Chapter 3

The cyber insurance market

This chapter provides an overview of the cyber insurance market, including the types of losses that are commonly covered across stand-alone cyber insurance policies and traditional policies and also the losses that are more difficult to cover. It provides some data on the size of the stand-alone cyber insurance market, penetration levels and pricing, as well as information on how insurers underwrite cyber insurance coverage approach and the additional risk mitigation and crisis response services that are often offered with cyber insurance policies.

Coverage for losses and damages resulting from cyber incidents may be provided as stand-alone coverage for certain cyber risks or as a specific endorsement (either on a primary or difference-in-conditions basis) on existing policies (e.g. errors and omissions/professional indemnity, general liability, property or others). Such coverage might also be included in other coverages (without a specific endorsement) either unintentionally (such as in the case of a court-imposed legal interpretation of policy language) or intentionally (where insurance companies themselves interpret their policy language as including coverage for some cyber security related losses). In general, cyber insurance buyers are commercial entities, although some coverage for cyber risks faced by individuals is starting to emerge (see Box 3.2).

While the market for cyber insurance is generally perceived as being in its infancy, specific cyber insurance products have been available for nearly 20 years in some countries, particularly in the United States. The initial focus of the cyber insurance market was on providing errors and omissions coverage for companies providing technology-based services (Fitch Ratings, 2017; Bolot and Lelarge, 2008). The increasing occurrence of cyber incidents and, in particular, the establishment of privacy breach notification requirements and penalties (beginning in 2003 in the US state of California) resulted in new exposures to first party losses (such as incident response costs) and third party liability claims that insurers had not considered when underwriting property and liability coverage. As a result, a number of exclusions have been developed and written into traditional insurance policies - leading to the development of stand-alone cyber insurance products to address risks excluded from traditional policies (see Box 3.1).
Box 3.1. Common cyber-related exclusions to traditional policies

Cyber incidents have emerged as potential sources of damage, theft and liability that were not previously considered in the underwriting of property, crime, kidnap and ransom, liability and other traditional policies. For some types of policies (e.g. named peril property insurance policies), cyber-related losses would normally be excluded unless a cyber incident leads to a named peril such as fire. In other traditional business lines (including all-risk policies and specialty lines), the scope of any coverage for cyber risk may be defined by the use of specific exclusions (although there is limited information on how frequently these exclusions are applied). There are three main types of general exclusions (in addition to individual loss types that may be excluded from individual policies):

- **General exclusion for all losses resulting from a cyber attack**: The Institute Cyber Attack Exclusion Clause CL380 is the broadest exclusion clause, stating that "in no case shall this insurance cover loss damage liability or expense directly or indirectly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system".1 This exclusion is sometimes - but not consistently - used in property policies, as well as in sectorial specialty line policies (e.g. marine, energy) (Quy, 2014) and appears to provide an exclusion from coverage for all of the main types of losses normally generated by a malicious cyber attack.2 Another means of excluding certain types of incidents is found in the NMA Information Technology Hazards Clarification Clause and Electronic Data Endorsements 2912. The NMA 2912 exclusion ("endorsement") clarifies that the loss, alteration, damage or reduction in functionality of a computer system, hardware, or software is not considered an insured event (unless it arose from another covered peril (e.g. fire)).

- **General exclusion for losses related to specific types of incidents (i.e. data breach)**: Beginning in 2014, the Insurance Services Office (ISO), which provides standardised forms for insurance policies in the US market, has included the "Exclusion - Access Or Disclosure Of Confidential Or Personal Information And Data-Related Liability - Limited Bodily Injury Exception Not Included" in its standard commercial general liability policy forms (these policies, and specifically coverage for "Personal and Advertising Injury Liability", have often been the basis for claims in litigation involving victims of past data breaches). This exclusion states that the insurance will not apply in the case of "Access Or Disclosure Of Confidential Or Personal Information And Data-related Liability" and will not cover "damages arising out of: (1) Any access to or disclosure of any person’s or organization’s confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any other type of nonpublic information; or (2) The loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data." It further sets out a list of commonly incurred costs related to third party data confidentiality breaches (such as notification expenses, credit monitoring, forensic investigation, etc.) that will not be covered when this exclusion is included (Anderson, 2013a; Aschkenasy, 2013). Liability resulting from bodily injury and property damage, while not specifically listed, might also be excluded based on the second clause (and title) of the ISO exclusion (Watkins, n.d.).

- **General exclusions for specific types of losses (i.e. data and software loss)**: There are also general exclusions used to exclude the costs of reinstating damaged, altered or lost data (i.e. data and software loss) such as the NMA Information Technology Hazards Clarification Clause and Electronic Data Endorsements 2914 and 2915 and ISO's Electronic Data Exclusion. The NMA exclusions exclude coverage for loss, damage, destruction, erasure, corruption or alteration of electronic data from any cause whatsoever. The ISO Electronic Data Exclusion limits the definition of property damage to damage to tangible property where electronic data is not included within the definition of tangible property (Malecki, 2004; Aon, 2013). The robustness of electronic data exclusions have been tested in litigation in the United States - although judgments have been made both supporting and invalidating the exclusions depending on the circumstances of the given event (Anderson, 2013c).
Box 3.1. Common cyber-related exclusions to traditional policies (cont.)

In addition, many traditional policies include an exclusion for loss or damage caused by acts of war or terrorism. For example, since 2002 in the United States, standard ISO exclusions have been applied to property and general liability policies that preclude coverage for damages and losses above a certain threshold resulting from acts of terrorism (Woodward, 2002). As a result, damages and losses resulting from cyber terrorism events that meet the definition of acts of terrorism in property and liability policies (as well as any thresholds) could be excluded from coverage.

Responses to the OECD questionnaire provided some anecdotal insight into the use of these general exclusions in various countries:

- Property policies: Respondents from the United States, United Kingdom, Australia and New Zealand indicated that physical asset damage and business interruption losses caused by cyber attack and data and software losses were often excluded from property policies (suggesting use of named peril policies, the general CL 380 or NMA exclusions as well as the NMA or ISO electronic data exclusions). In Australia, standard industrial special risks policies (known as “Mark IV and Mark V”) for large businesses exclude property damage resulting from unauthorised access to the insured’s computer system (Australian Reinsurance Pool Corporation, 2016). Respondents from continental Europe also indicated that data and software losses and losses other than those caused by physical peril were excluded but that business interruption without material damage may not be excluded. That said, commercial property policies for large industrial risks are rarely standardised and therefore cyber incidents may be treated differently across large commercial policies (Lathrop, 2016). In addition, there are reports that a number of insurance companies have begun eliminating these exclusions from large commercial property policies (i.e. covering cyber risks in large commercial property policies). Finally, the CL 380 exclusion only applies to malicious cyber attacks so some property policies may provide coverage for damage to property (and potentially business interruption) resulting from unintentional information technology failures - unless the policy was written on a named perils basis excluding cyber incidents as a peril (i.e. the property only covered specific listed (non-cyber) perils).

- General liability policies: A number of respondents (especially in the United States and Australia) indicated that losses related to third party data confidentiality breaches (incident response costs, breach of privacy compensation, etc.) as well as inadvertent disruption of third party systems (i.e. transmission of malware and the resulting network security failure liability) are excluded from general liability policies suggesting use of the ISO commercial general liability exclusion or the broader CL 380 cyber attack exclusion in many general liability policies. In the UK market, general liability policies excluded these types of losses in some cases although many traditional policies do not include these exclusions. The exclusions are not generally used in continental Europe either as general liability policies with a pure financial loss extension would be expected to cover these types of losses in some cases although in France (and potentially in other European countries) some policies will apply exclusions or other limits on cyber-related losses (Fédération française de l'assurance, 2017).

1. Institute clauses are developed by the “London Market”, comprising Lloyd’s and the International Underwriting Association.

2. Importantly, the CL380 does not exclude loss, damage or liability resulting from an unintentional system malfunction.

3. Pure financial loss coverage can be added to general liability/professional indemnity policies in continental Europe and elsewhere and provides coverage for liability arising out of events where no physical damage or bodily injury has been caused.
Stand-alone cyber insurance market

**Market size and scope**

The size of the stand-alone cyber insurance market in 2016 is estimated to be in the range of USD 2.5 billion to USD 3.5 billion in gross written premiums (which excludes premiums collected for cyber risk coverage included in other policies as companies do not generally provide breakdowns of premiums by individual perils). The US market accounts for an estimated 85% to 90% of all gross written premiums (USD 2.5 billion to USD 3.0 billion) (PwC, 2015; Betterley, 2015; Marsh, 2016b), while the European market is estimated to account for approximately 5% to 9% (USD 150 million to USD 400 million in gross written premiums (Thomas and Finkle, 2014; Marsh, 2016b; Wong, 2017)) - including an estimated EUR 90 million in Germany (Segger and Lorscheid, 2017) and EUR 30 million in France (Thevenin, 2017). Asia-Pacific accounts for approximately USD 50 million in gross written premiums (Wong, 2017).

In many countries, the market is growing at an extremely fast pace with some projecting that it could reach USD 5 billion in the United States (PwC, 2015) and EUR 900 million in Europe (Insurance Information Institute, 2015) by 2018 and USD 20 billion in global premiums by 2025 (Swiss Re, 2017). Based on data from Eling and Wirfs (2016), the global market grew at a compound annual growth rate of almost 25% between 2012 and 2015 and most estimates of the future size of the market predict a similar rate of growth over the next decade (see Figure 3.1). However, it is also possible that the market could grow even quicker. A recent survey by CFC Underwriting, for example, found that more than 40% of respondents had seen growth in their cyber coverage book of more than 50% over 2016 (Hancock, 2017a). There is also substantial room for growth given that the stand-alone cyber insurance market is only a fraction of the size of other markets, despite the high-level of potential exposure to cyber risk (Swiss Re, 2016b). In OECD countries, for example, USD 277 billion in premiums were written for fire and property damage (commercial and residential) and USD 171 billion for general liability insurance in 2015 (OECD, 2017b), relative to the estimated USD 2.5 billion in stand-alone cyber insurance premiums that year.

The level of future demand will depend on the frequency of high-profile cyber incidents as well as the evolving legislative and regulatory environment for privacy protections in many countries. The implementation of the General Data Protection Regulation (GDPR) in the European Union could lead to significant growth in take-up with some reports suggesting that the EU market could eventually equal the size of the US market (Marsh, 2016b).
In the US market, cyber insurance coverage is generally available from approximately 70 insurance companies, which may include coverage available on both a stand-alone basis and through cyber-specific endorsements to traditional policies (Harrington, 2017). That said, over 500 companies responded to the US National Association of Insurance Commissioner's most recent "Cybersecurity Annual Statement Supplement" which collects information on premiums collected - and losses paid - for cyber insurance coverage suggesting that a much larger number of insurance companies are providing coverage for some risks that can be interpreted as "cyber" risks. The US market is dominated by a few large providers, including AIG, Chubb and XL Group which account for approximately 40% of the market (Fitch Ratings, 2017). Travelers Companies, Beazley Insurance, CNA Financial, Liberty Mutual, BCS Insurance, Axis Capital and Zurich American Insurance are also significant providers of coverage. According to one recent estimate, approximately 10 companies collect more than USD 100 million in annual written premiums and approximately 10 others collect USD 25 million to USD 100 million in annual written premiums (Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, 2017).

Lloyd's (2016a) has reported that 63 syndicates are writing cyber insurance coverage (GBP 322 million in gross written premiums in 2015), of which more than 80% is earned for providing coverage to US-domiciled companies. In Germany, there are reportedly 15 insurance companies that offer some form of cyber insurance coverage to German companies (up from 4 in 2014), including many of the same companies offering this coverage in the United States (Allianz, AIG, Chubb, XL Catlin, Zurich) as well as AXA, ARAG, ERGO, HDI, Hiscox, Swiss Re, and Tokio Marine (List, 2015). According to one report, there were 11 insurance companies offering this coverage in France (Parsoire, 2014). Respondents to the OECD questionnaire revealed that insurance companies are providing stand-alone cyber coverage in Australia, Belgium, Canada, Ireland, Israel, New Zealand, and South Africa. Significant stand-alone cyber insurance markets also exist in...
Japan, Singapore and Hong Kong (China) although no responses were received from companies specifically operating in those economies. In India, recent data confidentiality breaches at a number of banks is expected to lead to an increase in companies offering cyber insurance coverage, and also in demand for such coverage (Howard, 2016), with some companies reportedly developing stand-alone products (Advisen, 2017). In mid-2017, two global insurance companies announced a partnership for providing coverage and crisis response services in Brazil (Insurance Journal, 2017i).

**Coverage provided**

The coverage provided by stand-alone cyber insurance policies for commercial entities (coverage for individuals is described in Box 3.2) can vary significantly across providers, prompting one analyst to suggest that "if you have seen one cyber policy, you have seen one cyber policy" (Nordman, 2012). According to one recent (US-based) estimate, there are at least 65 different policy forms in use for the coverage of cyber risk (Laurie and Vitkowsky, 2017). The abundance of policy forms may be partly due to the common practice of offering a menu of possible coverage options across the same categories of potential losses - allowing policyholders to tailor their policy terms based on their particular level of exposure (e.g. companies that do hold significant amounts of personally-identifiable information are able to secure coverage focused on this cyber risk, as well as business interruption or cyber fraud/theft). Despite coverage differences, there is sufficient convergence to allow companies to seek price quotes for a defined coverage need (Aon, 2013).

![Figure 3.2. Loss categories commonly included in stand-alone policies](image)

*Source:* "OECD review" includes: (i) eight policies provided or described in the context of the OECD's survey questionnaire (SHA and Hollard from South Africa; QBE Europe and CFC Underwriting from the United Kingdom; Munich Re (Corporate Solutions) from Germany; General Re from the United States; Zurich Insurance from Switzerland; and Delta Insurance from New Zealand); and (ii) publicly available information on fifteen policies provided by insurance companies, brokers and other related providers (CNA Insurance, QBE North America, AIG, Chubb, ISO, Tokio Marine HCC and XL Catlin from the United States; Tokio Marine Kiln, Marsh, Hiscox and Beazley from the United Kingdom; Hiscox from France; Allianz Global Corporate and Specialty from Germany; and Swiss Re (Corporate Solutions) from Switzerland). "CCRS/RMS review" is from Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies (2016) and includes 26 stand-alone policies. In the case of both the OECD review and the CCRS/RMS review, many (but not all) of the policies are those that are made available on a global basis.
Box 3.2. Cyber coverage for individuals

While the focus of this study is on the commercial market, cyber risks are also an increasing concern for individuals who could face many of the same types of losses as commercial entities. Identity theft insurance, which provides coverage to individuals for expenses, expert assistance as well as credit monitoring services has been available in many countries for several years (approximately 10 years in the United States) (Cullina, 2017). However, the scope of potential losses that individuals could face is quickly expanding:

- Individuals (particularly high- and mid-net worth individuals) are increasingly targeted by ransomware and fraud attempts (Insurance Journal, 2017d) based on both the increasing amounts of personal information freely available online, as well as through attempts to access personal information that is not publicly available - leading to potential financial losses and costs related to investigating unauthorised access and data restoration;
- Individuals can become victims of social media impersonation which could lead to various types of social engineering (such as solicitations to relatives for money (Cullina, 2017)) and potential liability claims (similar to communication and media liability faced by companies);
- Individuals may fall victim to cyber bullying or other online reputational harm, leading to costs (and assistance needs) to respond to harmful statements; and
- Connected home devices could be affected by malware that causes malfunction. A survey of US consumers found that 10% had been affected by cyber attacks on non-computing home systems and smart appliances, often leading most often to malware infection and/or damage to software or operating systems. Among those affected, 87% faced financial losses including 42% that spent between USD 1 000 and USD 5 000 (Insurance Journal, 2017b).

A number of insurers are beginning to respond to these emerging risks to individuals:

- In Europe, some companies are beginning to offer insurance coverage for e-reputation which provides coverage for identity theft as well as reputational harm resulting from content that is posted online. One company is also considering an insurance coverage for data recovery (which can also be endorsed in some residential property policies).
- In the United States, identity theft insurance is being expanded by some companies to also include coverage for extortion, online fraud and cyber bullying (Carrier Management, 2016a; Insurance Information Institute, 2014; Insurance Journal, 2016a). Insurers are also starting to develop coverage for expenses resulting from cyber attacks on computers and connected devices as well as cyber extortion (Insurance Journal, 2017b). Similar to the commercial market (see section below on “additional services”), a number of insurers are also offering risk mitigation services (Simpson, 2017).
- In the United Kingdom, coverage for cyber bullying is available from some London underwriters and an insurance company while at least one broker and one Lloyd's syndicate are offering coverage for cyber extortion, fraud and social media reputation harm focused on high-net worth individuals.
- In South Africa, at least one insurer is providing liability, extortion and identity theft coverage for individuals.

There is limited information on the penetration of such coverage although some insurers are offering coverage for cyber risks as an endorsement to existing property or other homeowner policies.

Figure 3.2 provides an overview of coverage for different categories of cyber-related losses included in stand-alone policies. The overview is based on responses to the OECD questionnaire as well as an OECD review of selected publicly-available descriptions of
policies from major providers (total of 23 providers based in 7 countries, although often the policies offered are available on a global basis). For comparison, it also shows the results of a similar exercise undertaken by Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies (2016) of 26 stand-alone policies.

In general, the stand-alone cyber insurance policies provide coverage, either on a standard-basis or as an optional add-on, for most of the main types of losses that could result from the following types of incidents:

- **Data confidentiality breaches:** The incident response costs, regulatory and legal defence costs, breach of privacy compensation and, to a lesser extent, fines and penalties that may result from a third party confidentiality breach (often termed a "data breach" or "privacy breach"), are usually covered in stand-alone cyber insurance policies. Most policies were designed with a focus on breaches involving personal data, although many also cover losses related to breaches of third party corporate data (such as the trade secrets of a third party corporate).

  Some policies will not cover fines and penalties or will only provide such coverage where permissible by law. This is becoming a more significant issue in the context of the implementation of the GDPR in the European Union which could involve significant fines that may be uninsurable and/or far above the amounts currently provided in cyber insurance policies (Fitch Ratings, 2017; Reactions, 2017). There are also varying levels of coverage for contractual penalties, such as the assessments that could be imposed by payment card networks to recover costs related to card replacement and fraudulent transactions. According to some reports, these Payment Card Industry (PCI) assessments are not normally included in stand-alone cyber insurance coverage despite accounting for a significant component of the cost of responding to a data confidentiality breach involving payment card data (Johnson, 2016). Just over 40% of the policies reviewed provided coverage for PCI assessments (often as an add-on to standard coverage).

- **System malfunctions:** The business interruption losses that might result from a denial-of-service attack (and other system malfunctions) as well as the liability that may be established as a result of an inadvertent disruption to a third-party system (e.g. malware transmission - often referred to as "network security failure [liability]") are usually covered in stand-alone cyber insurance policies. Some reports suggest that the business interruption coverage provided in stand-alone cyber insurance policies is less robust than coverage provided in property policies (e.g. more limited scope of coverage, lower limits or no coverage for extra expense) (Johnson, 2016). Among the policies reviewed, just under 60% provided explicit coverage for extra expense (i.e. the additional cost of doing business) which is normally included in property policy coverage for business interruption. Stand-alone policies are also increasingly covering accidental system malfunctions although at least two of the policies reviewed were limited to malicious cyber attacks.

- **Data integrity/availability:** The data and software losses resulting from the deletion or corruption of data as well as the cyber ransom and extortion losses involved in responding to the encryption of data by ransomware are generally covered.
In the case of cyber ransom and extortion, there is some variation in the types of losses covered (e.g. one major provider will only cover costs related to efforts to avoid paying a ransom, not the payment of a ransom itself) as well as whether the coverage includes both incidents and threats of incidents (i.e. whether a ransom payment would be also covered in the context of a threat of harm such as a data confidentiality breach). One impediment to providing insurance coverage for ransom payments is the difficulty in attributing the source of the ransomware and the possibility that the ransom payments could be made to a named terrorist organisation (the International Association of Insurance Supervisors has noted that compensation for ransom payments made to a named terrorist organisation could be considered a violation of United Nations sanctions). Insurance companies may also choose not to provide such coverage in order to be consistent with government policies that are explicitly opposed to making ransom payments in response to kidnapping/extortion.

Malicious activity: The communication and media [liability] that could result from the misuse of a system for defamatory purposes (often referred to as "media liability") is also usually covered in stand-alone cyber insurance policies.

However, certain categories of losses that could result from various incident types are less consistently (or even rarely) covered by stand-alone cyber insurance policies:

- **Data confidentiality breaches**: Coverage for breach of the confidentiality of own data (such as trade secrets) was provided in very few of the policies reviewed by the OECD (less than 5%).
- **Intellectual property theft** is challenging to insure given the difficulties related to valuing lost opportunity (Freedman, 2014; Insurance Journal, 2017). For example, the theft of a design for a new product or the pirating of a film before its release would very likely cause significant harm to the owners of that intellectual property in terms of lost future revenue although the amount of that loss is extremely difficult to estimate. In the OECD review of policies, only one policy explicitly provided coverage for losses of own intellectual property theft (as an optional add-on to its "standard" coverage). As noted above, the theft of a third party's intellectual property, by contrast, is more commonly insurable and is covered by many of the stand-alone cyber insurance policies reviewed, as the value of any stolen intellectual property would be determined by the value of the claim against the insured (once proven).

Data confidentiality breaches (and other types of incidents) can also lead to reputational damage. A number of stand-alone cyber insurance policies will cover costs aimed at minimising reputational harm (e.g. by covering the cost of engaging a public relations firm) although only a small minority will provide any coverage for lost business resulting from longer term reputational damage (i.e. beyond the period of disruption). It should be noted that the lack of coverage for lost business related to reputational harm is not exclusively an issue for cyber incidents - such coverage is not generally available for other perils either (Freedman, 2014). However, the risk may be more significant in the case of cyber incidents (particularly data confidentiality breaches involving personal information) which have often had negative reputational impacts on those impacted (although, as noted in Chapter 2, these impacts may be declining as acceptance of data breaches increases). Some companies are responding to this gap in coverage by developing specific coverage for loss of revenue with limits of up to USD 100 million (Aon, 2013). Three of the policies reviewed by the
OECD included specific coverage (standard or add-on) for lost profits due to brand or reputational damage.\footnote{5}

- **System malfunctions**: Given the general focus of stand-alone cyber policies on addressing losses from data confidentiality breaches (and extortion), physical asset damage resulting from cyber incidents has not normally been included in stand-alone policies. This is beginning to change however. In 2013, a Lloyd's syndicate began offering coverage for physical damage (including for data restoration) and business interruption losses resulting from a cyber attack to supervisory control and data acquisition (SCADA) control systems (i.e. systems that monitor and control processes, commonly used in the electricity and other utility sectors) (JLT Mining, 2014). Another Lloyd's Managing General Agent has begun providing specific coverage tailored towards cyber risks to industrial systems and operational technologies with the potential to cause physical damage (Cohn and Saul, 2017). One company began offering up to USD 100 million in coverage for property damage caused by cyber attack in 2014 (on a primary, excess or difference-in-conditions basis) with other insurers also indicating an interest in providing such coverage (Basak, 2015). In the OECD review of policies, only three of the policies examined offered coverage for physical asset damage. Similarly, few stand-alone cyber insurance policies provide coverage for bodily injury resulting from a cyber incident. The OECD review identified two policies that offer such coverage while the CCRS/RMS review identified approximately four providers with one company reportedly offering up to USD 100 million in coverage for bodily injury (Basak, 2015).

Business interruption resulting from the disruption of a third party digital service provider (i.e. contingent business interruption in a cyber context) is covered by one third of the policies examined by CCRS/RMS. The OECD questionnaire did not seek specific information on this category of losses although the review of policy documents identified only one that provided coverage for this type of loss and only in the case of a cloud service provider disruption. The inclusion of sub-limits on contingent business interruption coverage is also common. In the cloud service failure scenario developed by Lloyd's and Cyence (2017) (see Box 4.1), sub-limits ranging from 20% of annual revenues for small companies to 50% for large companies were used to reflect this market practice.

- **Malicious activity**: Less than half of the policies reviewed by the OECD (and less than a quarter of the policies reviewed by CCRS/RMS) provided coverage for financial theft and fraud. The low level of coverage may be because many traditional crime policies provide coverage for financial theft without any exclusion of cyber-related incidents (therefore limiting the need for coverage in stand-alone cyber insurance policies) (ABI, 2016). Some stand-alone cyber policies that do provide coverage for financial theft and fraud have developed coverage specifically for social engineering fraud (i.e. theft resulting from the impersonation of a responsible executive within an organisation with instructions to transfer funds or provide access credentials) (Ydstie, 2015) as there may be exceptions to coverage of this type of fraud under traditional crime policies limited to unintentional acts (as a transfer of funds, even where initiated under false pretences, still involves an intentional act by an employee - which has led to numerous claims disputes).\footnote{6} At least one major broker has also developed specific coverage to bridge the gap between crime/fidelity and stand-alone cyber policies.
Stand-alone cyber insurance policies also make varying use of the terrorism exclusion that is normally included in other types of commercial policies (although all policies continue to include a war exclusion). Some of the policies reviewed by the OECD were silent on the coverage of terrorism (i.e. did not specifically exclude (or include) terrorist acts as an insured peril). In two policies, a specific terrorism exclusion was included in the policy although cyber terrorism was carved-out of that exclusion. In one policy, affirmative coverage is provided for business interruption resulting from an act of terrorism. According to Allianz Global Corporate and Specialty (2016), the insurance industry has been eliminating terrorism exclusions from cyber insurance coverage in recognition of the challenges of attributing individual cyber incidents. This has potential implications for the coverage provided by terrorism insurance programmes established in a number of countries (see Box 4.2).

These findings are consistent with other analyses of the coverage provided by the stand-alone cyber insurance market (Aon, 2013; Cyber Risk Insurance Forum, n.d.; IRT System X, 2016; ENISA, 2016) and also confirm that stand-alone cyber coverage is responding to many of the gaps in coverage that have emerged in traditional policies (damage to intangible assets, business interruption without material damage, etc.). It should be noted that no significant divergence in the coverage offered by stand-alone policies across different regions was observed which may be because many policies are offered on a global basis.

Penetration of stand-alone cyber insurance

Estimates of the penetration of stand-alone cyber insurance coverage vary widely. Most estimates are based on responses to surveys of what can be very different business communities. These surveys also formulate questions in a way that could lead to disparate responses. For example, a survey might specifically ask about the take-up of stand-alone cyber insurance coverage or, more generally, might ask whether the company has insurance coverage for cyber risks - which could lead to very different estimates of the share of companies that have actually purchased stand-alone cyber insurance policies or endorsements.

Estimates of cyber insurance penetration rates across countries generally find higher levels of penetration in the United States than in the United Kingdom, continental Europe or Asia-Pacific (no information on penetration levels outside of these countries was found):

- In the United States, some estimates suggest that approximately 20% to 35% of all companies have specific cyber insurance coverage (PwC, 2015, S&P Global Market Intelligence, 2015; Council of Insurance Agents & Brokers, 2017) although other more recent reports have found higher penetration levels, from 55% (Hiscox, 2017) to 65% (up from 35% in 2011) (Advisen, 2016). According to one estimate, approximately 72% of companies with coverage for cyber risks purchase stand-alone coverage (up from 64% in 2015) while 28% rely on coverage in existing policies (including through endorsements) (Council of Insurance Agents & Brokers, 2015a and 2017).
In the United Kingdom, estimates of penetration range from less than 2% (Z/Yen Group, 2015) to 20.6% (Marsh, 2016c) to 36% (Hiscox, 2017) to 38% of companies (Department for Culture, Media and Sport, 2017).

According to Marsh (2016b), 24% of organisations in continental Europe had purchased, or were in the process of applying for, cyber insurance coverage in 2016 (up from 20% in 2015). Hiscox (2017) found a penetration level of 30% among German companies in its survey. A recent estimate suggested that penetration among the largest companies in France was close to 60% to 70%, falling to 40% among mid-to-large companies and 2% to 3% among SMEs (Thevinin, 2017).

There are fewer estimates about the level of penetration of cyber insurance coverage in Asia-Pacific although Chubb has suggested that it is below 1% (Wong, 2017).

Penetration is reportedly higher among health, education, retail and technology companies (approaching 50% (PwC, 2015; Insurance Information Institute, 2015) or even 80% in the US retail healthcare and financial services sectors according to some surveys (Council of Insurance Agents and Brokers, 2016b; Advisen, 2016)). A global insurance broker, Marsh, publishes take-up rates for stand-alone cyber insurance and growth in take-up rates by sector among its brokerage clients (with a concentration of US companies). According to its estimates, take-up rates are highest in the healthcare, education and hospitality and gaming sectors (see Figure 3.3). The increasing availability of coverage for business interruption and other first party costs is driving increasing demand in sectors less concerned with third party (personal) data confidentiality breaches. For example, there are some reports that cyber insurance purchasing by manufacturing firms almost doubled between 2015 and 2016 (Insurance Journal, 2017a).

Some of the insurance companies and brokers that responded to the OECD questionnaire provided details on the types of companies that have purchased cyber insurance coverage. In the United States, respondents noted demand from all sectors of the economy although with some variation in terms of the type of coverage being sought (i.e. those holding significant amounts of personally-identifiable information were most concerned with coverage related to a third party data confidentiality breach whereas sectors such as manufacturing were more concerned with business interruption, intellectual property theft and extortion and fraud coverage). Among respondents from the United Kingdom, policyholders were generally concentrated in the retail, healthcare, and financial services sectors, although companies in other sectors also purchase cyber insurance coverage. Larger companies account for a larger share of all policyholders among respondents from continental Europe, in many of the same sectors identified in other countries/regions (with the addition of the communications, media, technology and hospitality sectors). For respondents from other countries (Australia, Canada, New Zealand and South Africa), the distribution of policyholders was also concentrated in retail, healthcare, technology and financial services as well as among professional services companies (such as law firms) which could be targeted for information on strategies or acquisition plans of their larger clients.
Figure 3.3. Estimated stand-alone cyber insurance take-up rates by sector (Marsh clients)

![Graph showing estimated take-up rates by sector from 2013 to 2015.]

Source: Marsh (2015b) reported take-up rates in 2013 and 2014 among its clients. Marsh (2016a) only reported growth in take-up among its clients so the estimated take-up rate in 2015 is derived from reported growth rates.

Most surveys have found a much lower level of coverage among SMEs - for example, a survey of US small businesses (10 or fewer employees) in April 2015 found that only 5% had cyber insurance coverage (Endurance International Group, 2015). There is some evidence that coverage levels among SMEs are increasing. The recent Advisen (2016) survey, for example, also found a high-level of penetration among smaller firms. In the United Kingdom, one study found that the penetration of cyber insurance among SMEs had increased from 2.1% in 2014 to 13.7% in 2016 (Hancock, 2017b). In the United States, the penetration rate for cyber insurance among small companies reportedly increased 26 percentage points between 2011 and 2016 (Advisen, 2016). More than 95% of the 22 insurance companies and brokers that provided details on the characteristics of their clients indicated that they have - or are developing - specific products tailored to the needs of smaller businesses (lower limits, less extensive underwriting process). SMEs accounted for 50% or more of policyholders for approximately 60% of the 14 companies that provided breakdowns of their portfolio by size of companies.

**Level of coverage**

The most common level of coverage available from a single insurer for a single policyholder is estimated to be around USD 25 million (Council of Insurance Agents & Brokers, 2015a), although some individual companies and joint ventures are reportedly willing to offer coverage of USD 75 million to USD 100 million to certain individual clients (Finkle, 2015; Insurance Journal, 2017a; Faulkner, 2017).

Among respondents to the OECD questionnaire, four insurance companies indicated that they had capacity to provide coverage of more than USD 25 million while seven indicated a maximum available level of coverage between USD 5 and USD 15 million. For larger companies, coverage towers involving a number of insurers can be constructed with reported limits as high as USD 700 million for most industries and up to USD 500 million for the financial services, retail and healthcare sectors (Marsh, 2014). In 2017, a USD 600 million tower for stand-alone coverage was reportedly developed with the involvement of 40 cyber underwriters (Hemenway, 2017). Coverage limits do not
vary significantly across regions as limits of up to EUR 500 million have been reported as possible, for example, in Germany and Austria (List, 2015). A major broker has also launched a product aimed at providing GBP 500 million in cyber insurance coverage to mid- to large-sized companies outside the United States (Insurance Journal, 2017c).

The average coverage limit purchased in 2016 among Marsh (mostly US-based) clients was USD 16.9 million, up from USD 11.3 million in 2013. This is much higher than the average coverage limit of USD 6 million reported by the Council of Insurance Agents and Brokers (which has doubled since October 2016) (2016a, 2016b, 2017) and the GBP 1 million to GBP 5 million in coverage limits that have been commonly purchased in the United Kingdom (as reported in 2012) (Airmic, 2012). In France, most companies seek limits of USD 25 million or less while SMEs will normally purchase EUR 150 000 to EUR 200 000 in coverage. In Europe more generally, a survey of risk managers found that 25% of responding companies purchased less than EUR 50 million in cyber insurance coverage, 7% purchased between EUR 50 million and EUR 100 million in coverage and 5% purchased more than EUR 100 million in coverage (FERMA, 2016).

On average, most companies are not purchasing limits near the reported maximum coverage levels available although large companies in some sectors are purchasing more than what is normally available from a single insurer for a single client. Among Marsh clients, coverage limits purchased have been generally increasing annually although with some signs of recent stabilisation among large companies in those sectors that have been purchasing the highest limits (communications/media technology and financial institutions) (see Figure 3.4). The Council of Insurance Agents and Brokers survey (2016b) of US brokers also found that US companies were generally increasing their coverage limits (and that the share of companies increasing their levels of coverage accelerated in the second half of 2016). Despite the growth in the amount of coverage purchased, limits remain well-below comparable policies covering property risks. For example, a typical US company with revenues over USD 5 billion would normally purchase over USD 500 million in property coverage (Lathrop, 2016).

Most reports on the adequacy of coverage limits (focused on the US market) have found sufficient capacity for smaller companies that typically purchase about USD 25 000 in coverage (S&P Global Market Intelligence, 2015), particularly in sectors that have been generally less targeted by cyber attacks. However, companies in high-risk sectors such as health care, education (and to a lesser extent, retail, financial services, technology and hospitality) have reportedly faced capacity constraints as a result of reduced offers of coverage and the exit of some providers in the aftermath of large data confidentiality breaches (Betterley, 2015; Council of Insurance Agents & Brokers, 2016a; Council of Insurance Agents & Brokers, 2016b; Council of Insurance Agents & Brokers, 2017; Sclafane, 2015). PwC (2015) suggests that most large companies have difficulty securing anything above USD 300 million in coverage. According to a recent survey of companies worldwide, 16% indicated that they had purchased the maximum amount of coverage available on the market (Ponemon Institute, 2017).

Some insurers are also placing sub-limits on component parts of the policy coverage and/or imposing deductibles. Among OECD questionnaire respondents, full limits were generally offered for each sub component. Typical reported deductibles in the US market range from USD 5 000 to USD 100 000 for smaller companies and USD 250 000 to USD 10 million for larger companies (Aon, 2013) (although Anthem Insurance reportedly faced a USD 25 million deductible on USD 100 million in insurance coverage...
after being impacted by a major data confidentiality breach in 2015 (Finkle, 2015)). OECD questionnaire respondents reported similar ranges for deductibles although some companies offer deductibles below USD 1 000. Most respondents indicated that they would vary deductibles with the level of risk while many insureds also seek higher deductibles in order to reduce the cost of insurance (Sclafane, 2015). Business interruption coverage usually includes a minimum outage time deductible of between 8- to-12 hours (with a shift towards lower time deductibles) although some respondents to the survey offered coverage from 6 hours onwards while others offered coverage only after 24 hours or longer (some business interruption coverage is offered without a time deductible, replaced with a higher value deductible in its place). A survey of cyber insurance policies in Sweden found a wide variety of time deductibles imposed, including a 2-hour deductible provided by one insurer on a negotiated basis (Franke, 2017).

**Figure 3.4. Cyber insurance limits purchased by large and all companies (Marsh clients)**

<table>
<thead>
<tr>
<th>Average limits purchased by large companies (over USD 1 billion in revenues)</th>
<th>Average limits purchased by all companies</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012</td>
<td>2013</td>
</tr>
</tbody>
</table>

Source: Marsh (2014, 2015b, 2016a)

**Pricing**

A limited amount of information is available on the cost of cyber insurance coverage in different countries and sectors, and for companies of different sizes:

- A 2013 report by Aon indicated that, in the United States, the price of USD 1 million in coverage ranged from USD 5 000 to USD 10 000 for smaller firms to USD 10 000 to USD 50 000 for large firms with an average cost of about USD 10 000 to USD 25 000 per USD 1 million in coverage (Thomas and Finkle, 2014). One brokerage firm that responded to the OECD questionnaire indicated
that prices are now significantly lower for smaller US firms, with premiums starting below USD 1,000 for USD 1 million in coverage. This is consistent with another recent estimate of premiums of USD 5,000 to USD 7,000 for a "comprehensive policy" to meet the needs of companies with USD 5 million to USD 8 million in revenues (Tsangaris, 2016). One company offered a USD 100,000 estimate of the cost of USD 10 million in coverage for energy companies against data breach incidents (and up to USD 700,000 for USD 10 million in coverage that includes physical damage) (Saul and Cohn, 2017).

- A 2012 report by Airmic (a group representing risk managers, usually from larger firms) estimated the price of GBP 1 million in coverage in the United Kingdom to be GBP 30,000 while GBP 10 million in coverage would normally be priced at GBP 15,000 per million (or GBP 150,000 in total for GBP 10 million in coverage).

- In Europe, the cost per EUR 1 million in coverage is approximately EUR 2,000 to EUR 5,000 for EUR 50 million to EUR 90 million in coverage (Thomas and Finkle, 2014). In Germany, the reported cost of EUR 1 million in coverage ranges from EUR 7,000 to EUR 15,000 while the cost of EUR 5 million in coverage ranges from EUR 4,000 to EUR 24,000 per million (List, 2015). The survey of policies offered in Sweden found a cost ranging from SEK 5,000 to SEK 15,000 per SEK 1 million in coverage although with some coverage available for less than SEK 5,000 per SEK 1 million (Franke, 2017).

The cost of cyber insurance coverage is expensive relative to other types of insurance coverage - it has been reported that cyber insurance coverage (for the same amount of coverage) is three times more expensive than general liability coverage (PwC, 2015) and six times more expensive than property coverage (Z/Yen Group, 2015). There is also some evidence that the cost of cyber insurance has been increasing more quickly, leading to a widening gap in the cost of cyber insurance relative to commercial property and casualty insurance. The cost per million of cyber liability insurance has increased by over 200% since Q1 2012 relative to a 17% decline in US commercial property and casualty pricing (on a composite basis - see Figure 3.5). However, there are recent signs of a stabilisation in pricing After large increases in 2015, rates stabilised in 2016 and declined in 2017 in the United States for most companies (only 15% of companies surveyed by the Council of Insurance Agents and Brokers (2017) indicated that they had faced price increases in the first quarter of 2017 while 31% saw a decline in rates charged). Pricing for SMEs has generally been more stable as a result of higher levels of competition in that market (Betterley, 2015). Some reports have suggested that pricing for cyber insurance is relatively flat as a result of the limited ability of insurance companies to differentiate across risks (Swiss Re, 2017). However, reports on pricing in the United States indicate some differentiation. For example, in 2015, increased prices for cyber insurance particularly targeted the US health care and retail sectors (ranging from a 10% to 200% increase in the cost of coverage in 2015 (Betterley, 2015)), as a result of major breach experiences and differing values for the personally-identifiable data held by health care and retail companies (i.e. the higher value of health care information and social security numbers) (Marsh, 2015a; Sclafane, 2015; Betterley, 2015).

Several respondents to the OECD questionnaire indicated that they also differentiate premiums based on the level of cyber security. For example, London market respondents indicated that credits or premium discounts are sometimes provided for compliance with
standards, audits, penetration tests as well as staff training initiatives. Broker respondents from other countries also suggested that security factors played an important role in pricing (and that they often helped their clients improve security practices before seeking insurance quotes). In Sweden, many of the insurers providing cyber insurance coverage take security parameters into account and vary premiums accordingly (Franke, 2017). In addition, some retail and healthcare organisations have reportedly been able to avoid premium increases imposed on other organisations in their sector based on better security controls (Willis Towers Watson, 2017).

Figure 3.5. US Commercial and Cyber Insurance Price Indices

![Graph showing US Commercial and Cyber Insurance Price Indices]

Source: OECD calculations based on rate changes reported by Marsh (2017) (2012 Q1=100).

There is also some evidence that uncertainty about the level of exposure could be leading to relatively high levels of variation in pricing (Taylor, 2017). For example, a company in Germany reportedly received quotes for EUR 5 million in coverage that ranged between EUR 20 000 and EUR 120 000 while a pharmaceutical company in the United States was quoted premiums that varied by 300% for a defined set of coverage (Sclafane, 2015).

**Underwriting approach**

The underwriting of insurance coverage is based on an analysis of the probability that covered incidents of different severities might occur (taking into account the level of protection) and the implications in terms of claims payments (taking into account the level of retention). This kind of analysis can provide various estimates that insurance companies use when establishing prices, including average annual loss and probable maximum loss. These kinds of assessments are usually based on historical experience in terms of the frequency and severity of incidents combined with expert judgement and/or scientific evidence that allow for adjustments to be made to account for changes in frequency or severity (such as, for example, a changing climate in the context of natural hazards, or a material development in terms of preventative technology).

The limited availability of data on cyber incidents (and the evolving nature of the risk itself - see Chapter 4) has made it difficult to develop full probabilistic models for use in pricing cyber insurance cover. While a few insurance companies, brokers and other
companies (see Chapter 5) have developed pricing models that provide probabilistic estimates of potential losses, the vast majority of insurers continue to use deterministic or scenario-based approaches for estimating the potential frequency and severity of cyber incidents. Assessments of frequency and severity are usually based on publicly available data on past incidents, enhanced by the underwriter’s own claims experience. There are a few commercial companies that collect and market data on past incidents and at least one annual report that provides an overview of claims experience based on data provided by a number of insurance companies (see Chapter 4).

In the case of data confidentiality breaches, data on past breaches provides insurance companies with a basis to assess the level of risk based on different company characteristics (e.g. size, sector, geographical footprint) and estimate the per record cost of a breach (as noted in Chapter 2, these costs can vary depending on the type of record, the number of records stolen and other factors). Therefore, part of the underwriting process involves understanding the business activities and number and types of information records held by the company. Given the longer experience with data breach notification laws and the more developed stand-alone cyber insurance market, much of the available data is based on experience in the United States.

Insurance companies also focus significant attention on the company’s security practices and policies, depending on company size and amount of coverage being sought. For smaller companies/coverage amounts, the underwriting process will focus on basic cyber security practices such as use of a firewall, anti-virus/malware software and data encryption, as well as frequency of data backups and use of intrusion detection tools. In some cases, applications may ask about compliance with specific standards, such as the International Organization for Standardization/International Electrotechnical Commission standard on Information Security (ISO/IEC 27001); the US National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity; or the UK Cyber Essentials. Companies that hold payment card information might also be asked about their compliance with the PCI Data Security Standard while US companies with health records might be asked about their compliance with Health Insurance Portability and Accountability Act security requirements. Some stand-alone cyber insurance applications also request information on plans and policies, such as data protection policies, network access policies, internal auditing policies, disaster recovery plans, etc., as well as governance processes in place for those policies (leadership, frequency of update, etc.). Information on outsourcing of information technology and other operational services is also commonly sought as part of the application process. Larger companies (or companies seeking larger limits) would face additional scrutiny, potentially involving on-site interviews, security audits and/or penetration testing. Risk and vulnerability assessments by external security consultants are offered by some companies as an additional service included as part of the insurance policy (see next section).

Insurance companies use the information gathered through the underwriting process to determine premium levels (or whether to provide coverage at all). Some insurers may also establish minimum security standards that must be maintained through the coverage period in order for coverage to be maintained, such as timely patching of vulnerabilities and/or other software updates (although these types of requirements are usually discouraged by brokers and prone to claim disputes). The May 2017 "WannaCry“ ransomware attacks, which capitalised on a vulnerability for which a security patch had been made available (see Box 2.8), may offer a test of the validity and relevance of these types of requirements.
Robust underwriting of cyber insurance coverage can contribute to reducing cyber risk at an aggregate level by disseminating and ensuring compliance with good security practices (similar to the market for large commercial property coverage where insurance companies play a valuable risk consulting role (Betterley, 2015)). A survey of US security professionals in early 2016 found that 91% of companies had to make adjustments to their security practices or policies in order to secure cyber insurance coverage, including implementing and updating policies and processes, acquiring new technical controls and/or implementing a data/information governance programme (Filkins, 2016). However, efforts to gain market share based on lower underwriting standards could undermine this contribution (there are some reports that certain sectors in the United States are being underwritten with very little review (Council of Insurance Agents & Brokers, 2016b)).

There are also significant concerns related to the level of information available to underwriters - which could have implications for the quality of underwriting. Insurers have raised concerns about access to information on security controls while some risk managers are sometimes impeded from providing underwriters (or their security consultants) with the full access they seek due to concerns about providing access to sensitive data (Airmic, 2012).

Additional services provided with stand-alone policies

In addition to providing insurance coverage for the expenses incurred as a result of a cyber incident, many insurance companies provide additional services with their policies, either as risk management advice during the underwriting process, as a means to reduce vulnerability to cyber incidents during the period of coverage or in order to reduce the impact of cyber incidents that occur. The first two types of services are often referred to as pre-breach services or risk mitigation services while the latter type is identified as post-breach or response services. Some insurance companies have developed significant internal expertise and offer these types of services directly, while others have developed networks and/or partnerships with a variety of service providers, often involving some form of discounted pricing for its policyholders (e.g. information technology security consultants, legal firms, public relations firms, etc.) (see Figure 3.6).

As noted in the previous section, some insurance companies provide specific risk assessment services as part of the underwriting process (sometimes even if no insurance coverage is entered into) ranging from online or onsite security assessments to advice on security policies and practices, to vulnerability scans and penetration testing which should benefit both the insurance company and the company's risk management (Insurance Information Institute, 2014; Carrier Management, 2016d). Insurance companies are also offering an assortment of risk mitigation services during the coverage period, including threat and intelligence warnings and detection, access to specialised protection technologies, preparation and testing of contingency plans, helplines or information portals and employee training (Betterley, 2015; Swiss Re, 2017; Wells Fargo Insurance Services, 2016; Insurance Journal, 2017e).

A range of services for managing the impact of a cyber incident are also being offered, including forensic investigative services necessary to identify the source of any breach, legal assistance to help manage legal and regulatory requirements and potential liability, providers of call centre capacity, notification services, credit monitoring and/or identity theft protection to support interaction with affected clients, and public relations companies to minimise the reputational impact of cyber incidents (Betterley, 2015; Swiss Re, 2017; Insurance Journal, 2017e).
According to one survey, 70% of insurers provide (or plan to provide) cyber risk mitigation or response services (Swiss Re, 2016a). Seventeen of the 23 policies reviewed by the OECD advertised access to risk mitigation and/or response services, including (among other services):

1. in-house risk management advice (35%);

2. specific external risk mitigation services such as periodic penetration testing, tabletop exercises, assessments of security practices, or back-up cloud storage (30%); and

3. response service providers including forensic investigators and legal assistance (66%), public relations advisors (60%), call centre providers (30%), credit monitoring services providers (20%), notification services providers (13%) and even data restoration services (7%).

A recent survey found that a large proportion of companies have access to various response services through their insurance provider and that 40% to 50% have access to risk mitigation services (see Figure 3.7).

There is some evidence that companies see value in these additional services (Swiss Re, 2016a). A survey found that a large share of companies use external providers for risk mitigation and response services, particularly for assessments of company practices, access to real-time threat information, training for employees and executives, specialised legal services, call centre services, forensic investigations and credit monitoring services (Advisen, 2016). Some surveys have found that additional service offerings (risk mitigation and response together) are as important as risk transfer in motivating insurance purchase among US SMEs (Council of Insurance Agents & Brokers, 2016c) and are also the most important driver for more than 30% of large US companies (Council of
3. THE CYBER INSURANCE MARKET

Insurance Agents & Brokers, 2017). These services might also have a positive impact in terms of reducing the cost of responding to breaches (by as much as 30% according to one estimate (NetDiligence, 2015)). One report suggested that companies without access to these services could pay as much as three times more for the same service (and without the benefit of knowing that the service provider has been previously vetted by the insurance company) (Donlon, 2015).

Figure 3.7. Companies provided with risk mitigation and response services by their insurer

Source: Ponemon Institute, 2017

Coverage for cyber-related losses in existing (traditional) policies

As noted above, some insurance coverage for losses resulting from cyber incidents may exist in traditional insurance lines, including property, general liability, directors and officers, errors and omissions/professional indemnity, crime and all-risk policies for owners of small businesses (known as "business owner's policies" in the United States or "business pack" policies in Australia) (Simpson, 2016a) (see Figure 3.8) and potentially even in individual homeowner policies (see Box 3.2). The inclusion of this coverage may be explicitly understood by the insurance companies that are providing it (as well as the policyholders) - through the inclusion of a specific endorsement or, potentially, an intentional decision not to apply one of the common exclusions for cyber-related incidents. For example, many insurance companies will specifically provide endorsements of some of the exclusion clauses described in Box 3.1 above. In other cases, cyber losses may be implicitly covered under traditional policies and only "discovered" as a result of claims disputes and/or litigation. The following provides some examples of how cyber-related losses may be explicitly or implicitly covered in traditional policies:

- **Property insurance policies**: As noted above, property insurance policies may exclude losses resulting from a cyber incident through the use of named perils policies or general exclusions covering all cyber attacks (i.e. CL 380) or all events resulting from loss, alteration, damage or reduction in functionality of a computer system, hardware, or software (i.e. NMA 2912). They may also
exclude coverage for damage to intangible assets (ISO Electronic Data Exclusion and NMA 2914 and 2915). At least one insurance company or broker respondent from each of the main markets represented in the responses (United States, United Kingdom, continental Europe, Australia, New Zealand and South Africa) indicated that losses due to business interruption without material damage and data losses were excluded in traditional policies, suggesting some use of named peril policies and/or exclusions in all of these markets.

However, the increasing recognition of the potential for physical asset damage and business interruption to result from cyber incidents and the need for coverage of intangible assets has led some providers to specifically include such coverage in traditional policies. For example, some property policies are offering endorsements based on these exclusions, thereby reinstating coverage that would have otherwise been excluded (according to the Insurance Information Institute (2014), property policies often include these endorsements). Also, if not specifically excluded, it is possible that insurance coverage for cyber-related losses (e.g. property damage, data restoration or business interruption caused by a cyber incident) could be found in all-risk property insurance policies. Traditional policies will usually have larger limits for property damage and business interruption than those available in stand-alone cyber policies which means that coverage (and exposure) for these losses could be higher in traditional policies without exclusions (property policies regularly provide limits of USD 500 million or more which would be an exceptional level of coverage for a stand-alone cyber insurance policy (Marsh & McLennan Companies, 2016)).

- **General liability policies:** A number of different types of liability coverage provided in stand-alone cyber insurance policies could potentially be found (or might still be found) in general liability policies, particularly network security failure liability and communication and media liability. Prior to the use of exclusions (as described in Box 3.1 above), implicit coverage of breach of privacy compensation had been found through litigation in the United States (although not consistently). Physical damage (and bodily injury) caused to a third party are also usually included in general liability policies.

Many general liability policies now exclude claims related to many types of cyber incidents. In the United States, the exclusion is focused on liability resulting from data confidentiality breaches involving third party personal or commercial information although, as noted in Box 3.1, the exclusion may also apply to physical damage and/or bodily injury liability related to a cyber incident. A specific exclusion of liability related to data confidentiality breaches is less common in the United Kingdom and continental Europe (where there is limited experience in finding liability for breach of privacy). That said, at least one insurance company and/or broker respondent from each of the main markets indicated that exclusions related to both data confidentiality breaches and virus transmission were applied in general liability policies. As in the case of property policies, some insurers will allow for coverage of cyber risks to be added back into general liability policies as an endorsement, although often with sublimits and restrictions on the types of expenses covered (Betterley, 2015; Lloyd's and Cyence, 2017).
Figure 3.8. Potential coverage for cyber risk in traditional policies

- **Directors and Officers liability policies**: Companies impacted by a significant cyber incident with implications for business performance could face lawsuits from shareholders over the role of company executives or the company’s board in ensuring appropriate management of cyber risks (including response to a breach and, for US public companies, the level of risk disclosure relative to the SEC’s disclosure guidance) (Augustinos, Deem and Kamaiko, 2014) - although so far, such lawsuits have rarely led to findings or settlements in favour of shareholders in the United States (Vitkowski and Laurie, 2017). In New York State, a director or senior officer of a financial institution is now required to certify compliance with the state’s *Cyber Security Requirements for Financial Services Companies* which could provide a new avenue for shareholder claims (Carrier Management, 2017).

Currently, there is no general exclusion of cyber-related losses in directors and officers policies which suggests that such losses would normally be covered. However, some analysts believe that an exclusion for application in directors and officers policies will likely be developed with some anecdotal evidence that individual companies may be aiming to exclude cyber risks from individual policies (e.g. through the use of a clarification letter) (Barker, 2016). In other cases, insurance companies are affirming (or enhancing) the coverage of cyber incidents in their directors and officers policies (Insurance Journal, 2017f). The importance of this issue outside of the United States is likely to increase due to: (i) the spread of securities (and other) class action lawsuits to the United Kingdom, continental Europe and countries in Asia (Randall, 2017); (ii) the
recent precedent of large (USD 1 billion) directors and officers settlements in the United Kingdom (LaCroix, 2017); and (iii) the implementation of the General Data Protection Regulation (GDPR) in 2018 which should lead to more widespread publication of data confidentiality breaches in Europe (CGI Group, 2017). The GDPR requires the establishment of a Data Protection Officer with responsibilities that could lead to liability and some insurers have accordingly extended their definition of insured persons to include Data Protection Officers.

- **Errors and Omissions liability/Professional Indemnity policies**: In terms of cyber risks, errors and omissions/professional indemnity policies are mostly (although not only) relevant for technology companies who may be found liable for damages should the professional services (technology) that they provide play a role in a damaging cyber incident for one of their clients (e.g. in the case where the technology provided included vulnerabilities that were later exploited). Cyber liability is usually excluded from the errors and omissions policies offered to technology companies in the United States but can be added through an endorsement (Insurance Noodle, n.d.). For example, one company has begun offering coverage for data confidentiality breaches and malware transmission to its professional liability products for some professions (e.g. architects and engineers) (Carrier Management, 2016c). Professional indemnity/liability policies in Australia, New Zealand, the United Kingdom and many other countries normally include coverage for cyber incidents. In continental Europe, at least one company has started specifically including some cyber-related liabilities (communication and media liability due to online publishing) in its professional indemnity coverage (Insurance Journal, 2017g).

- **Crime (fidelity)**: As noted above, crime or fidelity insurance policies often provide coverage for cyber fraud/theft (Insurance Journal, 2017h). However, traditional crime policies may consider the act of transferring funds, even under fraudulent circumstances, an intentional act by a company’s employee that is excluded from coverage - which has led to the inclusion of specific social engineering coverage in some stand-alone cyber insurance policies.

- **Kidnap and Ransom**: The costs related to addressing a ransomware attack (including, in some cases, a ransom payment) could be covered by a traditional kidnap and ransom policy where the definition of an insured event includes a threat to damage or destroy data or insert a malicious code in a computer network (Weyland, 2016) and many providers of traditional kidnap and ransom insurance provide some coverage for cyber extortion (Wells Fargo Insurance Services, 2016). However, the increase in ransomware attacks is leading some to amend their policy language to exclude coverage for costs resulting from ransomware attacks, impose specific deductibles for ransomware incidents and/or limit coverage for some of the losses that may be caused by ransomware, such as business interruption (Barlyn and Cohn, 2017).

- **All-risk/business owner's policies**: Many smaller companies and certain types of companies (e.g. construction contractors) use all-risk insurance policies to cover both property and liability-related risks. In the United States, many business owner's policies for small businesses will include a cyber incident as a covered event and offer coverage for costs related to incident response, data and software restoration, cyber ransom and extortion and business interruption (whether as a standard inclusion, offered endorsement or combination) (Insurance Information...
Institute, 2014; Insurance Information Institute, 2015). One US business owner's policy reviewed also included coverage for communication and media liability and network security failure liability.

There is very little information available on the extent of explicit or implicit coverage of cyber-related risks in traditional policies. Lloyd's completed a consultation on cyber attack exposures with Lloyd's Market Association underwriters for all lines of business ("LMA panels") and received responses suggesting that there is some cyber exposure in all of its classes of business. A Swiss Re (2016a) survey of insurers from around the world found that 27% provided coverage for cyber risks in existing policies (rather than as separate coverage), while 10% provided both stand-alone coverage and coverage in traditional policies (with little variation across regions). Most (65%) of the respondents to the OECD questionnaire (including 80% of North American and 75% of European insurance sector respondents) perceive the coverage in existing policies of cyber risks to be a moderate or high risk factor which suggests that a significant share of overall coverage for cyber risks remains in traditional policies.

Notes

1. Some stand-alone cyber insurance policies and endorsements provide coverage on a "difference-in-conditions" basis, which means that coverage is only provided where the loss or damage is excluded from existing (primary) coverage. This type of insurance coverage is specifically provided to address gaps in existing coverage.

2. In many jurisdictions, the insurability (from a legal perspective) of a fine or penalty will depend on the circumstances. For example, the insurability of regulatory fines and penalties has been tested in a number of court cases in the United States based on the legal principle of *ex turpi causa non oritur actio* (from a dishonourable cause an action does not arise) - i.e. insureds should not receive the benefit of an insurance payout from an intentional wrongful or negligent act. Similarly, some respondents questioned whether fines imposed by the UK Information Commissioner's Officer would be legally insurable, while a working group led by IRT System X (2016) examining the coverage provided by cyber insurance in France found that regulatory penalties and fines may be uninsurable. Some insurance companies will not provide any cover for regulatory fines and penalties on principle, whether or not permissible by law (Gordon, 2014; Iole and Divelbiss, 2015).

3. The difference in the share of policies providing coverage for business interruption and network security liability between the RMS/CCRS review and the OECD review is likely linked to the timing of each review. A more recent review by RMS/CCRS found an increase in the inclusion of both of these types of losses (Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, 2017).

4. The RMS/CCRS review found a much higher share of policies providing coverage for intellectual property theft (23%). However, this may be explained by the difference in timing between the reviews as an update published in 2017 found a significant decline in the coverage of this type of loss (Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, 2017).

5. The RMS/CCRS review found that 46% of the policies reviewed included coverage for "reputational damage", defined in the review as "loss of revenues arising from an increase in customer churn or reduced transaction volumes, which can be directly
attributed to the publication of a defined security breach event." This was much higher than the share of policies offering this coverage observed in the OECD review of policies - which only included specific coverage for loss of profits (not coverage related to managing reputational damage) in its review.

6. For example, one US insurance company denied coverage for funds transferred as a result of a social engineering fraud on at least two occasions in 2015 and 2016 (and faced litigation in both cases). In at least one of the two examples, the disputed coverage was in a crime/fidelity policy (not a cyber insurance policy) (Krebs, 2016). Two other recent cyber insurance policy disputes related to social engineering that led to fraudulent transfers came to contradictory conclusions with one court finding in favour of the policyholder and the other in favour of the insurer denying coverage (based on slightly different policy wordings) (Collins, 2017). Recently, a court in the Canadian province of Alberta found that an insurer was not liable under a commercial crime policy for fraudulent payments made to a bank account by an employee deceived by an individual impersonating a supplier (Dunbar, 2017). A social engineering fraud incident at Leoni AG was partially covered under the company's fidelity policy and not covered under its cyber insurance policy which only covered financial losses caused by a network breach (Suess, 2017).

7. Some reports suggest that physical damage due to a covered peril (such as fire) resulting from a cyber incident could be covered under traditional policies (Gen Re, 2016) although it is not clear whether this would be the case where either the CL 380 or NMA 2912 exclusions were applied. No cases were identified where this was tested. As a result of the complexity of this issue, insurance companies that provide coverage for physical damage understand cyber insurance policies often do so on a difference-in-conditions basis. Similarly, business interruption coverage provided in stand-alone cyber insurance policies is often provided based on a disruption to information systems (i.e. non-material damage).

8. For example, a federal appeals court in the US state of Virginia upheld a lower court's decision obligating Travelers to cover costs related to defending Portal Healthcare Solutions against claims related to a privacy breach under its commercial general liability policy (Simpson, 2016b). This contradicts an earlier court decision which found that Zurich had no obligation under its commercial general liability policy to cover defence costs incurred by Sony as a result of a privacy breach (Insurance Information Institute, 2015).

9. For example, a professional services firm that has custody of client funds that are later lost to fraud could potentially seek coverage under an errors and omissions or professional indemnity policy (Kamaiko, 2016).

References


CGI (2017), "Severe cyber breaches cost PLCs 1.8% of company value or £120 million, according to new CGI study", *Media Centre*, 12 April, www.cgi-group.co.uk/news/cost-of-cyber-breach-to-plcs-cgi-study.


3. THE CYBER INSURANCE MARKET


3. THE CYBER INSURANCE MARKET


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

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


3. THE CYBER INSURANCE MARKET


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.


