-cyber-insurance.

Young, D. et al. (2016), "A framework for incorporating insurance in critical infrastructure cyber risk strategies", *International Journal of Critical Infrastructure Protection*.

Z/Yen Group (2015), *Promoting UK Cyber Prosperity: Public-Private Cyber-Catastrophe Reinsurance*, Long Finance.