Encouraging Clarity in Cyber Insurance Coverage

THE ROLE OF PUBLIC POLICY AND REGULATION

OECD

Encouraging Clarity in Cyber Insurance Coverage

The Role of Public Policy and Regulation

Please cite this publication as:

OECD (2020), *Encouraging Clarity in Cyber Insurance Coverage: The Role of Public Policy and Regulation,* www.oecd.org/finance/insurance/Encouraging-Clarity-in-Cyber-Insurance-Coverage.pdf

Foreword

The increased reliance on digital technologies has led to increasing digital security and privacy risks and the emergence of a cyber insurance market to provide policyholders with financial protection against many of those risks. The stand-alone cyber insurance market has grown rapidly in recent years and surveys have found an increase in take-up among both large and small businesses. However, despite the growth in premium volume and take-up, the affirmative cyber insurance market remains small relative to other commercial insurance business lines.

In February 2018, the OECD organised a conference (Unleashing the potential of the cyber insurance market) with the aim of building some consensus around how different stakeholders could contribute to addressing the main challenges to the market's development. Providing greater clarity on coverage for cyber risk was identified as one of the most important actions to support the development of the cyber insurance market.

This report examines the potential role of governments (ministries of finance and insurance regulators and supervisors) in: (i) encouraging greater clarity and consistency in the products that are being offered (taking into account the more limited need for government intervention in a corporate insurance market); and (ii) how legislation, regulation, guidance and other public policy measures (henceforth referred to as “public policy and regulation”) impact the variation in scope and form of insurance coverage for cyber risk. The development of this report has been informed by responses to a questionnaire provided by OECD member and non-member authorities as well as informal consultations with (re)insurance industry representatives undertaken in September and October of 2019. Responses were received from Argentina, Austria, Belgium, Bermuda, Brazil, Chile, Colombia, Estonia, France, Germany, Italy, Japan, Latvia, Lithuania, Portugal, Russian Federation, Slovak Republic, Slovenia, South Africa, Switzerland, the United Kingdom and the United States.

Enhancing the Availability of Data for Cyber Insurance Underwriting: The Role of Public Policy and Regulation is a complementary report focusing on the impact of the lack of data on past incidents necessary for underwriting and the role of governments in facilitating information sharing on cyber threats and incidents. *Insurance Coverage for Cyber Terrorism in Australia* assesses the potential gaps in insurance coverage for cyber-terrorism and other politically-motivated and destructive attacks, both in Australia and internationally.

Table of contents

Tables

Figures

Boxes

1 Insurance coverage for cyber risks

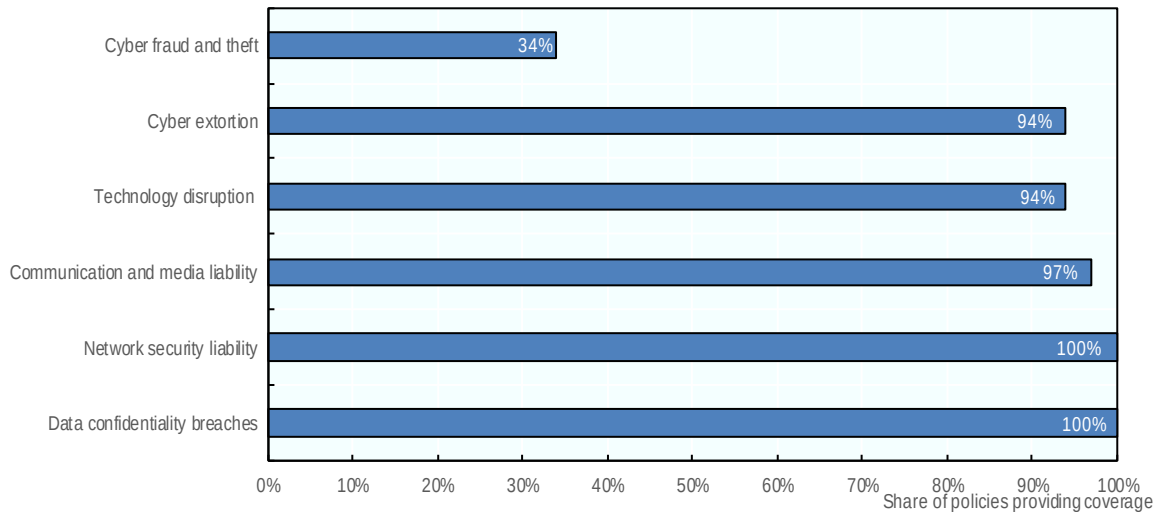
The increased reliance on digital technologies has led increasing digital security and privacy risks and the emergence of a cyber insurance market to provide policyholders with financial protection against many of those risks. The affirmative cyber insurance market (*i.e.,* stand-alone cyber insurance policies and cyber endorsements added to other policies) is focused on protecting businesses against some of the consequences of six main types of (mostly malicious) cyber incidents:[1]

- data confidentiality breaches (including privacy breaches): where a company has allowed (or has not prevented) unauthorised access to the private information (financial, medical, biometric, commercial) of individuals or companies resulting in incident management and notification costs, data, software and hardware[2] restoration costs, legal and defence costs, compensation to injured parties and fines and penalties (regulatory and/or contractual);
- network security liability: where a company has allowed (or has not prevented) the use of its network in a cyber attack on a third party leading to legal and defence costs and compensation to injured parties;
- communication and media liability: where a company's digital communications activities (intentional or accidental) result in defamation, libel, slander or other harm to a third party leading to legal and defence costs and compensation to injured parties;
- technology disruptions: where a company's operations have been disrupted as the result of a technology failure (accidental or malicious) at the company or one of its service providers leading to business interruption losses (or contingent business interruption losses) and potentially data, software and hardware restoration costs;
- cyber extortion: where a company's ability to access its data (or network) has been compromised or breached as part of an extortion (ransomware) attempt, leading to incident management costs, financial losses (ransom payment) and/or business interruption and data, software and hardware restoration costs; and
- cyber fraud and theft: where a company's funds or assets are stolen or fraudulently expropriated, including through social engineering, resulting in financial losses.

While some insurance companies might offer coverage for losses from these types of incidents in other types of policies, such as business interruption coverage in property policies, financial loss coverage in crime/fidelity policies or legal defence and compensation cost coverage in general liability/professional indemnity policies, almost all affirmative cyber insurance policies include coverage aimed at addressing these types of incidents (see Figure 1.1).

The stand-alone cyber insurance market has grown rapidly in recent years. Most estimates suggest written premiums of approximately USD 4-5 billion globally, up from approximately USD 3 billion in 2016, with expectations that the market will double or triple over the next five years (Deloitte Center for Financial Services, 2018[1]), (Orbis Research, 2018[2]), (OECD, 2017[3]), (Howard, 2019[4]). In a number of countries, surveys have found an increase in take-up among both large and small businesses.

Figure 1.1. Types of incidents covered by affirmative cyber insurance policies



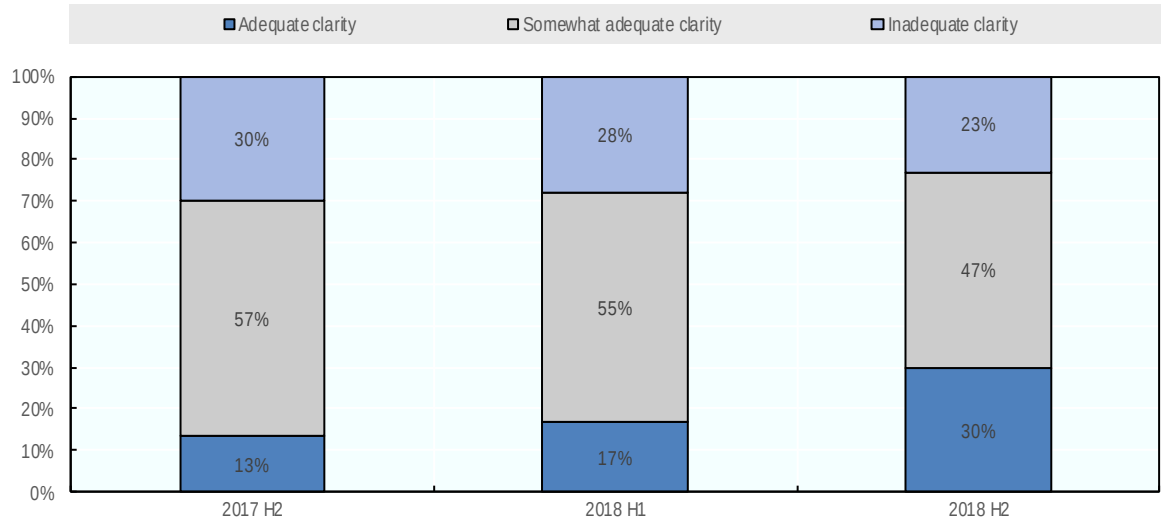
Source: OECD review of 35 publicly-available policy documents or summaries for cyber insurance policies offered in Australia, Canada, Japan, Netherlands, United Kingdom, United States or offered on a regional (Europe) or global basis.

However, despite the growth in premium volume and take-up, the affirmative cyber insurance market remains small relative to other commercial insurance business lines. The development of the affirmative cyber insurance market has been hindered by a number of challenges, including the difficulty in quantifying and underwriting cyber risks, the potential for accumulation risk and a lack of awareness of the need for insurance coverage for cyber risks (see (OECD, 2017[3]) for a more detailed discussion of these challenges). In February 2018, the OECD organised a conference (Unleashing the potential of the cyber insurance market[3]) with the aim of building some consensus around how different stakeholders could contribute to addressing these challenges to the market's development (OECD, 2018[5]).

Providing greater clarity on coverage for cyber risk was identified as one of the five most important actions to support the development of the cyber insurance market – and the most important action for insurance companies – by participants in the OECD conference. Policyholder misunderstandings about insurance coverage for cyber risk results from: (i) misunderstandings about the extent of coverage for cyber risks in other lines of business (i.e. where cyber risk coverage is found); and (ii) misunderstandings about the types of incidents and losses that are covered in affirmative cyber insurance policies (i.e. what coverage for cyber risk is included).

Periodic surveys of commercial insurance brokers in the United States by The Council of Insurance Agents and Brokers have continued to find that the majority of brokers perceive there to be inadequate clarity on coverage and exclusions in cyber insurance policies (70%, although down from 87% in 2017 - see Figure 1.2). In the United Kingdom, 31% of brokers surveyed in 2018 indicated that they had a poor or very poor understanding of cyber insurance and cyber risks (DAS UK Group, 2018[6]). In a survey of North American (and some international) underwriters and brokers published in 2018, 56% of respondents cited a lack of understanding of the coverage offered as a top obstacle to cyber-insurance take-up (Partner Re and Advisen, 2018[7]).

Figure 1.2. The perspective of brokers on cyber insurance coverage clarity



Source: (CIAB, 2019[8]), (CIAB, 2018[9]), (CIAB, 2017[10])

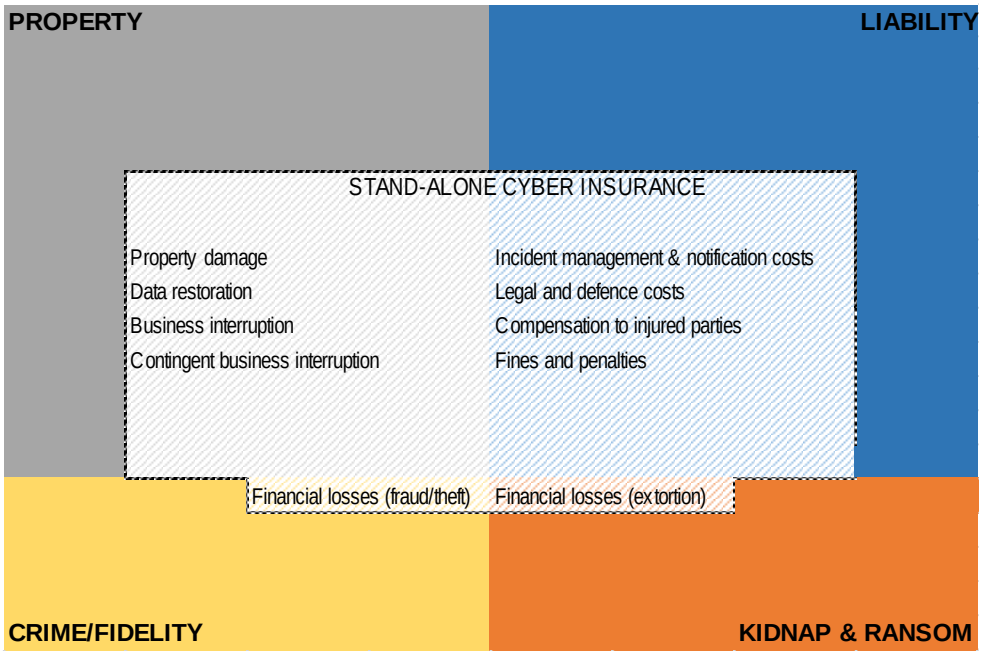
The development of this report has been informed by responses to a questionnaire by OECD member and non-member authorities[4] as well as informal consultations with (re)insurance industry representatives undertaken in September and October of 2019.

2 Where coverage for cyber risk is found

Overlaps in coverage for cyber risks

While cyber risks are insured through stand-alone cyber insurance policies, they may also be covered (either explicitly or implicitly) in various other insurance lines, including property insurance policies, various liability policies and crime/fidelity and kidnap and ransom insurance policies (see Figure 2.1). A survey of mostly North American underwriters and brokers found that, where endorsements for cyber risks are provided, they are most commonly attached to crime, property and various liability policies (particularly errors and omissions/professional indemnity, directors and officers and general liability policies) (Partner Re and Advisen, 2018[7]).[5] A number of reports and surveys have suggested that the expectation of coverage for cyber risks in other types of policies is one reason for low levels of take-up of stand-alone cyber insurance coverage (ENISA, 2012[11]); (Swiss Re and IBM Institute for Business Value, 2016[12]); (Friedman and Thomas, 2017[13]); (Ponemon Institute LLC, 2017[14]).

Figure 2.1. Coverage for cyber risks across lines of business



Note: Some of the costs identified above as liability costs (specifically incident management and notification costs and legal and defence costs) are actually first-party costs incurred by the insurer (rather than the reimbursement of costs incurred by a third-party as a result of a liability). However, they have been classified as such as they will generally only arise as a result of obligations to third parties.
Source: Adapted from (OECD, 2017[3]).

In reality, property and liability insurance policies may contain exclusions for losses that result from cyber incidents although there is uncertainty regarding the extent to which these exclusions are applied:

- Commercial property policies: Property insurance policies may apply an exclusion for all losses arising from the use of a "computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system" to inflict harm (Institute Cyber Attack Exclusion (CL 380)) or a more general exclusion for losses caused by computer malicious acts or human error or system failures affecting computer systems (IMIA Cyber Exclusion 2018 (International Association of Engineering Insurers, 2018[15])). In addition, data is normally not considered as tangible property insured in commercial property insurance policies, reinforced by the application of Electronic Data Endorsements in many policies (NMA 2914 or 2915 (Lloyd's Market Association, 2015[16]); (Lloyd's Market Association, 2015[17])). The coverage of business interruption losses in property policies is contingent on the occurrence of damage to tangible property covered by the policy (i.e. the losses will also be excluded if the property damage is not covered).
- Liability insurance policies: In the United States, in response to a number of coverage disputes,[6] standard commercial general liability forms published by the Insurance Services Office (ISO) now contain an exclusion for liability related to loss, damage or loss of access to data and for the disclosure of confidential or personal information. In Australia, some public liability policies exclude liability related to the insured's internet operations. There is also a Lloyd's market exclusion for losses resulting from malicious cyber incidents (LMA5274 (Lloyd's Market Association, 2016[18])), which was developed for casualty treaty reinsurance although is also used in some types of liability policies.
- Crime/fidelity insurance policies: There are no specific exclusions in general use that have been developed to remove cyber fraud and theft from crime/fidelity insurance policies.[7] As a result, crimes committed through the use of computers are often covered (Box 2.1 provides an overview of the increasing significance of these types of attacks). However, some types of cyber fraud and theft (social engineering) may fall outside the scope of traditional crime insurance coverage because employee involvement in the authorisation of the fund transfer coverage following a deception by social engineering may be deemed a voluntary action. This has led some insurers to offer specific endorsements for social engineering fraud as add-ons to crime/fidelity coverage (as well as to cyber insurance coverage) (Godes, 2019[19]) (NorthStar Insurance Services, 2018[20]). It has also led to coverage disputes and litigation that, at least in the United States, has led to some uncertainty as to whether crime/fidelity policy coverage for social engineering fraud is effective.8
- Kidnap and ransom insurance policies: Similar to crime/fidelity policies, there are no specific exclusions in general use to remove cyber extortion from kidnap and ransom insurance coverage.[9] However, whether coverage is provided will depend on the specific policy language with some policies providing more narrow coverage for extortion demands (e.g. relating only to the kidnap of a person (Skidmore, 2018[21])) – and some insurers have re-visited policy language in the aftermath of widespread ransomware attacks in 2017 (Barlyn and Cohn, 2017[22]). According to one large insurer, many insurers will now only provide coverage for cyber-extortion in kidnap and ransom policies if endorsed.

Box 2.1. The significance of theft of funds

Theft of funds through phishing, business email compromise (BEC), social engineering and other forms of payment diversion is accounting for an increasing share of cyber-related losses and claims. The US Federal Bureau of Investigation received over 20 000 BEC complaints in 2018 with estimated losses of USD 1.2 billion (FBI, 2019[23]) (overall losses for the three years since June 2016 have reportedly reached USD 26 billion (Newman, 2019[24])). New technologies, such as voice-synthesis software and other tools that can be used to create "deepfakes", provide new methods for deceiving company employees and have reportedly been used to incite fraudulent fund transfers (successfully for GBP 200 000 in one case) (Harwell, 2019[25]) (Best, 2019[26]).

Among the insurers and other organisations that provide statistics on cyber claims, theft of funds claims accounted for 10%-29% of all cyber claims in 2017 (CFC Underwriting, 2018[27]), (Hiscox, 2018[28]), (Beazley, 2018[29]), (NetDiligence, 2018[30]). One individual insurer experienced a 133% increase in BEC claims in 2018 (on a global basis) (Beazley, 2019[31]). The average amount of funds stolen normally ranges from USD 70 000 to USD 130 000 although one policyholder was paid USD 2.5 million for a BEC claim in 2018 (and some past claims have reached USD 9 million) (Beazley, 2019[31]), (NetDiligence, 2018[30]) (Reseller Middle East (UAE), 2019[32]). In August 2019, a European auto parts supplier reportedly lost USD 37 million to a BEC (Matthews, 2019[33]).

Note: Phishing generally refers to broad, indiscriminate and impersonal attempts to trick individuals into transferring funds. Business email compromises refer to targeted attempts using a personalised email message that appears legitimate. Social engineering generally refers to targeted attempts that may involve electronic communication as wells as phone calls (NetDiligence, 2018[30]). Cyber criminals also use social engineering to access user credentials in order to change payment information for the purposes of diverting funds (Beazley, 2019[31]).

Politically-motivated cyber attacks

The involvement of politically motivated actors in perpetrating cyber attacks adds a further layer of complexity to questions around where (or whether) cyber losses are covered. War and/or terrorism are often excluded from many types of insurance policies (property, liability) – and served by specialty war and terrorism (or political violence) markets – although this exclusion is driven by insurance market practices rather than any legislative or regulatory requirement.[10]

As a result, coverage for damages and losses from cyber attacks that might be expected to be found in property or liability policies may not materialise if it is determined that the attacks originated from an actor linked to a state or a terrorist organisation.[11] At least two companies affected by the 2017 NotPetya ransomware attacks are reportedly involved in litigation with insurers that denied claims based on war exclusions applied in their property insurance polices. The litigation is being closely watched as the first instance of a war exclusion being applied to deny coverage for a cyber attack (although the circumstances may be relatively unique given the potential link to an ongoing conflict between two nation-states) (see Box 2.2).

Box 2.2. A first test of the war exclusion for cyber attacks linked to states

The NotPetya malware attack in 2017 affected a number of companies around the world. It was disseminated through a corrupt software update in a Ukrainian tax software application and resulted in the corruption of data in affected systems (Levine and Ellis, 2019[34]). The attack was attributed by a number of governments (including Australia, Canada, United Kingdom and the United States) to Russian attackers – and specifically in some statements to the "Kremlin" as an "effort to destabilize [the] Ukraine" as part of an "ongoing conflict" (Bershidsky, 2019[35]).

One of the affected companies, Mondelez International, reportedly faced losses of over USD 100 million as a result of damages to equipment and interruption to its business after being affected by NotPetya. Mondelez had property insurance coverage through Zurich America Insurance for physical loss or damage to electronic data as well as for non-physical losses due to a failure of electronic processing equipment as a result of a cyber attack (Shooter, 2019[36]). The claim was (eventually) denied by Zurich as the policy excluded losses resulting from an act of war (the definition of which included "hostile or warlike action in time of peace or war") (Bershidsky, 2019[35]). Mondelez has launched litigation against Zurich which, at the time of writing, remains before the courts.

Another affected company, Merck, reportedly made claims of USD 1.3 billion under property insurance coverage provided by a number of insurance companies for damage to computers and business interruption losses. The company has collected from some of its insurers – and entered into settlements with others – although an ongoing dispute is being litigated in a New Jersey court (Voreacos, Chiglinsky and Griffin, 2019[37]).

Market developments and perspectives on providing clarity on cyber risk coverage across business lines

Consultations with (re)insurance companies for the development of this report suggested an increasing level of consensus on the need to provide greater clarity on whether cyber is covered in a given policy (i.e. providing affirmative cover for - or clear exclusions of – cyber risk in each relevant line of business). Some large insurance providers (e.g. Lloyd's, AIG, Allianz, FM Global)[12] have made specific commitments to provide clarity on cyber risk coverage by a target date.

There are industry efforts to identify where there may be a lack of clarity on whether cyber risk is covered. The Lloyd's Market Association recently undertook a review of the use of cyber exclusion clauses across a number of business lines (focused on the Lloyd's market). The review found very limited use of cyber exclusions in many lines of business[13] which could indicate that either affirmative coverage is being provided in many policies or that significant silent/non-affirmative coverage remains to be addressed (Lloyd's Market Association, 2018[38]). An annual report on silent cyber risk has found declining concerns about the frequency of cyber claims in some lines of business suggesting that either: (i) cyber is not considered to be a significant peril for property and liability underwriters; or (ii) the use of exclusions in property and liability policies will successfully limit the frequency of cyber claims (Willis Towers Watson, 2019[39]).[14]

The insurance industry is also developing standard exclusions for use across business lines where coverage for cyber risk or certain cyber risks is not intended. In June 2019, the International Underwriting Association published two new model clauses for potential use in excluding cyber risks across lines of business – either on an absolute or limited basis (IUA, 2019[40]), (IUA, 2019[41]).[15] There is also an effort to provide greater clarity on coverage for politically-motivated cyber attacks that is reportedly considering how

to exclude large-scale cyber warfare while providing clarity of coverage for smaller-scale cyber attacks with state involvement (Spoerry, 2019[42]). One UK-based reinsurance broker has published a proposed war exclusion adapted to cyber risk that would limit the scope of the exclusion to cyber-attacks between governments in a state of war (Capiscum Re, 2019[43]).

However, a recent EIOPA survey found that there is still significant work to be done by companies in the European Union to accomplish full clarity as 41% of surveyed insurance companies had not taken any action to identify non-affirmative exposures across lines of business (EIOPA, 2019[44]).[16] A number of the companies consulted during the development of this report indicated that they expected that the AIG and, particularly, the Lloyd's commitments would drive the market to address this issue (as the Lloyd's market is a major provider of reinsurance for cyber exposure).

Many of the terrorism (re)insurance programmes are also working to prepare for the possibility of cyber-terrorism (and potentially other politically-motivated destructive attacks) by examining the coverage they provide and taking steps to clarify or expand their coverage where needed. For example, the Australian Reinsurance Pool Corporation invited the OECD to undertake an assessment of possible gaps in insurance coverage for cyber-terrorism losses in Australia and to provide advice on how to respond to any gaps (OECD, 2020[45]). The Geneva Association and the International Forum for Terrorism Risk (Re)Insurance Pools (IFTRIP) have established a joint task force on cyber terrorism and cyber warfare to conduct research into these issues (The Geneva Association, 2019[46]).

There appears to be some continued debate within the (re)insurance sector (and among insurance buyers) on whether cyber should be considered a peril covered in many lines of business or a line of business on its own (i.e. with all or most types of cyber losses covered by a stand-alone cyber insurance policy).[17] One recent survey found some evidence that the extent of overlapping coverage in cyber insurance and other policies is perceived to be increasing (36% indicated that overlap increased relative to 24% that indicated that overlap decreased) (Partner Re and Advisen, 2019[47]).

The potential role of governments in supporting clarity on cyber risk coverage across business lines

Insurance product development requirements and expectations

Public policy and regulation can have a direct impact on whether a given type of insurance policy will cover a specific risk where the risks that need to be covered by specific types of policies are prescribed. In some cases, public policy and regulation prescribes that coverage for certain perils be included (or offered) in certain types of policies.[18] Consistent with the IAIS Insurance Core Principle 19 on Conduct of Business, supervisors will also normally have the ability to require insurance companies (and intermediaries) to ensure that the products they offer clearly disclose the risks insured and excluded under a given policy (IAIS, 2019[48]) which may be implemented through a product approval requirement[19] or through the establishment of principles for product development. A number of countries (including Brazil, Chile, Colombia, Japan, Russia and European Union members) have legislation or regulation that generally requires policies to clearly define what is included and excluded in a given policy. In Colombia, for example, regulatory requirements oblige insurers to state the primary coverage and exclusions up front in clear and concise language.

Some insurance supervisors have focused specifically on encouraging better disclosure of the scope of coverage for cyber risk in different types of policies. For example, in the United Kingdom, the Prudential Regulation Authority (PRA) issued a supervisory statement outlining its expectations with respect to the management of cyber insurance underwriting risk. Among other expectations, the supervisory statement suggests that companies should either offer explicit cover for cyber risks or introduce robust wording exclusions for those risks (Bank of England Prudential Regulation Authority, 2017[49]).[20] The guidance

developed by the PRA has unquestionably contributed to encouraging the (re)insurance sector to provide greater clarity and could be a model for supervisory guidance in other jurisdictions.

Insurance regulators and supervisors could also require that coverage for cyber risks be included in specific lines of business or prohibit the exclusion of cyber risks from certain policies (as is done in some jurisdictions for natural catastrophe and/or terrorism perils). However, given the continued debate about how best to provide coverage for cyber risks (or some cyber risks - i.e. as a peril or as a separate line of business), it may be better to wait to see how the market develops (and how the needs of policyholders evolve). If the effort by (re)insurers to provide greater clarity on the coverage of cyber risks across lines of business leads to significant exclusions and gaps in coverage, this could be re-visited.

Terrorism insurance programmes

The involvement of terrorism (re)insurance programmes in providing insurance, co-insurance or reinsurance coverage for terrorism losses could have an impact on how and where cyber-terrorism risk is covered. For example, in the United Kingdom, the reinsurance for terrorism incidents provided by Pool Re has been expanded to cover physical damage from cyber-terrorism, which could encourage coverage for cyber incidents (or cyber-terrorism incidents) in property insurance policies. In France, the definition of terrorism insurance coverage that must be provided in commercial property (and other) policies includes cyber-terrorism (limited to direct property damage and business interruption). In the United States, a requirement for mandatory offer of coverage for terrorism is applicable to cyber insurance policies.

Insurance regulators and supervisors (or governments more generally) are likely to face increasing pressure to address the insurance coverage of politically-motivated attacks (including terrorism), particularly if these attacks lead to more significant losses and the industry develops and applies an (effective and implementable[21]) exclusion for such losses. The Recommendation of the OECD Council on the Establishment of a Check-List of Criteria to define Terrorism for the Purpose of Compensation (2004), which contributed to the development of a common approach to terrorism (re)insurance in the aftermath of the September 11th attacks in the United States, could potentially be updated to play a similar role in addressing politically-motivated cyber attacks.

Box 2.3. Supporting clarity in cyber insurance coverage: recommendations

- As some companies have not begun to address non-affirmative (silent) cyber risk across their lines of business, insurance regulators and supervisors should explicitly require insurance companies to clearly state whether cyber risks are covered or not in all relevant policies (i.e. across relevant lines of business). The transition to affirmative coverage for cyber risk should be closely monitored to ensure that significant gaps in coverage do not emerge based on the application of broad exclusions of cyber risk.
- Governments should clarify the availability and scope of (re)insurance coverage through terrorism (re)insurance programmes for cyber-terrorism and other politically-motivated (and destructive) cyber-attacks – and address any gaps that may emerge due to the application of exclusions by the insurance sector.

3 What types of losses are covered

Differences in the coverage of cyber losses

In addition to differences in terms of which policies provide coverage for cyber risks, there are also differences in terms of the types of losses that affirmative cyber insurance policies will cover (and how that coverage is described). A number of reports and surveys have found significant differences in the scope of coverage, exclusions and conditions found in stand-alone cyber insurance policies (ENISA, 2012[11]), (Friedman and Thomas, 2017[50]), (Lloyd's and Cyence, 2017[51]), (CCRS and RMS, 2017[52]). Some have suggested that the variation in coverage has: (i) reduced the number of policies that intermediaries will offer their clients (CIAB, 2016[53]); (ii) drove decisions to not acquire cyber insurance coverage (Ponemon Institute LLC, 2017[14]); and (iii) reduced trust in whether cyber insurance policies would payout on incurred losses (Reeve, n.d.[54])

Much of the variation in coverage results from differences in definitions, conditions and exclusions as policies have evolved very quickly, hindering the emergence of standardised language (Blosfield, 2019[55]). Insurers often use different terminology to describe similar types of covered losses or incidents or applicable conditions (Wraight, 2019[56]). Table 3.1 provides an example of how three different policies offered on the Australian market describe the coverage provided for common losses from a data confidentiality breach involving personal information.

Table 3.1. Comparison of coverage for data confidentiality breach costs (Australia)

	Policy #1	Policy #2	Policy #3
Incident management and notification	"Privacy Breach Costs" "Data breach notification costs" (sub-limited extension)	"Response management costs" (IT services, public relations services, data breach notification costs)	"Privacy Notification and Crisis Management Costs"
Data, software and hardware restoration costs	Digital Asset Replacement and Betterment Costs	"Response management costs" (data restoration costs)	"Data Recovery"
Legal and defence costs	"Regulatory proceeding defence costs and penalties" (sub-limited extension) "GDPR Proceedings" (sub-limited extension)	"Response management costs" (legal services) "Data Protection Regulatory Obligations" (investigation costs)	"Third Party Liability Coverages" (Regulatory Defence and Fines)
Compensation to injured parties	"Security and Privacy Liability"	"Third Party Liability" (breach of personal or corporate information)	"Third Party Liability Coverages" (Privacy and Security)
Fines and penalties (regulatory and/or contractual)	"Regulatory proceeding defence costs and penalties" (sub-limited extension "PCI Security Standards fines and penalties" (sub-limited extension) "GDPR Proceedings" (sub-limited extension)	"Data Protection Regulatory Obligations" (investigation costs, fines, PCI-DSS fines and penalties)	"Third Party Liability Coverages" (Regulatory Defence and Fines)

Source: Review of publicly-available policy language for three cyber insurance policies offered in Australia by globally-active insurance companies.

In addition, while outside the scope of this report, public policy has important implications for the types of losses that materialise in the aftermath of a cyber incident which adds a layer of complexity based on differences in the obligations established by public policy in different countries (see Box 3.1).

Box 3.1. The implications of public policy on losses resulting from cyber incidents

Public policy establishes the obligations of companies to their shareholders in terms of protecting their business against cyber incidents, and to their employees and customers in terms of protecting them from unnecessary collection and disclosure of personal information – as well as the penalties and claims that they will face if these obligations are not met.

Public companies have a general obligation to their shareholders to disclose and manage material risks to their business. In the United States, the Securities and Exchange Commission (SEC) has published interpretive guidance on cybersecurity disclosure which, if not adhered to, could lead to enforcement actions and shareholder claims on directors and officers (Securities and Exchange Commission, 2018[57]). In addition, the SEC recently undertook an examination of the internal accounting controls at nine companies affected by social engineering fraud losses and suggested that enforcement action could be taken in the future as a result of failures in accounting controls (Johnson, 2018[58]).

Companies (public and private) that collect personal information from employees and customers (that are covered within the scope of privacy protection legislation) have various obligations related to the collection and use of that data – sometimes at both the national and subnational level. In the United States, privacy legislation has been enacted in all states and also for certain types of personal information at the federal level (e.g. health information) (BakerHostetler, 2019[59]). In Canada, there is a federal Privacy Act as well as provincial privacy laws in most provinces, covering provincial government employees, health or education information and/or the private sector (Office of the Privacy Commissioner of Canada, n.d.[60]). In Australia, Japan, Mexico and other countries, there is national privacy protection legislation (Office of the Australian Information Commissioner (OAIC), n.d.[61]), (Hayashi and Shimada, 2019[62]) (Montes de Oca and Bandeira, 2019[63]). In Europe, the General Data Protection Regulation (GDPR) is a single set of requirements that applies across all member states.

The obligations imposed on companies vary substantially across (and even sometimes within) countries (BakerHostetler, 2019[59]), (McQuinn and Castro, 2019[64]), in terms of:

- the types of obligations imposed on companies that are collecting data (e.g. obtaining consent; limitations, disclosures or opt-out provisions related to data use or sale; portability requirements; obligations to delete data upon request);
- the types of personal information that is protected (e.g. specified types of records vs. broad definition of any type of data related (sometimes even indirectly) to an identifiable natural person, inclusion of biometric data[1]);
- requirements for notifying data protection authorities and affected individuals (e.g. all cases vs. cases where harm is likely);
- the potential magnitude of fines and penalties that can be imposed; and
- the ability of affected individuals to seek compensation for breach of obligations (i.e. private right of action).[2]

The international reach of privacy protection requirements adds a further level of complexity. The EU GDPR imposes obligations on any company that collects data from EU citizens. Similarly, in the United States, state legislation (such as the California Consumer Privacy Act) imposes obligations on any company collecting data on state residents, no matter where the company is based. One law firm that

provides incident management support estimates that 25% of all the US-based incidents that it manages involved international reporting requirements (BakerHostetler, 2019[59]). The Equifax data breach in 2017 led to fines in the United Kingdom and Australia, a compliance agreement in Canada and a financial settlement with two US federal agencies and 50 US states and territories (Saxena, 2019[65]), (Office of the Privacy Commissioner of Canada, 2019[66]), (FTC, 2019[67]). A data breach at Uber in 2016 led to fines in the Netherlands, United Kingdom and a settlement with the Attorneys General of all 50 US states (Soylu and Oztoprak, 2019[68]).

Although outside the scope of insurance regulators and supervisors mandates, these differences in obligations to shareholders, employees and customers and the ability of those stakeholders to seek compensation for breaches of those obligations are a significant contributor to the complexity of providing coverage for cyber insurance.

1. In some jurisdictions, biometric data is subject to different legislation and protection requirements. In the United States, the state of Illinois was the first to impose requirements for the collection, sale and disclosure, safeguarding and retention of biometric data that has since been replicated in a number of other US states. The Illinois legislation allows a private right of action that has led to a number of class action lawsuits (Kuehner-Hebert, 2019[69]).
2. In addition to differences in terms of whether a private right to action exists, there have also been different judicial decisions in the United States as to whether claimants had standing to make claims for damages as a result of data breaches and the requirements for demonstrating harm linked to a specific breach (Navetta, Friedman and Ebrahem, 2019[70]) – with important differences across states due to existing or proposed legislation (Duffy, Slawe and Busta, 2019[71]). In other countries, including most EU countries and New Zealand, privacy protection requirements providing a private right of action are new (or not yet implemented), creating significant uncertainty about the types of incidents that will lead to compensation and the magnitude of that compensation. In the European Union, affected individuals can notably seek compensation for both material (financial loss) and non-material (emotional distress) damages (Aon and DLA Piper, 2019[72]). In an early test in the United Kingdom, the High Court provided authorisation for customers affected by the British Airways breach to seek compensation (Saunt, 2019[73]).

The implications of public policy and regulation on which cyber losses may be covered

In a few areas, public policy and regulation has direct implications on whether losses from cyber incidents can be reimbursed by insurance (whether provided as stand-alone affirmative coverage or in another line of business).

Insurance coverage for fines and penalties

Fines and penalties may be imposed by a variety of regulatory authorities for breaches of obligations to shareholders, employees and/or consumers. The ability of affected policyholders to be reimbursed by insurance for fines and penalties imposed depends on the terms and conditions of the coverage[22], the authority imposing the fine and the type of fine (civil/administrative or criminal and whether punitive or compensatory), the specific jurisdiction where the fine is being imposed and the nature of the act being penalised – which could lead to uncertainty regarding which fines and penalties are likely to be reimbursed under an insurance policy.

The OECD reviewed publicly-available policy language (or summaries of coverage) for 35 stand-alone cyber insurance policies offered in Australia, Canada, Japan, Netherlands, United Kingdom, United States and/or on a regional (Europe) or global basis. Some coverage for fines and penalties was found in all but five of the policies reviewed (see Table 3.2). In most countries (with the exception of Japan – which may be due to the limited sample size of one policy), the vast majority of cyber insurance policies offer some coverage for fines and penalties.

Table 3.2. Coverage for fines and penalties

	Advertised coverage for fines and penalties (number of policies)	No advertised coverage for fines and penalties (number of policies)
Australia	7	1
Canada	4	1
Japan	0	1
Netherlands	1	0
United Kingdom	3	1
United States	8	1
Europe (offered on a regional basis)	2	0
Global (offered on a global basis)	5	0

Source: OECD review of publicly available cyber insurance policies

Box 3.2. The significance of regulatory fines and penalties

Fines and penalties have not been a significant component of (published) cyber claims. In Europe, only 4% of AIG's claims between 2013 and 2016 were classified as legal and regulatory proceedings due to privacy regulation violations (which would also include notification, investigation and defence costs in addition to any (insurable) fines and penalties) (AIG Europe, 2016[74]). In the (US-focused) NetDiligence claims studies, only 17 claims between 2014 and 2018 reported regulatory defence costs, of which ten reported regulatory fines – with claims payments for fines averaging from USD 5 000 to USD 60 000 in most cases although with one claim related to a USD 3.5 million fine (NetDiligence, 2019[75]).

However, the expansion of privacy protection requirements – in terms of both the scope of requirements and the number of jurisdictions covered – and strengthened enforcement creates a significant potential for an increase in the imposition of regulatory fines and penalties. In the United States, the Federal Trade Commission (FTC) reportedly initiated or resolved 29 data security and consumer privacy actions (Mondaq Business Briefing, 2019[76]) while the Department of Health and Human Services Office for Civil Rights (OCR - responsible for enforcing privacy protections for health data) reached ten settlements and obtained one summary judgement in 2018 (Mondaq Business Briefing, 2019[77]). Uber agreed to a USD 148 million penalty settlement with all 50 states and the District of Columbia as a result of a 2016 data breach (New York State Attorney General, 2018[78]). In Europe, the first 20 months of GDPR implementation has led to more than 160 000 notifications to regulators of personal data breaches according to one estimate (although this includes many minor breaches unlikely to lead to a fine or penalty) (DLA Piper, 2020[79]).

The magnitude of fines and penalties may also increase. The OCR imposed its largest ever fine (USD 16 million) for a health information privacy violation on a health insurer in October 2018 (Office for Civil Rights, 2018[80]) while the FTC approved a USD 5 billion settlement with Facebook for allegedly violating a 2011 consent decree related to the use of collected data (Kang, 2019[81]) (Shepardson, 2019[82]). Under the California Consumer Privacy Act, implemented in 2020, the state Attorney General may impose fines of up to USD 7 500 per record (Jergler, 2019[83]). In the European Union, where the GDPR allows fines and penalties of up to 4% of a company's global turnover, significant (preliminary) fines have been imposed on Google in France (EUR 50 million) and Marriott and British Airways in the United Kingdom (GBP 110 million and GBP 204 million, respectively) with a number of smaller fines imposed in Belgium, Denmark, France, Germany, Greece, Hungary, Italy, Norway, Poland, Portugal, Romania, Spain and Sweden, amongst others (Rosemain, 2019[84]), (MamoTCV Advocates, 2019[85]), (Latham & Watkins LLP, 2019[86]), (Aon and DLA Piper, 2019[72]). In many cases, the fines imposed were equivalent to 1% or more of the company's worldwide turnover (Latham & Watkins LLP, 2019[87]), (Kadar and Gaillard, n.d.[88]). In Australia, the government recently announced changes that would allow for fines and penalties for Privacy Act violations of up to AUD 10 million with the possibility of imposing fines of more than AUD 100 million for some companies (Breakspear et al., 2019[89]).

However, in all of the policies reviewed, any coverage for fines and penalties is subject to conditions:

- The reviewed policies offered in Australia limit reimbursement to fines that are "insurable" or "insurable under applicable law". Two of the policies specifically exclude civil and criminal fines and penalties (although in one case, only civil and criminal fines other than regulatory fines are excluded). Most of the policies also refer to "regulatory" fines and penalties with some policies referring more specifically to data protection or privacy regulation.
- In Canada, the reviewed policies offer coverage for fines and penalties imposed as a result of regulatory actions (in one case, "privacy regulatory action") where insurable under applicable law.
- In the United Kingdom, the reviewed policies limited coverage to civil or regulatory fines and penalties imposed by (or payable to) a government authority (national or sub-national, including EU authorities) or resulting from an investigation by a government, regulatory, law enforcement or statutory body - and where insurable under applicable law. In one case, the coverage only included fines following a "privacy investigation". For reviewed policies offered across Europe, reimbursement is also limited to fines and penalties imposed by a government or public authority.
- The reviewed policies offered in the United States tend to apply a general exclusion for any civil or criminal fines or penalties except those for which explicit coverage is provided. Explicit coverage is provided for "privacy regulatory fines" or fines resulting from "regulatory action" where insurable under applicable law.

The insurability of regulatory fines and penalties varies across jurisdictions and is also dependent on the nature of the violation being penalised and the type of fine being imposed. The insurability of fines and penalties imposed under specific legislation or by a specific regulatory authority is not normally directly addressed in the statute or by the regulatory authority (with some exceptions, such as the UK Financial Conduct Authority's prohibition of insurance payments to reimburse the cost of financial penalties it imposes (FCA, 2018[90])). As a result, assessments of the insurability of regulatory fines and penalties will often require interpretation with reference to jurisprudence or other public policy and regulation (including insurance legislation):

- In many countries, regulatory fines and penalties can be imposed (or interpreted) as either criminal penalties or administrative penalties. In the EU, GDPR fines for non-compliance are administrative fines although each member state may establish additional rules on penalties for infringements that may be either criminal or administrative in nature (Intersoft Consulting, n.d.[91]), (European Union, n.d.[92]). A number of countries in the EU (at least fourteen23) are expected to allow for criminal fines (Aon and DLA Piper, 2018[93]), (Aon and DLA Piper, 2019[72]).
- In most (if not all) countries, criminal fines and penalties are not insurable based on the principle that a person (legal or natural) that has committed a (by definition) intentional and malicious (criminal) act should be required to bear the consequences (penalties) of that act. Otherwise, the deterrent effect of the penalty would be reduced (Anthony, 2019[94]).
- In some countries (Austria, Denmark, France, Italy, Luxembourg, Portugal, Russia, Switzerland), all regulatory fines and penalties (whether criminal or administrative) are not insurable either as a result of legislation or existing jurisprudence that has found such insurance to be unlawful or counter to public order (Aon and DLA Piper, 2018[93]). In a number of other EU countries,[24] administrative fines imposed under GDPR may be found to be uninsurable as counter to public order or to the principle that the negligent party should bear the cost, although there is no specific legislation or clear jurisprudence. In a few jurisdictions, administrative or civil fines might be uninsurable in certain circumstances depending on the nature of the act (such as whether there is intent or malice in the case of Croatia, Greece, Netherlands, Sweden) or the purpose of the fine (such as whether the fine is meant to be punitive or dissuasive, in the case of Ireland, Norway, United Kingdom, some US states) (Anthony, 2019[94]), (Iole and Divelbiss, 2015[95]) (Aon and DLA Piper, 2018[93]), (Aon and DLA Piper, 2019[72]).

- Insurance legislation, regulation or supervisory practice may specifically deem (or confirm) that insurance contracts that indemnify policyholders for any type of fine or penalty are impermissible, invalid, a violation of public order principles or counter to the purpose of insuring only random/unintentional events (Argentina, Austria, Bulgaria, Colombia, Croatia, Estonia , Finland, Germany, Hungary, Italy, Latvia, Portugal, Romania, Spain, California (United States)[25]) (Aon and DLA Piper, 2018[93]), (Marsh, 2018[96]) (Greene et al., 2019[97]).[26]

A further complexity is introduced by the possibility that companies with operations in more than one jurisdiction could seek to assert coverage in a jurisdiction where public policy and regulation is more favourable to allowing such coverage – even if the fine and penalty is imposed in another jurisdiction (in fact, some legal advisors recommend that policyholders should aim to confirm coverage in favourable jurisdictions (Oehninger and Moura, 2019[98])). Three of the policies reviewed explicitly allowed for the reimbursement of fines and penalties *where insurable under the laws of an applicable jurisdiction most favourable to the insured* suggesting that the applicable law may not specifically be the law of the jurisdiction where the fine was imposed or where the policy was underwritten. A number of cyber policies offered in North America (and other non-EU jurisdictions) provide specific coverage for GDPR fines (Marsh, 2018[96]). Only one of the policies reviewed explicitly indicated that fines would not be reimbursed if uninsurable under the law of the jurisdiction imposing the fine or penalty.[27]

Insurance coverage for fines and penalties might also be limited to incidents that trigger coverage in the policy, such as an actual data breach incident, whereas privacy protection regulation in various jurisdictions allow for fines and penalties for non-compliance of regulatory requirements more broadly, including in cases where no specific network breach has occurred (Aon and DLA Piper, 2019[72]).

Ultimately, where there are no direct or specific legal or regulatory impediments to providing coverage, insurability or uninsurability is subject to interpretation by the insurer and potentially to disputes and litigation (LaCroix, 2018[99]).

Insurance coverage for ransom payments

Cyber extortion attacks (whether ransomware or other types of extortion) could lead to a number of losses, including business interruption (where the extortion impedes access to data that is necessary for operations), incident (crisis) management costs, data (and hardware) restoration and potentially ransom payments to terminate the attack or threat of attack.

The OECD reviewed publicly-available policy language (or summaries of coverage) for 35 stand-alone cyber insurance policies offered in Australia, Canada, Japan, Netherlands, United Kingdom, United States and/or on a regional (Europe) or global basis. In almost all countries, the vast majority of cyber insurance policies (if not all) offer some coverage for expenses resulting from cyber extortion (see Table 3.3).

Table 3.3. Coverage for cyber extortion losses

	Advertised coverage for cyber extortion (number of policies)	No advertised coverage for cyber extortion (number of policies)
Australia	8	0
Canada	5	0
Japan	0	1
Netherlands	1	0
United Kingdom	4	0
United States	9	0
Europe (offered on a regional basis)	2	0
Global (offered on a global basis)	4	1

Source: OECD review of publicly available cyber insurance policies.

Box 3.3. The significance of ransom payments

Demands for ransom payments can result from the installation of malware on a company's network that makes data or systems inaccessible or inoperable until the ransom demand is met (i.e. ransomware) or from a threat to release confidential data, unleash a distributed denial-of-service attack or even post a number of bad customer reviews unless a payment is made. Ransomware and other types of cyber extortion accounted for approximately 10% to 20% of cyber insurance claims (including ransom payments as well as crisis management costs) prior to 2017 when the global WannaCry and Not Petya ransomware attacks led to a significant increase in the claims accounted for by cyber extortion (ranging from 21% to 31% among insurers and other organisations that published claims data) (CFC Underwriting, 2018[27]), (Hiscox, 2018[28]), (NetDiligence, 2018[30]) (Burns, 2018[100]).

While most ransom demands and payments have been for relatively small amounts (USD 10 000 to 30 000 (NetDiligence, 2018[30]), (NAS Insurance, 2019[101]), (BakerHostetler, 2019[59])), 2018 and 2019 have witnessed a shift towards targeted attacks on more critical information technology assets and much more significant ransom demands (Iram, 2019[102]). A number of companies reported an increase in ransom demands to more than USD 50 000 with a handful of demands reaching USD 1 million or more (and some being paid) (BakerHostetler, 2019[59]), (Beazley, 2019[31]), (NAS Insurance, 2019[101]), (Burns, 2018[100]). In 2019, municipal governments (and local government services) have been particularly targeted (966 government agencies in the United States in 2019, according to one report (Emsisoft, 2019[103])). As a result, some insurance companies have reportedly begun examining their exposure to ransomware and considering possible coverage limitations and/or premium increases (Barlyn, 2020[104]).

A global contagious ransomware scenario developed by the public-private Cyber Risk Management (CyRiM) project estimated that total economic losses of USD 85 billion to USD 193 billion (depending on level of severity) could be incurred, including USD 200 to USD 400 million in insured cyber extortion costs (Cambridge Centre for Risk Studies, Lloyd's of London and Nanyang Technological University, 2019[105]).

However, public policy and regulation has implications for one of the expenses commonly incurred in cyber extortion attacks – the payment of ransoms to the perpetrators of the attack. In some jurisdictions, ransom payments could be considered inconsistent with public policy as such payments could encourage further extortion attempts. Some countries, such as Australia and the United States, have explicit policies against paying ransoms (Wesson, 2015[106]). Other countries, including Brazil, Colombia, Italy, Portugal and Russia, specifically prohibit insurance coverage and/or indemnification for kidnapping (and related ransom payments). In Portugal and Russia, this prohibition applies only to the kidnapping of persons, not cyber extortion. In Germany, where guidance has been issued to ensure that kidnap and ransom insurance practices are consistent with public policy, the German Financial Supervisory Authority (BaFin) has issued a specific clarification indicating that the reimbursement of ransom payments related to cyber-extortion is permitted (Schaloske and Feldmann, 2017[107]) – but cannot be advertised. In France and Japan, there are no explicit restrictions on reimbursing the costs of ransoms paid as a result of cyber extortion although such payments might be considered counter to public order and coverage for ransom payments may not be included in cyber insurance policies.

Many of the policies reviewed provided explicit coverage for ransom payments, sometimes with conditions related to insurability or legality:

- Among the eight reviewed cyber insurance policies offered in Australia, all provided explicit coverage for ransom payments, although three applied a condition related to either the insurability of those payments or the consistency of payments with local legal requirements;

- For Canada, all of the reviewed policies explicitly included coverage for ransom payments (although the specific policy wordings were not available to examine whether any conditions were applied);
- In the United Kingdom, all of the policies reviewed provided explicit coverage for ransom payments with one policy applying a condition on where such coverage is insurable;
- In the United States, there was sufficient information available to find explicit coverage for ransom payments for six of the policies reviewed (full policy wordings were not generally available);
- The two policies reviewed that offered coverage across Europe also provided explicit coverage for ransom payments (although full policy wordings were not available).

In addition to general public policy or regulatory impediments to reimbursing ransom payments, the anonymity of the perpetrators of cyber extortion attacks could also limit the ability of insurers to reimburse ransom payments in cases where the perpetrators could potentially be persons or entities subject to sanctions. Sanctions may be imposed by the United Nations or individual jurisdictions (as supplemental sanctions) and may involve broad restrictions that apply to countries as a whole or to specific listed individuals. The sanctions imposed might involve restrictions on trade in goods and services or providing financing or financial assistance.

Insurance companies apply an exclusion for the payment of any claim that would violate sanctions policy across a number of lines of business. There are a variety of market and company-specific exclusion clauses, but many are similar to a standard Lloyd's Market Association sanctions clause (LMA 3100) – "*No (re)insurer shall be deemed to provide cover and no (re)insurer shall be liable to pay any claim or provide any benefit hereunder to the extent that the provision of such cover, payment of such claim or provision of such benefit would expose that (re)insurer to any sanctions, prohibition or restriction under United Nations resolutions or the trade or economic sanctions, laws or regulations of the European Union, United Kingdom or United States of America*" (a more recent version also includes trade or economic sanctions, laws or regulations of Australia) (Wragg, 2015[108]). Many of the cyber insurance policies reviewed, across all jurisdictions where policy wordings were available, applied a similar sanctions exclusion clause (with some differences in terms of the list of countries whose sanctions would be recognised).

In the context of cyber extortion, the sanctions imposed on terrorist organisations (Al-Qaeda, ISIL/Daesch) and specific countries (North Korea, Russia) might be relevant based on the attribution of past events (see Box 3.4).[28] A key challenge for insurance companies' ability to apply restrictions on making payments that benefit sanctioned entities may be the difficulty in attributing cyber extortion attacks. A number of recent ransomware attacks have been attributed to specific entities or countries by official sources.[29] However, other wide-ranging ransomware campaigns have been more challenging to attribute. For example, attribution of the Ryuk ransomware, which has been among the costliest ransomware attacks in terms of ransom payments, has been the subject of debate among cyber security firms (Fokker and Beek, 2019[109]), (Arghire, 2019[110]), (Brewster, 2019[111]). Clear attribution remains subject to a number of challenges, including the possibility that the underlying code, which is often used to compare one attack with past incidents for the purpose of attribution, has been copied or intentionally manipulated (O'Brien, 2018[112]).

Market developments and perspectives on improving consistency in the types of cyber losses covered

Almost all of the (re)insurance underwriters and intermediaries consulted indicated that there has been a significant increase in the level of consistency of terminology, coverage terms and conditions offered in cyber insurance policies in recent years. A number of market providers, especially smaller insurers and new entrants, offer policies developed by intermediaries, other insurers or reinsurers (often combined with proportional reinsurance) which has had a positive impact on reducing differences in policy language. In

the United States, the Insurance Services Office (ISO) has developed a standardised cyber insurance policy form for SMEs and a menu-based policy form for larger commercial entities (Verisk Analytics, n.d.[113]) which is available (approved) in at least 42 states (ISO, 2018[114]). The German Insurance Association (GDV) has developed a standard cyber insurance policy form for SMEs which is reportedly used by 50% of insurance companies.

Most market participants are aware of the need to develop greater consistency in terminology although are concerned that any requirement for standardisation could stifle innovation. New coverages, conditions and exclusions are being applied continuously as new policyholder needs emerge (e.g. bricking) or as new (potentially uninsurable) risks arise. In some cases, coverage is changing on an annual basis (Blosfield, 2019[55]).

Fines and penalties

Insurers and reinsurers operating in the US market seem to have a fairly clear understanding of which types of fines and penalties are insurable (and in which states, as insurability varies across states). The practice of filing policies in each state where the policy is offered was identified by some as a means to ensure clarity on this issue as states where fines are not insurable will not approve a policy that provides coverage for fines.

However, in the European Union, there is confusion about the insurability of fines imposed under the GDPR. The GDPR does not explicitly state whether fines are insurable and most national privacy regulators have not provided any clarity. The possibility that some GDPR fines would be considered criminal fines seems to be one source of the confusion. There also appears to be confusion about the insurability of regulatory fines in many Asian countries. Most (re)insurance companies indicated that they would aim to reimburse fines and penalties where allowed, unless the reimbursement of the fine would create reputational risks for the (re)insurer.[30]

There were differing views on whether fines that are uninsurable in the jurisdiction where they are imposed could (or would) be reimbursed to a policyholder in another jurisdiction where reimbursement of fines is permitted. Some insurance companies suggested that reimbursement in a favourable jurisdiction is a relatively common practice while others indicated that they would be reluctant to reimburse a fine anywhere if the imposing jurisdiction did not allow a reimbursement.

In general, and particularly outside the United States, there was limited experience with claims for fines and penalties as many jurisdictions have only begun imposing fines for breaches of privacy regulation and the fines have often been a small share of the overall cost of responding to a privacy breach. However, as noted in Box 3.2, many privacy regulators have been given the authority to impose more large fines and some recent fines have been significant.

Ransom payments

Most insurance companies indicated that they (or the responsible underwriters) were aware of where ransom payments are not insurable. However, discussions with insurance companies suggested that their might be some lack of clarity.[31]

Among some insurance companies, it is generally understood that restrictions on payments to sanctioned entities apply not only to payments made by policyholders (direct payments) but also to reimbursements of ransom payments made by insurers (indirect payments). For example, in its guidance on the use of sanctions clauses by its syndicates, Lloyd's indicates that for sanctions involving asset freezes, the "insurer (and/or the broker) may not be able, directly or indirectly, to make payments to or for the benefit of, or receive payments from, the individual or entity designated under sanctions" (Wragg, 2015[108]). Similarly, a brief on sanctions compliance by Munich Re from the perspective of a reinsurer indicates that the "reinsurer is obliged to vet all possible beneficiaries (insofar as they are known) who might profit from a payment by

the cedant in order to ascertain whether any relevant sanctions are in force" (Mayer, 2016[115]). The International Association of Insurance Supervisors has also noted that ransom payments made to a named terrorist organisation, for example, could be considered a violation of United Nations sanctions (a criminal offense in most countries).[32]

Many of the (re)insurance companies consulted during the development of this study clearly take into account the potential for sanctions restrictions to be applicable to insurance reimbursements of ransom payments (and recognised the inherent difficulty in ensuring that that ransom payments were not directed to sanctioned entities). However, this understanding (that sanctions restrictions might also be applicable to insurance reimbursements of ransom payments) does not appear to be universally shared by all insurance companies. Some of the companies consulted noted that they will often (if not always) consult law enforcement agencies as part of the response to extortion attempts and that decisions to make payments were made by the policyholder, not the insurance company.

As in the case of coverage for fines and penalties, in the absence of clear rules or guidance, the implementation of the sanctions exclusion clause would be at the discretion (based on the interpretation) of the insurer, potentially resulting in claims disputes and/or litigation. It would normally be up to the insurer to prove that the sanctions exclusion clause would apply (Wesson, 2015[106]).[33]

One particular area where this issue could arise is in the coverage for cyber-terrorism provided in many cyber insurance policies (across all regions reviewed). Many of the policies reviewed applied a general exclusion of terrorism (and war) losses although with cyber-terrorism carved-out of that exclusion. The definition of cyber terrorism included in these policies often captured all of the relevant types of incidents covered under the policy, including cyber extortion (where it should, by definition, be a breach of sanctions if a ransom payment were reimbursed).

The potential role of governments in improving consistency in the types of cyber losses covered

Insurance regulators and supervisors do not normally become involved in the development of standard policy language or terms and conditions – particularly not for policies targeting sophisticated corporate policyholders. However, as noted above, supervisors have a role in overseeing business conduct which, under IAIS Insurance Core Principle 19 on Conduct of Business, would normally include the ability to require companies to ensure that the information provided to potential policyholders is clear and drafted in plain language (IAIS, 2019[48]). If harmonisation of terminology, coverages and exclusions does not improve as the market develops, supervisors could consider whether additional guidance is required.

In the case of coverage for fines, penalties and ransoms, the insurance regulators and supervisors can support greater consistency by clarifying whether these losses are insurable in their jurisdiction (and/or under what conditions) – and encouraging insurance companies to reflect any national position on insurability in their policy language. As noted above, some regulators or supervisors have specifically provided clarity on the (un)insurability of fines and penalties and/or ransoms (e.g. Finland for fines and penalties). Where uninsurable, a clear statement could also reduce the possibility that coverage would be provided in another jurisdiction.[34]

A clear statement would, of course, require insurance regulators or supervisors to develop a position on the conditions for insurability. In the case of fines and penalties, the development of a position would have to consider whether fines and penalties unrelated to cyber incidents are insurable (and if unclear, provide clarity on all types of fines and penalties, not just those related to privacy breaches or cyber security requirements). As noted above, the main issues that will generally affect insurability across countries are the nature of the fine (criminal vs. civil/administrative) and the purpose of the fine (whether it is meant to

be punitive). Other considerations might include the degree of negligence of the affected policyholder or the degree of intent.[35]

Any further restriction on the insurability of fines and penalties would likely have some impact on the demand for cyber insurance coverage. One recent survey of insurance buyers (global, although mostly from the United States) found that coverage for fines and penalties was expected by a vast majority of policyholders (71%) and, for many, an explicit motivation for acquiring cyber insurance coverage (35%) (Advisen and Zurich North America, 2019[116]). It could also reduce the incentive for insurance companies from supporting and advising policyholders on compliance with privacy and cyber security regulations – although this would be mitigated as long as other costs of regulatory actions (such as required investigations) remained insurable.

In the case of ransom payments, the development of a position would have to consider the approach taken for ransom demands related to physical kidnapping. In general, countries that have taken a policy position against paying ransoms have done so to avoid contributing to the profitability of extortion – which is also a relevant consideration for cyber-extortion. There have been some suggestions that insurance reimbursements of ransom payments may be fuelling the rise in cyber-extortion and that (re)insurance companies may be incentivised to encourage ransom payments to avoid costly business interruption and data restoration claims (Dudley, 2019[117]) (which, according to one recent study, are usually multiples (23x) of the average ransom demand (Datto, 2019[118])). The involvement of (re)insurance companies might also potentially facilitate the ransom transaction by bringing in experts with experience in negotiating with extortionists and successfully meeting ransom demands. One report suggested that a public list of cyber insurance policyholders may have led to the targeting of some of those policyholders with cyber extortion demands (Dudley, 2019[117]).

The (re)insurance companies consulted are aware of these issues. It was noted that decisions on ransom payments were made by policyholders, sometimes in consultation with law enforcement. Many also noted their own reluctance to encourage policyholders to respond to ransom demands as there was no guarantee that the extortionist would restore access once payment was made while a ransom payment might encourage another attack against the policyholder in the future.[36] There was also a recognition that cyber-extortion is a (somewhat) avoidable loss if robust back-up procedures are in place. Partly as a result of these considerations, some companies will not provide coverage for ransom payments even where such coverage is allowed. However, it was also clear that (re)insurers would find it difficult to remove coverage for ransom payments unilaterally as they would lose business to others willing to provide that coverage.

A broad restriction on the reimbursement of ransom payments would allow (re)insurance companies to remove that coverage without being left at a competitive disadvantage – although there will continue to be scenarios where making a payment might provide the most desirable outcome (for example, in the case of a cyber-extortion attack against a hospital that limits access to critical patient records or against a municipal government that limits the availability of critical local government services)[37]. This would be consistent with the advice of law enforcement in many countries.[38]

Some have suggested that a set of criteria could be developed for when a ransom payment might be reimbursable – potentially linked to the likelihood of significant risks to life or property (Lubin, 2019[119]). Ultimately, the most effective approach would be a commitment by companies and governments to not pay ransoms. The United States Conference of Mayors passed such a resolution earlier this year (United States Conference of Mayors, n.d.[120]).

Where ransom payments remain insurable, there will be a need for greater clarity on whether insurance reimbursements of ransom payments to a sanctioned entity are illegal. As noted, (re)insurance companies have differing views on whether insurance reimbursements are subject to sanctions-related restrictions.

As in the case of fines and penalties, restrictions on ransom payments could reduce the incentive for insurance companies to support mitigation of this risk – which has been cited as an important benefit of

insurance coverage for cyber extortion (Marsh JLT Specialty, 2019[121]). However, insurers that provide coverage for other impacts of ransomware (business interruption, data restoration) would still have an interest in ensuring that policyholders are well-protected. Consideration would also need to be given to how any restriction on ransom payment insurability would impact SMEs, as SMEs are clearly targeted by ransomware attacks but might not have the resources to invest in ensuring proper back-up procedures. That said, allowing ransom payments to be insurable might also have negative implications for SMEs if ransom demands continue to rise (as described in Box 3.3) and insurers decide to limit the availability of full coverage for payments.

Box 3.4. Supporting consistency in cyber insurance coverage: recommendations

- Insurance regulators and supervisors should encourage the harmonisation of coverage definitions and exclusions applied to cyber risks and monitor the level of claims disputes that arise due to ambiguous policy language – while taking into account the risk that any forced standardisation could stifle innovations in coverage. If sufficient convergence is not achieved in the near-term, governments should encourage industry associations to develop standardised language for voluntary use.
- Governments should provide a clear statement on the insurability of fines, penalties and ransoms in their jurisdiction. Any decision limiting insurability should consider the possibility of exceptions for: (i) situations where the insured was not directly negligent (in the case of fines); and/or (ii) in the case of ransom payments, where the payment of a ransom is necessary to avoid significant harm to life or property. A consistent approach to these issues across jurisdictions would reduce the risk of insurers providing coverage for uninsurable losses on a cross-border basis and support a level-playing field for insurance providers and policyholders.
- Where ransoms payments are insurable, governments should clarify (or confirm) the responsibility of insurance companies for ensuring compliance with relevant sanctions. Insurance companies' implementation of international sanctions in the context of cyber-extortion claims may require increased attention in supervisory reviews.

References

Advisen and Zurich North America (2019), *2019 Information Security and Cyber Risk Management Survey*, Advisen and Zurich North America, https://www.advisenltd.com/2019-information-security-and-cyber-risk-management-zurich-cyber-survey/. [116]

AFP (2019), "EU adopts powers to respond to cyberattacks", *France24*, https://www.france24.com/en/20190517-eu-adopts-powers-respond-cyberattacks. [143]

AIG Europe (2016), *Behind the numbers: Key drivers of cyber insurance claims*, https://www.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/Insights/aig-claims-intelligence-cyber.pdf. [74]

Analytical Support and Sanctions Monitoring Team (2014), *Letter dated 27 October 2014 from the Chair of the Security Council Committee pursuant to resolutions 1267 (1999) and 1989 (2011) concerning Al-Qaida and associated individuals and entities addressed to the President of the Security Council (S/2014/770)*, United Nations Security Council, http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2014_770.pdf. [152]

Anthony, G. (2019), *Can English Law Insurance Policies Cover Fines Imposed Under GDPR?*, Squire Patton Boggs Insurance and Reinsurance Disputes Blog, https://www.inredisputesblog.com/2019/01/can-english-law-insurance-policies-cover-fines-imposed-under-gdpr/#page=1. [94]

Aon and DLA Piper (2019), *The Price of Data Security (Second Edition)*, Aon and DLA Piper, https://www.dlapiper.com/fr/france/insights/publications/2019/07/updated-guide-on-the-insurability-of-gdpr-fines-across-europe/. [72]

Aon and DLA Piper (2018), *The price of data security: A guide to the insurability of GDPR fines across Europe*, Aon and DLA Piper, http://www.aon.com/attachments/risk-services/Aon_DLA-Piper-GDPR-Fines-Guide_Final_May2018.pdf. [93]

Arghire, I. (2019), *Was North Korea Wrongly Accused of Ransomware Attacks?*, Security Week, https://www.securityweek.com/was-north-korea-wrongly-accused-ransomware-attacks. [110]

BakerHostetler (2019), *Managing Enterprise Risks in a Digital World: Privacy, Cybersecurity, and Compliance Collide (2019 Data Security Incident Response Report)*, BakerHostetler, https://f.datasrvr.com/fr1/419/17257/2019_BakerHostetler_DSIR_Final.pdf?cbcachex=990603. [59]

Bank of England Prudential Regulation Authority (2017), *Cyber insurance underwriting risk (Supervisory Statement SS4/17)*, Bank of England, https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2017/ss417.pdf. [49]

Barlyn, S. (2020), "Insurers look to curb ransomware exposure as U.S. cyber rates rise", *Reuters*, https://www.reuters.com/article/us-ransomware-insurance/insurers-look-to-curb-ransomware-exposure-as-u-s-cyber-rates-rise-idUSKBN1ZL1J2. [104]

Barlyn, S. and C. Cohn (2017), "Companies Without Cyber Cover Relying on Kidnap Insurance to Recoup Ransomware Losses", *Carrier Management*, https://www.carriermanagement.com/news/2017/05/19/167321.htm. [22]

Bear, D. (2018), "Court: Travelers Insurer Off the Hook in Florida Hotel Chain Data Breach Suit", *Insurance Journal*, https://www.insurancejournal.com/news/southeast/2018/11/21/509313.htm. [127]

Beazley (2019), *Beazley 2019 Breach Briefing*, Beazley, https://www.beazley.com/Documents/2019/beazley-breach-briefing-2019.pdf. [31]

Beazley (2018), *Beazley 2018 Breach Briefing*, Beazley, https://www.beazley.com/documents/Whitepapers/201802-beazley-breach-briefing.pdf. [29]

Bershidsky, L. (2019), "New world of cyberattacks: $100 million lawsuit against Zurich", *Property & Casualty 360*, https://www.propertycasualty360.com/2019/01/11/new-world-of-cyberattacks-100-million-lawsuit-against-zurich/?slreturn=20200125101417. [35]

Best, S. (2019), "Cybercriminals scam £200,000 out of energy firm by using AI to mimic CEO's voice", *Mirror Online*, https://www.mirror.co.uk/tech/cybercriminals-scam-200000-out-energy-19167075. [26]

Blosfield, E. (2019), "How to Turn Today's Confusion Into a Sustainable Cyber Insurance Market", *Insurance Journal*, https://www.insurancejournal.com/news/national/2019/03/26/521646.htm. [55]

Breakspear, B. et al. (2019), *It's no secret – $10 million penalties to be introduced for privacy law breaches*, McCullough Robertson, http://www.mccullough.com.au/2019/04/09/its-no-secret-10-million-penalties-to-be-introduced-for-privacy-law-breaches/. [89]

Brewster, T. (2019), "Mistaken For North Koreans, The 'Ryuk' Ransomware Hackers Are Making Millions", *Forbes*, https://www.forbes.com/sites/thomasbrewster/2019/02/20/mistaken-for-north-koreans-the-ryuk-ransomware-hackers-are-making-millions/#242e223875f4. [111]

Burgess, M. (2017), "Bad Rabbit ransomware: everything you need to know", *Wired*, https://www.wired.co.uk/article/bad-rabbit-ransomware-flash-explained. [150]

Burns, J. (2018), "The changing face of cyber claims", *Property Casualty 360*, https://www.propertycasualty360.com/2018/10/15/the-changing-face-of-cyber-claims/. [100]

Cambridge Centre for Risk Studies, Lloyd's of London and Nanyang Technological University (2019), *Bashe attack - Global infection by contagious malware (CyRiM Report 2019)*, Cambridge Centre for Risk Studies, https://www.lloyds.com/~/media/files/news-and-insight/risk-insight/2018/cyrimbasheattack_final.pdf. [105]

Capiscum Re (2019), *Cry cyber and let slip the dogs of war: Exploring the issues of attribution in the context of war and cyber*, Capiscum Re, https://www.capsicumre.com/wp-content/uploads/2019/07/Capsicum-Re-Cry-Cyber.pdf. [43]

Carrier Management (2019), "AIG Will Finalize Transition to Affirmative Cyber Coverage in January 2020", *Carrier Management*, https://www.carriermanagement.com/news/2019/09/06/197494.htm. [135]

CCRS and RMS (2017), *2017 Cyber Risk Landscape*, University of Cambridge Centre for Risk Studies and Risk Management Solutions, https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/crs-rms-cyber-risk-landscape-2017.pdf. [52]

CFC Underwriting (2018), *Cyber Insurance Guide*, CFC Underwriting, https://cfcunderwritingblog.com/wp-content/uploads/2018/07/Cyber-Guide_July-2018.pdf. [27]

CIAB (2019), *Cyber Insurance Market Watch Survey: Executive Summary (February 2019)*, The Council of Insurance Agents & Brokers, https://www.ciab.com/download/16876/. [8]

CIAB (2018), *Cyber Insurance Market Watch Survey: Executive Summary (July 2018)*, The Council of Insurance Agents & Brokers, https://www.ciab.com/download/15077/. [9]

CIAB (2017), *Cyber Insurance Market Watch Survey: Executive Summary (December 2017)*, The Council of Insurance Agents & Brokers, https://www.ciab.com/download/11984/. [10]

CIAB (2016), *Cyber Insurance Market Watch Survey: Executive Summary (April 2016)*, The Council of Insurance Agents & Brokers, https://www.ciab.com/wp-content/uploads/2017/04/2ndCyberMarketWatch_ExecutiveSummary_FINAL.pdf. [53]

Collins, S. (2019), "FM Global to charge for data cover and clarify cyber wordings", *Commercial Risk*, https://www.commercialriskonline.com/fm-global-charge-cyber-data-cover-clarify-wordings/. [137]

Congressional Research Service (2019), *Iran Sanctions*, Congressional Research Service, https://crsreports.congress.gov. [145]

CYBEREDGE Group (2019), *2019 Cyberthreat Defense Report*, CYBEREDGE Group, https://cyber-edge.com/wp-content/uploads/2019/03/CyberEdge-2019-CDR-Report.pdf. [154]

DAS UK Group (2018), *DAS Market Barometer: Cyber*, DAS UK Group and HSB Engineering Insurance. [6]

Datto (2019), *The Global State of the Channel Ransomware Report*, Datto, https://www.datto.com/resources/dattos-global-state-of-the-channel-ransomware-report. [118]

Deloitte Center for Financial Services (2018), *2019 Insurance Outlook: Growing economy bolsters insurers, but longer-term trends may require transformation*, Deloitte, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-dcfs-2019-insurance-industry-outlook.pdf. [1]

DLA Piper (2020), *DLA Piper GDPR Data Breach Survey (January 2020)*, DLA Piper, https://www.dlapiper.com/~/media/files/insights/publications/2020/01/dla-piper_data-breach-report-2020.pdf. [79]

Dudley, R. (2019), "The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks", *ProPublica*, https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks. [117]

Duffy, S., S. Slawe and J. Busta (2019), "Divergent State Privacy Laws Show Need For Federal Solution", *Mondaq*, http://www.mondaq.com/unitedstates/x/840000/Data+Protection+Privacy/Divergent+State+Privacy+Laws+Show+Need+For+Federal+Solution. [71]

EIOPA (2019), *Cyber Risk for Insurers – Challenges and Opportunities*, European Insurance and Occupational Pensions Authority, https://eiopa.europa.eu/Publications/Reports/EIOPA_Cyber%20risk%20for%20insurers_Sept2019.pdf. [44]

Emsisoft (2019), *The State of Ransomware in the US: Report and Statistics 2019*, Emsisoft Security Blog, https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/. [103]

ENISA (2012), *Incentives and barriers of the cyber insurance market in Europe*, European Network and Information Security Agency, https://www.enisa.europa.eu/publications/incentives-and-barriers-of-the-cyber-insurance-market-in-europe/at_download/fullReport. [11]

European Union (2019), *EU Sanctions Map*, European Union, https://sanctionsmap.eu/#/main. [142]

European Union (n.d.), *Regulation (EU) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, Official Journal of the European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 [92]

Europol (n.d.), *Tips & advice to prevent ransomware from infecting your electronic devices*, Europol Public Awareness and Prevention Guides, https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/tips-advice-to-prevent-ransomware-infecting-your-electronic-devices. [157]

Faulkner, M. (2020), "Lloyd's specifies further phases of 'silent' cyber crackdown", *Insurance Day*, https://insuranceday.maritimeintelligence.informa.com/ID1130229/Lloyds-specifies-further-phases-of-silent-cyber-crackdown. [158]

Faulkner, M. (2019), "Lloyd's moves to rein in 'silent' cyber exposures", *Insurance Day*, https://insuranceday.maritimeintelligence.informa.com/ID1127905/Lloyds-moves-to-rein-in-silent-cyber-exposures. [134]

FBI (2019), *2018 Internet Crime Report*, Federal Bureau of Investigation. [23]

FCA (2018), *FCA Handbook of rules and guidance: Chapter 6 (Insurance against financial penalties)*, http://www.handbook.fca.org.uk. [90]

Foggan, L. (2019), *Brief of Amici Curiae (United States Court of Appeals for the Eleventh Circuit, St. Paul Fire & Marine Ins. Co. v. Rosen Millennium, Inc.)*, Complex Insurance Claims Litigation Association and the American Property Casualty Insurance Association, https://www.huntoninsurancerecoveryblog.com/wp-content/uploads/sites/27/2019/03/Brief.pdf. [126]

Fokker, J. and C. Beek (2019), *Ryuk Ransomware Attack: Rush to Attribution Misses the Point*, McAfee Blogs, https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/ryuk-ransomware-attack-rush-to-attribution-misses-the-point/. [109]

Friedman, S. and A. Thomas (2017), *Demystifying cyber insurance coverage: Clearing obstacles in a problematic but promising growth market*, Deloitte, https://www2.deloitte.com/insights/us/en/industry/financial-services/demystifying-cybersecurity-insurance.htm. [13]

Friedman, S. and A. Thomas (2017), *Demystifying cybersecurity insurance*, Deloitte Insights, https://www2.deloitte.com/insights/us/en/industry/financial-services/demystifying-cybersecurity-insurance.html. [50]

FTC (2019), *Equifax Data Breach Settlement*, Federal Trade Commission, https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement. [67]

Godes, S. (2019), *Courts Favor Crime Coverage Of Email Hacks – For Now*, Barnes & Thornburg, https://btlaw.com/insights/publications/2019/courts-favor-crime-coverage-of-email-hacks---for-now. [19]

Greene, L. et al. (2019), *Part 3: Coverage Considerations Under CGL Policies for CCPA Violations*, Goldberg Segalla: The Insurance & Reinsurance Report, https://www.insurerereport.com/part-3-coverage-considerations-under-cgl-policies-for-ccpa-violations/. [97]

Harwell, D. (2019), "Artificial-intelligence voice is used in a theft", *The Washington Post*, https://www.washingtonpost.com/technology/2019/09/04/an-artificial-intelligence-first-voice-mimicking-software-reportedly-used-major-theft/. [25]

Hayashi, H. and R. Shimada (2019), *Japan: Data Protection 2018 (International Comparative Legal Guides)*, Global Legal Group, https://iclg.com/practice-areas/data-protection-laws-and-regulations/japan. [62]

Hiscox (2018), *Hiscox Cyber Claims Report 2018*, Hiscox, www.hiscoxgroup.com/sites/group/files/documents/2018-07/2018%20Cyber%20Claims%20Report%20Final_0.pdf. [28]

Howard, L. (2019), "Reinsurers Look at Cyber's Massive Growth Possibilities—With Caution", *Carrier Management*, https://www.carriermanagement.com/features/2019/10/18/199207.htm. [4]

IAIS (2019), *Insurance Core Principles and Common Framework for the Supervision of Internationally Active Insurance Groups (Updated November 2019)*, International Association of Insurance Supervisors. [48]

IAIS (2018), *Insurance Core Principles (Updated November 2018)*, International Association of Insurance Supervisors. [123]

International Association of Engineering Insurers (2018), *Endorsement- IMIA Cyber Exclusion 2018 (short version)*, International Association of Engineering Insurers, www.imia.com/wp-content/uploads/2018/09/Endorsement-IMIA-Cyber-Exclusion-2018-short-version-and-PD-BI-write-back-24-09-2018.pdf. [15]

Internet Crime Complaint Center (IC3) (2019), *High-Impact Ransomware Attacks Threaten U.S. Businesses And Organizations*, FBI Public Service Announcement, https://www.ic3.gov/media/2019/191002.aspx. [156]

Intersoft Consulting (n.d.), *General Data Protection Regulation (GDPR): Key Issues (Fines/Penalties)*, Intersoft Consulting, https://gdpr-info.eu/issues/fines-penalties/. [91]

Iole, J. and M. Divelbiss (2015), *Understanding "Fines and Penalties Coverage" Under Cyber Insurance*, Jones Day Blogs, https://www.jonesday.com/Understanding-Fines-and-Penalties-Coverage-Under-Cyber-Insurance-iInsurance-Policyholder-Advocatei-02-26-2015/. [95]

Iram, R. (2019), "How to underwrite 2019's emerging cyber risks", *Property Casualty 360*, https://www.propertycasualty360.com/2019/01/24/how-to-underwrite-2019s-emerging-cyber-risks/. [102]

ISO (2018), "Now Available in 42 States: ISO's Cyber Insurance Program", *Carrier Management*, https://www.carriermanagement.com/news/2018/03/26/177127.htm. [114]

IUA (2019), *IUA 09-081 Cyber Loss Absolute Exclusion Clause*, International Underwriting Association. [40]

IUA (2019), *IUA 09-082 Cyber Loss Limited Exclusion Clause*, International Underwriting Association. [41]

Jergler, D. (2019), "Cyber Alert: New Era in Privacy Liability to Begin. California's Data Privacy Law Could Be Game-Changer", *Insurance Journal*, https://www.insurancejournal.com/magazines/mag-features/2019/07/15/532104.htm. [83]

Johnson, K. (2018), "Lax Cyber Security Could Be Federal Law Violation, SEC Warns", *Insurance Journal*, https://www.insurancejournal.com/news/national/2018/10/17/504783.htm. [58]

Kadar, D. and L. Gaillard (n.d.), *First sanction decision rendered by the CNIL regarding data breaches worth almost 1 per cent of the company's yearly turnover: the era of tolerance seems to be over*, Reed Smith Technology Law Dispatch, https://www.technologylawdispatch.com/2019/06/privacy-data-protection/first-sanction-decision-rendered-by-the-cnil-regarding-data-breaches-worth-almost-1-per-cent-of-the-companys-yearly-turnover-the-era-of-tolerance-seems-to-be-over/#page=1. [88]

Kang, C. (2019), "Facebook Fine Could Total Billions if F.T.C. Talks Lead to a Deal", *The New York Times*, https://www.nytimes.com/2019/02/14/technology/facebook-ftc-settlement.html. [81]

King & Spalding (2019), *Biometric Data Regulations: Do Your Insurance Policies Cover This Emerging Risk?*, JDSupra, https://www.jdsupra.com/legalnews/biometric-data-regulations-do-your-17015/. [139]

Kovacs, E. (2018), *UK, Australia Blame Russia for Bad Rabbit, Other Attacks*, Security Week, https://www.securityweek.com/uk-australia-blame-russia-bad-rabbit-other-attacks. [151]

Kuehner-Hebert, K. (2019), "Surge in class-action lawsuits resulting from biometric privacy laws", *PropertyCasualty360*, https://www.propertycasualty360.com/2019/09/10/surge-in-class-action-lawsuits-resulting-from-biometric-privacy-laws-414-162784/. [69]

LaCroix, K. (2018), *Are GDPR Fines and Penalties Insurable?*, The D&O Diary, https://www.dandodiary.com/2018/11/articles/cyber-liability/gdpr-fines-penalties-insurable/. [99]

Lassalle, M. (2019), *Are administrative fines insurable in Luxembourg?*, International Law Office - Newsletters, https://www.internationallawoffice.com/Newsletters/Insurance/Luxembourg/NautaDutilh-Avocats-Luxembourg-S-rl/Are-administrative-fines-insurable-in-Luxembourg. [141]

Latham & Watkins LLP (2019), *High GDPR Fines: German Data Protection Authority Joins the Club*, Latham & Watkins LLP Global Privacy & Security Compliance Law Blog, https://www.globalprivacyblog.com/gdpr/high-gdpr-fines-german-data-protection-authority-joins-the-club/#page=1. [86]

Latham & Watkins LLP (2019), *UK Regulator Imposes Two Substantial Fines for GDPR Data Breaches*, Latham & Watkins LLP Global Privacy & Security Compliance Law Blog, www.globalprivacyblog.com/gdpr/uk-regulator-imposes-two-substantial-fines-for-gdpr-data-breaches/. [87]

Levine, M. and L. Ellis (2020), "Top social engineering insurance cases of 2019", *PropertyCasualty360*, https://www.propertycasualty360.com/2020/01/28/year-in-review-top-social-engineering-insurance-cases-of-2019-414-170514/. [132]

Levine, M. and L. Ellis (2019), *Zurich Invokes War Exclusion in Battle Over Coverage for NotPetya Attack*, Hunton Andrews Kurth, https://www.huntoninsurancerecoveryblog.com/2019/01/articles/cyber/zurich-invokes-war-exclusion-in-battle-over-coverage-for-notpetya-attack/#page=1. [34]

Levine, M. and J. White (2017), "Will Your Crime Insurance Cover Cyber?", *Risk Management*, http://www.rmmagazine.com/2017/11/01/will-your-crime-insurance-cover-cyber/. [131]

Lloyd's and Cyence (2017), *Counting the cost - decoding cyber exposure*, Lloyd's and Cyence, https://www.lloyds.com/~/media/files/news-and-insight/risk-insight/2017/cyence/emerging-risk-report-2017---counting-the-cost.pdf. [51]

Lloyd's Market Association (2018), *Cyber Risks and Exposures: Model Clauses - Class of Business Review*, Lloyd's Market Association, http://www.lmalloyds.com/AsiCommon/Controls/BSA/Downloader.aspx?iDocumentStorageKey=c3910476-c5d4-47b1-bf3c-8b7e12e08299&iFileTypeCode=PDF&iFileName=Cyber%20Clauses%20Review. [38]

Lloyd's Market Association (2016), *Cyber Act Exclusion (Casualty Treaty Reinsurance) - LMA5274*, Lloyd's Market Association. [18]

Lloyd's Market Association (2015), *Electronic Data Endorsement C*, Lloyd's Market Association, https://www.lmalloyds.com/AsiCommon/Controls/BSA/Downloader.aspx?iDocumentStorageKey=f980fbb6-52d3-4d3a-87c5-d63052a9266f&iFileTypeCode=DOC&iFileName=NMA2914A. [16]

Lloyd's Market Association (2015), *Electronic Data Endorsement D*, Lloyd's Market Association, https://www.lmalloyds.com/AsiCommon/Controls/BSA/Downloader.aspx?iDocumentStorageKey=c8992553-d64d-4fc6-8f71-39a668695ffb&iFileTypeCode=DOC&iFileName=NMA2915A. [17]

Lubin, A. (2019), "The Insurability of Cyber Risk", *SSRN Electronic Journal*, http://dx.doi.org/10.2139/ssrn.3452833. [119]

MacAneney, J., J. Pitblado and A. Proctor (2018), "New Opinions From Second and Sixth Circuit Courts Rock Phishing Loss Coverage Landscape", *PropertyCasualtyFocus*, https://propertycasualtyfocus.com/new-opinions-from-second-and-sixth-circuit-courts-rock-phishing-loss-coverage-landscape/. [130]

MamoTCV Advocates (2019), *Recent GDPR Fines Issued in Various Countries*, MamoTCV Advocates Legal Update, https://www.mamotcv.com/resources/news/recent-gdpr-fines-issued-in-various-countries. [85]

Marsh (2018), *GDPR Fines and Penalties: Insurability will Vary by Location, Policy Details, and More*, Marsh LLC, https://www.marsh.com/content/dam/marsh/Documents/PDF/UK-en/Marsh%20Cyber%20Insurability%20Report%20UK.pdf. [96]

Marsh JLT Specialty (2019), *Cyber Insurance is Supporting the Fight Against Ransomware*, Marsh JLT Specialty, https://www.marsh.com/us/insights/research/cyber-insurance-supporting-fight-against-ransomware.html. [121]

Matthews, L. (2019), "Toyota Parts Supplier Hit By $37 Million Email Scam", *Forbes*, https://www.forbes.com/sites/leemathews/2019/09/06/toyota-parts-supplier-hit-by-37-million-email-scam/#153cfb4e5856. [33]

Mayer, U. (2016), *The science of sanctions compliance*, Munich Re Topics, https://www.munichre.com/topics-online/en/economy/global-trends-and-politics/science-sanctions-compliance.html. [115]

McQuinn, A. and D. Castro (2019), *A Grand Bargain on Data Privacy Legislation for America*, Information Technology and Innovation Foundation, http://www2.itif.org/2019-grand-bargain-privacy.pdf?_ga=2.265788943.1616827105.1554987620-10636168.1553095341. [64]

Mondaq Business Briefing (2019), "FTC Enforcement Trends In Consumer Protection", *Advisen Cyber News*, www.advisen.com/tools/fpnproc/fpns/articles_new_20/P/331715253.html?rid=331715253&list_id=20. [76]

Mondaq Business Briefing (2019), "HHS: 2018 Was All-Time Record Year For HIPAA Enforcement", *Advisen Cyber News*, www.advisen.com/tools/fpnproc/fpns/articles_new_20/P/334273997.html?rid=334273997&list_id=20. [77]

Montes de Oca, R. and P. Bandeira (2019), "New privacy laws taking shape worldwide", *PropertyCasualty360*, https://www.propertycasualty360.com/2019/06/18/new-privacy-laws-taking-shape-worldwide-414-157334/. [63]

NAS Insurance (2019), *2019 Cyber Claims Digest: Analysis of 2018 Cyber Claims Data*, NAS Insurance, https://nasinsurance.com/wp-content/uploads/2019/03/2019NASCyberClaimsDigest.pdf. [101]

Navetta, D., J. Friedman and A. Ebrahem (2019), *Standing to be Dismissed – The U.S. D.D.C. Weighs in on "Actual Damage" in Data Breach Litigation*, Cooley cyber/data/privacy insights, https://cdp.cooley.com/standing-to-be-dismissed-the-u-s-d-d-c-weighs-in-on-actual-damage-in-data-breach-litigation/. [70]

NetDiligence (2019), *Cyber Claims Study: 2019 Report*, https://netdiligence.com/2019-cyber-claims-study-landing/. [75]

NetDiligence (2018), *Cyber Claims Study 2018*, NetDiligence, https://netdiligence.com/wp-content/uploads/2018/11/2018-NetDiligence-Claims-Study_Version-1.0.pdf. [30]

New York State Attorney General (2018), *A.G. Underwood Announces Record $148 Million Settlement With Uber Over 2016 Data Breach*, New York State Attorney General, https://ag.ny.gov/press-release/ag-underwood-announces-record-148-million-settlement-uber-over-2016-data-breach. [78]

Newman, L. (2019), "281 Alleged Email Scammers Arrested in Massive Global Sweep", *WIRED*, https://www.wired.com/story/email-scammer-global-takedown/ [24]

NorthStar Insurance Services (2018), *Commercial Crime Insurance: Key Considerations*, NorthStar Insurance Services: Our Blog, https://www.nsins.com/commercial-crime-insurance-key-considerations/. [20]

O'Brien, C. (2018), *Why is 'Attribution' Still the Focus Following Cyber Attacks?*, https://www.infosecurity-magazine.com/opinions/attribution-focus-attacks/. [112]

Oddy, A. (2018), *Sanctions Clauses in a Changing Sanctions Regime*, Herbert Smith Freehills, https://hsfnotes.com/fsrandcorpcrime/2018/10/19/sanctions-clauses-in-a-changing-sanctions-regime/#page=1. [153]

OECD (2020), *Insurance coverage for cyber-terrorism in Australia*, Organisation for Economic Cooperation and Development and Australian Reinsurance Pool Corporation. [45]

OECD (2019), *Insurance coverage for cyber-terrorism in Australia: an assessment of gaps and options*, Organisation for Economic Cooperation and Development and Australian Reinsurance Pool Corporation. [122]

OECD (2018), *Unleashing the Potential of the Cyber Insurance Market: Conference Outcomes*, OECD, http://www.oecd.org/daf/fin/insurance/Unleashing-Potential-Cyber-Insurance-Market-Summary.pdf. [5]

OECD (2017), *Enhancing the Role of Insurance in Cyber Risk Management*, OECD, http://www.oecd.org/daf/fin/insurance/Enhancing-the-Role-of-Insurance-in-Cyber-Risk-Management.pdf. [3]

Oehninger, S. and P. Moura (2019), *Equifax's Hefty $700M Bill is a Powerful Reminder to Close Cyber & D&O Coverage Gaps*, Hunton Insurance Recovery Blog, https://www.huntoninsurancerecoveryblog.com/2019/07/articles/cyber/equifaxs-hefty-700m-bill-is-a-powerful-reminder-to-close-cyber-do-coverage-gaps/#page=1. [98]

Office for Civil Rights (2018), *Anthem Pays OCR $16 Million in Record HIPAA Settlement Following Largest U.S. Health Data Breach in History*, Department of Health and Human Services, https://www.hhs.gov/about/news/2018/10/15/anthem-pays-ocr-16-million-record-hipaa-settlement-following-largest-health-data-breach-history.html. [80]

Office of Foreign Assets Control (2016), *North Korea Sanctions Program*, Department of the Treasury, https://www.treasury.gov/resource-center/sanctions/Programs/Documents/nkorea.pdf. [144]

Office of the Australian Information Commissioner (OAIC) (n.d.), *Privacy law*, Australian Government, https://www.oaic.gov.au/privacy-law/. [61]

Office of the Privacy Commissioner of Canada (2019), *Privacy Commissioner finds Equifax safeguards "unacceptable" and will monitor company for six years following major data breach*, Office of the Privacy Commissioner of Canada: News release, https://www.priv.gc.ca/en/opc-news/news-and-announcements/2019/nr-c_190409 . [66]

Office of the Privacy Commissioner of Canada (n.d.), *Summary of privacy laws in Canada*, Office of the Privacy Commissioner of Canada, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/. [60]

Orbis Research (2018), *Global Cyber Security Insurance Market 2018*, https://www.reuters.com/brandfeatures/venture-capital/article?id=36676. [2]

Partner Re and Advisen (2019), *Cyber Insurance - The Market's View*, Partner Re and Advisen. [47]

Partner Re and Advisen (2018), *2018 Survey of Cyber Insurance Market Trends*, Partner Re and Advisen, https://partnerre.com/wp-content/uploads/2018/10/2018-Survey-of-Cyber-Insurance-Market-Trends.pdf. [7]

Partner Re and Advisen (2017), *2017 Survey of Cyber Insurance Market Trends*, Partner Re and Advisen, https://partnerre.com/wp-content/uploads/2017/10/PartnerRe-2017-Survey-of-Cyber-Insurance-Market-Trends.pdf. [125]

Ponemon Institute LLC (2017), *2017 Global Cyber Risk Transfer Comparison Report*, Ponemon Institute LLC, www.aon.com/attachments/risk-services/cyber/2017-Global-Cyber-Risk-Transfer-Report-Final.pdf. [14]

Prime Minister of Australia (2018), *Attribution of a pattern of malicious cyber activity to Russia*, Government of Australia, https://www.pm.gov.au/media/attribution-pattern-malicious-cyber-activity-russia. [149]

Raskin, J. (2019), *Consider Enhancing Cyberliability Insurance Policies to Align with CCPA: Part 1*, Morgan Lewis Health Law Scan, https://www.morganlewis.com/blogs/healthlawscan/2019/09/consider-enhancing-cyberliability-insurance-policies-to-align-with-ccpa-part-1#page=1. [138]

Reeve, T. (n.d.), *Cyber insurance not trusted by business, KPMG claims*, SC Media, https://www.scmagazineuk.com/cyber-insurance-not-trusted-business-kpmg-claims/article/1478868. [54]

Rennack, D. and C. Welt (2019), *U.S. Sanctions on Russia: An Overview*, Congressional Research Service, http://www.crs.gov|7-5700. [146]

Reseller Middle East (UAE) (2019), "Rising phishing threats push businesses to rethink security priorities: report", *Advisen Cyber News*, http://www.advisen.com/tools/fpnproc/fpns/articles_new_20/P/332916091.html?rid=332916091&list_id=20. [32]

Reyneri, R. (2019), *California Supreme Court Case to Address Scope of TCPA Insurance Coverage*, Covington & Burling LLP, https://www.insideprivacy.com/advertising-marketing/tcpa/california-supreme-court-case-to-address-scope-of-tcpa-insurance-coverage/. [129]

Rosemain, M. (2019), "France Fines Google $57M for Breaching EU's Data Privacy Rules Under GDPR", *Insurance Journal*, https://www.insurancejournal.com/news/international/2019/01/23/515593.htm). [84]

Saunt, R. (2019), "Half a million British Airways customers told they can sue the airline over data breach", *Daily Mail Online*, https://www.dailymail.co.uk/news/article-7539707/Half-million-British-Airways-customers-told-sue-airline-data-breach.html. [73]

Saxena, A. (2019), "Equifax says US regulators seek damages related to 2017 breach", *Reuters*, https://www.reuters.com/article/uk-equifax-cyber/equifax-says-us-regulators-seek-damages-related-to-2017-breach-idUSKCN1QB24R. [65]

Schaloske, H. and K. Feldmann (2017), *German Financial Supervisory Authority allows coverage of ransom payments in cyber policies*, Clyde & Co., https://www.clydeco.com/insight/article/german-financial-supervisory-authority-allows-coverage-of-ransom-payments-i. [107]

Schiffer, L. (2019), *A Brief Review of What's Happening in TCPA Insurance Coverage Cases from TCPAWorld*, Squire Patton Boggs Insurance and Reinsurance Disputes Blog, https://www.inredisputesblog.com/2019/06/a-brief-review-of-whats-happening-in-tcpa-insurance-coverage-cases-from-tcpaworld/#page=1. [140]

Schiffer, L. (2019), *War (Exclusions), What Is It Good For?*, Squire Patton Boggs Insurance and Reinsurance Disputes Blog, https://www.inredisputesblog.com/2019/07/war-exclusions-what-is-it-good-for/#page=1. [133]

Securities and Exchange Commission (2018), *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, Federal Register, https://www.sec.gov/rules/interp/2018/33-10459.pdf. [57]

Shepardson, D. (2019), "U.S. Announces $5 Billion Fine Against Facebook, Other Privacy Settlement Terms", *Insurance Journal*, https://www.insurancejournal.com/news/national/2019/07/24/533779.htm. [82]

Shooter, S. (2019), *The Cookie Crumbles: cyber insurance dust-up over denial of cover*, https://www.twobirds.com/en/news/articles/2019/global/the-cookie-crumbles-cyber-insurance-dust-up-over-denial-of-cover. [36]

Simpson, A. (2016), "Federal Court Rules CGL Insurance Covers Data Breach", *Insurance Journal*, https://www.insurancejournal.com/news/national/2016/04/12/404881.htm. [128]

Skidmore, M. (2018), *Kidnap Ransom Insurance: Unlocking Coverage for Ransomware Attacks*, Haynes Boone, http://www.haynesboone.com/alerts/kidnap-ransom-insurance-unlocking-coverage-for-ransomware. [21]

Soylu, M. and B. Oztoprak (2019), "A Case Study In Data Breaches - Uber's Data Security Breach Fines Reach USD 150 Million - Data Protection - Turkey", *Mondaq*, http://www.mondaq.com/turkey/x/768680/data+protection/A+Case+Study+In+Data+Breaches+Ubers+Data+Security+Breach+Fines+Reach+Usd+150+Million. [68]

Spoerry, L. (2019), "Lloyd's cyber underwriters look to solve war exclusion problem", *Insurance Day*, https://insuranceday.maritimeintelligence.informa.com/ID1125536/Lloyds-cyber-underwriters-look-to-solve-war-exclusion-problem. [42]

Swiss Re and IBM Institute for Business Value (2016), *Cyber: in search of resilience in an interconnected world*, Swiss Re and IBM Institute for Business Value, https://www.swissre.com/dam/jcr:30b64544-9514-4389-aaf1-13fb74f51eab/ZRH-16-09789-P1_Cyber+Publication_web.pdf. [12]

Thanawala, S. (2019), "Georgia County Ransomware Attack Highlights Cyber Exposures to Local Agencies", *Insurance Journal*, https://www.insurancejournal.com/news/southeast/2019/10/23/546298.htm. [155]

The Geneva Association (2019), *New Geneva Association and IFTRIP task force to address emerging cyber terror risks*, The Geneva Association, https://www.genevaassociation.org/news/ga-news-press-releases/new-geneva-association-and-iftrip-task-force-address-emerging-cyber. [46]

The White House (2018), *Statement from the Press Secretary - Foreign Policy*, The White House, https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/. [147]

The White House (2017), *Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea*, The White House, https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/. [148]

Thomas, J. (ed.) (2018), *New Appleman on Insurance Law (Library Edition): Volume 2*, Lexis Nexis. [124]

United States Conference of Mayors (n.d.), *Resolutions - United States Conference of Mayors*, United States Conference of Mayors, https://www.usmayors.org/the-conference/resolutions/?category=a0D4N00000FCb3LUAT&meeting=87th%20Annual%20Meeting. [120]

Verisk Analytics (n.d.), *ISO Cyber Risk Solutions*, Verisk Analytics, https://www.verisk.com/insurance/products/iso-cyber-risk-solutions/. [113]

Voreacos, D., K. Chiglinsky and R. Griffin (2019), "Merck Cyberattack's $1.3 Billion Question: Was It an Act of War?", *Bloomberg*, https://www.bloomberg.com/news/features/2019-12-03/merck-cyberattack-s-1-3-billion-question-was-it-an-act-of-war. [37]

Wesson, C. (2015), *Kidnap and ransom insurance: Don't wait until you need it!*, Clayton Utz, www.claytonutz.com/knowledge/2015/october/kidnap-and-ransom-insurance-don-t-wait-until-you-need-it. [106]

Willis Towers Watson (2019), *2019 Silent Cyber Risk Outlook*, Willis Towers Watson, https://www.willistowerswatson.com/en-GB/Insights/2019/08/silent-cyber-risk-concerns-decline-after-2018-spike. [39]

Wood, C. (2019), "Allianz to address silent cyber with updated policy wordings", *Reinsurance News*, https://www.reinsurancene.ws/allianz-to-address-silent-cyber-with-updated-policy-wordings/. [136]

Wragg, A. (2015), *Lloyd's Sanctions Guidance – Sanctions Clauses (Market Bulletin Y4832)*, Lloyd's of London, https://www.lloyds.com/~/media/files/the-market/communications/market-bulletins/2014/10/y4832.pdf. [108]

Wraight, P. (2019), "Cyber Coverage Confusion", *Insurance Journal*, https://www.insurancejournal.com/blogs/academy-journal/2019/09/05/538987.htm. [56]

Notes

[1] As noted below, different insurers might use different terminology or classifications to describe the types of incidents covered in cyber insurance policies.

[2] While cyber insurance coverage does not generally reimburse losses related to physical damage, coverage for "bricked" devices (i.e. hardware rendered useless due to malware infection) is increasingly offered.

[3] www.oecd.org/finance/insurance/2018-oecd-conference-cyber-insurance-market.htm).

[4] Responses to the questionnaire were received from Argentina, Austria, Belgium, Bermuda, Brazil, Chile, Colombia, Estonia, France, Germany, Italy, Japan, Latvia, Lithuania, Portugal, Russian Federation, Slovak Republic, Slovenia, South Africa, Switzerland, the United Kingdom and the United States.

[5] The share of survey respondents providing endorsements to these policies actually increased in 2018 relative to 2017 across most of these lines of business, which may be evidence that either cyber risks are increasingly being placed in other lines of business or, more likely, that cyber coverage is increasingly being provided on an affirmative (rather than silent) basis (as the survey also found an increasing use of stand-alone coverage over endorsements) (Partner Re and Advisen, 2017[125]), (Partner Re and Advisen, 2018[7]).

[6] The coverage disputes have generally focused on the coverage of losses resulting from privacy-related breaches under the coverage for personal and advertising injury liability that is included in standard commercial general liability policies in the United States. The disputes have focused on the definition of publication and whether the disclosure of private information in the possession of the insured as a result of data breach is an intentional act of publication by the insured (which would be covered). In at least three disputes involving unauthorised access to – and disclosure of – personal information by a third-party hacker, decisions have been in favour of the insurance company denying coverage (*Innovak International, Inc. v. The Hanover Insurance Co.*; *Zurich American Insurance Co. v. Sony Corporation of America*; *St. Paul Fire & Marine Ins. Co. v. Rosen Millennium, Inc.*) (Foggan, 2019[126]), (Bear, 2018[127]). In another case, which did not clearly involve a breach by a third party, the decision was in favour of the policyholder finding coverage for claims related to the release of confidential medical records (Simpson, 2016[128]). Some of these disputes were initiated before (and some after) the application of a confidential and personal information disclosure exclusion for such losses in standard ISO commercial general liability forms although it is not clear whether the policies in dispute applied that exclusion (or if it would have been effective in the case decided in favour of the policyholder). A further complexity may arise as the scope of privacy protection regulation expands beyond unauthorised disclosure of personal information to protect consumers against other related harms such as unwanted intrusion (see Box 3.1) (Reyneri, 2019[129]).

[7] Some individual companies have developed cyber fraud exclusions for use in crime/fidelity policies.

[8] The coverage disputes have generally focused on: (i) whether authorisation by an employee for the transfer of funds based on fraudulent instructions (i.e. social engineering) voids coverage for the losses; and (ii) the scope of coverage for computer fraud (which is often included in crime/fidelity policies). In most (but not all) recent litigation in the United States, disputes have (ultimately) been decided in the favour of policyholders as the fraudulent emails containing instructions for the fund transfer were deemed to be the proximate cause of the ultimate loss of funds, no matter the types of company processes in place for approving the payments. In these cases, computer fraud coverage - which appeared to be aimed at providing coverage for fraudulent transfers involving a network security breach - were interpreted broadly enough to find coverage for fraud perpetrated by email. However, one recent dispute involving similar circumstances and policy language was decided in favour of the insurance company denying coverage as the policyholder's failure to decline the fund transfer was deemed to be the proximate cause rather than the initial social

engineering calls and emails (MacAneney, Pitblado and Proctor, 2018[130]), (Levine and White, 2017[131]), (Levine and Ellis, 2020[132]).

[9] Some individual companies have developed cyber extortion exclusions for use in kidnap and ransom policies.

[10] None of the respondents to the OECD questionnaire indicated that there is a legislative, regulatory or supervisory requirement that terrorism or war incidents be excluded although some countries (e.g. Italy) have legislation that specifically allows insurance companies to exclude such risks.

[11] In one recent test of the scope of the war exclusion in the United States, an appellate court found that the generally understood meaning of "war" within the insurance sector as hostilities between *de facto* and *de jure* governments is applicable in coverage disputes (Schiffer, 2019[133]), suggesting that the strength of the link between a cyber attacker and a government could be a critical factor.

[12] In the Lloyd's market, all first party property damage policies that renew after 1 January 2020 will need to either provide affirmative coverage for – or exclude – cyber risks (and the same will apply to property catastrophe reinsurance from June/July 2020 and liability lines from 2021) (Faulkner, 2019[134]) (Faulkner, 2020[158]). AIG has committed to provide affirmative coverage or apply exclusions for physical and non-physical cyber risks across almost all commercial property and liability lines by January 2020 (Carrier Management, 2019[135]). Allianz has committed to clarify whether cyber risks are covered across property and casualty policies beginning with 2019 renewals (Wood, 2019[136]) and FM Global revised its commercial property policies to address silent cyber from July 2019 (Collins, 2019[137]).

[13] For example, in the United Kingdom commercial property market, less than 5% of policies applied the CL380 (cyber attack) exclusion although 75%-100% applied the NMA 2914 or 2915 (electronic data) exclusion. For liability lines, an estimated 0%-25% applied the CL380 (cyber-attack) exclusion to general liability and errors and omissions/professional indemnity policies (Lloyd's Market Association, 2018[38]).

[14] The report provides estimates by insurance companies of their exposure to cyber risk across different business lines (i.e. expected cyber claims in that business line as a share of all claims). The responses indicate that most insurers expect claims resulting from cyber incidents to account for less than 1% of all property and other liability claims. Estimates of cyber claim frequency in property policies has declined since 2017 although estimates for other liability lines has increased slightly (Willis Towers Watson, 2019[39]).

[15] The "absolute" exclusion would remove any coverage for "loss, damage, liability, expense, fines or penalties or any other amount" directly or indirectly caused by a cyber (computer, network or data) incident while the "limited" exclusion removes coverage for these types of losses if caused directly by a cyber incident.

[16] The reasons cited for not taking any action include: (i) it may be impractical to apply cyber exclusions to other types of policies; (ii) cyber exposure is not seen as a relevant threat; (iii) implementation of cyber exclusions are widely related to market dynamics; (iv) competitive impacts; and (v) a "wait-and-see" approach was being taken (EIOPA, 2019[44]).

[17] A 2018 survey found that, while most underwriters (54%) believed that property damage from cyber risks should be covered in property policies, 36% of underwriters (and 49% of surveyed brokers) thought it should be covered in cyber insurance policies (Partner Re and Advisen, 2019[47]). A survey of insurance buyers in 2019 found a slight preference for property damage from cyber incidents to be covered in cyber insurance policies rather than property policies (49% vs. 41%) (Advisen and Zurich North America, 2019[116]). A similar incongruity was found for fund transfer fraud as 74% of underwriters indicated the coverage should be provided in crime/fidelity policies while 17% thought it was best placed in cyber insurance policies (along with 38% of brokers) (Partner Re and Advisen, 2019[47]).

[18] For example, insurance coverage for various natural catastrophes must be included in residential and commercial property insurance coverage in France, Iceland, Spain and many Swiss cantons (along with terrorism coverage in France and Spain). Coverage for earthquake must be offered in residential property policies in Japan and California (United States) although policyholders can choose to opt-out of such coverage. In the United States, coverage for terrorism (including cyber-terrorism) must be offered in insurance policies across a number of business lines.

[19] Two countries that responded to the OECD questionnaire indicated that they require insurers to seek the approval (or non-objection) of insurance supervisors of policy forms providing coverage for cyber risks to corporate policyholders. In Argentina, the approval of the insurance supervisor (Superintendencia de Seguros de la Nación) must be sought for distributing all types of insurance products which includes a detailed review of the risks covered (in standard coverage and as endorsements). In Colombia, the financial sector supervisor (Superintendencia Financiera de Colombia) requires companies to seek prior authorisation of policy forms where an insurer intends to commence activity in a new line of business. In addition, in the United States, most state supervisors have broad authority to review and approve policy forms and prescribe policy provisions (Thomas, 2018[124]).

[20] A number of other countries (including Belgium, Bermuda and Germany) are specifically collecting information on non-affirmative coverage for cyber risks with some considering how that information might inform future regulatory or supervisory measures.

[21] A significant challenge related to excluding an incident based on the perpetrator is the ability to clearly attribute the source of a cyber-attack. This issue is discussed in the section on ransomware below.

[22] While not the focus of this report, there are a number of limitations within the terms and conditions of insurance policies that might lead to coverage denials (and disputes). For example, privacy protection legislation in the US state of California allows a private right of action where a company has not satisfactorily responded to a request from a consumer (i.e. to prevent harm) whereas many cyber insurance policies will only provide coverage for actions by the policyholders deemed to have caused an injury (Raskin, 2019[138]). Also in the United States, some insurers will exclude coverage for regulatory fines and penalties imposed under certain privacy (related) statutes, such as the Telephone Consumer Protection Act (TCPA) and state legislation protecting biometric data, either explicitly or based on the definitions used for covered regulatory investigations and fines (King & Spalding, 2019[139]), (Schiffer, 2019[140]).

[23] Including Belgium, Bulgaria, Cyprus, Denmark, Estonia, Hungary, Ireland, Lithuania, Luxembourg, Malta, Poland, Portugal, Slovenia, United Kingdom (under the Data Protection Act which complements the GDPR.

Note by Turkey: The information in this document with reference to “Cyprus” relates to the southern part of the Island. There is no single authority representing both Turkish and Greek Cypriot people on the Island. Turkey recognises the Turkish Republic of Northern Cyprus (TRNC). Until a lasting and equitable solution is found within the context of the United Nations, Turkey shall preserve its position concerning the “Cyprus issue”.

Note by all the European Union Member States of the OECD and the European Union: The Republic of Cyprus is recognised by all members of the United Nations with the exception of Turkey. The information in this document relates to the area under the effective control of the Government of the Republic of Cyprus.

[24] Including Belgium, Cyprus, Czech Republic, Denmark, Estonia, Germany, Hungary, Ireland, Latvia, Lithuania, Malta, Romania, Slovenia, United Kingdom.

[25] The California Insurance Code prohibits insurance coverage for fines and penalties imposed under the state’s Unfair Competition Law. The authority to impose CCPA fines and penalties is found in that legislation and therefore CCPA fines and penalties would also be deemed uninsurable.

[26] In Belgium, a penalty cannot be subject to an insurance contract although this only applies to criminal cases and regulations related to road traffic and transport.

[27] In some jurisdictions, insurance legislation or regulation may require that policies issued – or covering risk - within a jurisdiction must recognise the authority of courts within that jurisdiction in the context of any litigation or action against the insurer.

[28] For example, the European Union has imposed asset freezes and a prohibition on making funds available to a list of terrorist organisations as well as listed individuals and entities in Iran, North Korea and the Ukraine (including entities linked to governments and the military). North Korea is also subject to sanctions restricting financial assistance (including insurance) (European Union, 2019[142]). In May, the EU Council adopted a framework for imposing sanctions in response to cyber attacks that have a significant impact in the European Union (AFP, 2019[143]). The United States has imposed asset freezes (blocked property and interests in property) on categories of entities in North Korea

(including entities that are or are controlled by the Government of North Korea or the Workers' Party of Korea as well as entities engaged in money laundering or other illicit economic activity that involves or supports the Government of North Korea) (Office of Foreign Assets Control, 2016[144]); Iran (including entities involved in malicious cyber attacks as well as the Iran Revolutionary Guard) (Congressional Research Service, 2019[145]); and Russia (including intelligence and military intelligence agencies (FSB and GRU)) (Rennack and Welt, 2019[146]).

[29] The WannaCry ransomware, which infected networks around the world starting in May 2017, was attributed by the United States, United Kingdom, Australia, Canada, New Zealand, and Japan to North Korea (The White House, 2017[148]) – with other reports attributing the attack to a specific organisation with suspected links to the North Korean government (O'Brien, 2018[112]). The NotPetya malware, which infected networks around the world in June 2017, was attributed to the Russian military by the United States (as well as Australia, Canada and the United Kingdom) (The White House, 2018[147]). The BadRabbit ransomware, which mostly affected Ukrainian and Russian organisations in the media and transportation sectors in 2017, was also attributed ("with some certainty") to the Russian military by Australia and the United Kingdom (Prime Minister of Australia, 2018[149]), (Burgess, 2017[150]), (Kovacs, 2018[151]).

[30] Many of the (re)insurance companies suggested that, currently, their general aim is to demonstrate the value of cyber insurance as a form of coverage and that a positive response to claims was an important aspect of achieving that objective. Reputational risks could arise as the result of a reimbursement of a fine or penalty related to an egregious (and high-profile) act by the policyholder.

[31] For example, some (re)insurance companies had contradictory views as to whether ransom payments were insurable in country A – or did not seem aware of (relatively clear) restrictions on insurability in country B. It should be noted that many of the (re)insurance company representatives contacted had global responsibilities and so may not be aware of every country-specific restriction.

[32] This is consistent with a 2014 report of the Analytical Support and Sanctions Monitoring Team to the President of the United Nations Security Council which recommended that insurance companies be encouraged to apply a sanctions exclusion clause in kidnap and ransom policies in order to avoid contravening counter-terrorism sanctions (Analytical Support and Sanctions Monitoring Team, 2014[152]).

[33] For example, a recent marine insurance dispute in the United Kingdom established that the insurer must demonstrate not only a risk of exposure to a sanctions violation but that the payment of the claim would clearly breach an applicable law (Oddy, 2018[153]).

[34] There are potential level playing field issues inherent in the ability of only multinational companies to recover payments in a favourable jurisdictions – and in the ability of only insurance companies operating in another jurisdiction to offer such coverage.

[35] For example, the reimbursement of a fine imposed on a policyholder for a breach that occurred as the result of the negligence of a third party service provider (vicarious liability), a misunderstanding of the requirements of a new legal framework or due to a sophisticated attack by a nation-state-backed entity might be easier to accept (Lubin, 2019[119]).

[36] One recent study of companies affected by ransomware found that, among the 45% that paid the ransom, close to 40% did not gain access to their data after payment (CYBEREDGE Group, 2019[154]).

[37] For example, a number of ransomware attacks on municipal governments in the United States have led to disruptions to the dispatch systems for emergency services (Thanawala, 2019[155]).

[38] In the United States, the Federal Bureau of Investigation discourages the payment of ransoms for a number of reasons although the guidance recognises that "when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers" (Internet Crime Complaint Center (IC3), 2019[156]). In Europe, EUROPOL's tips and advice to prevent ransomware discourages the payment of ransoms and encourages consulting a website that can assist in decrypting data (Europol, n.d.[157]).

www.oecd.org/finance/insurance