Public

IAIS

INTERNATIONAL ASSOCIATION OF INSURANCE SUPERVISORS

ISSUES PAPER ON CYBER RISK TO THE INSURANCE SECTOR

DRAFT 25~~18~~ MAY 2016

About the IAIS

The International Association of Insurance Supervisors (IAIS) is a voluntary membership organisation of insurance supervisors and regulators from more than 200 jurisdictions in nearly 140 countries. The mission of the IAIS is to promote effective and globally consistent supervision of the insurance industry in order to develop and maintain fair, safe and stable insurance markets for the benefit and protection of policyholders and to contribute to global financial stability.

Established in 1994, the IAIS is the international standard setting body responsible for developing principles, standards and other supporting material for the supervision of the insurance sector and assisting in their implementation. The IAIS also provides a forum for Members to share their experiences and understanding of insurance supervision and insurance markets.

The IAIS coordinates its work with other international financial policymakers and associations of supervisors or regulators, and assists in shaping financial systems globally. In particular, the IAIS is a member of the Financial Stability Board (FSB), member of the Standards Advisory Council of the International Accounting Standards Board (IASB) and partner in the Access to Insurance Initiative (A2ii). In recognition of its collective expertise, the IAIS also is routinely called upon by the G20 leaders and other international standard setting bodies for input on insurance issues as well as on issues related to the regulation and supervision of the global financial sector.

Issues Papers provide background on particular topics, describe current practices, actual examples or case studies pertaining to a particular topic and/or identify related regulatory and supervisory issues and challenges. Issues Papers are primarily descriptive and not meant to create expectations on how supervisors should implement supervisory material. Issues Papers often form part of the preparatory work for developing standards and may contain recommendations for future work by the IAIS.

This document was prepared by the Financial Crime Task Force (FCTF).

This publication is available on the IAIS website (www.iaisweb.org).

Issues Paper on Cyber Risk to the Insurance Sector

Contents

I. Introduction

1. Concern over cybersecurity is growing across all sectors of the global economy, as cyber risks have grown and cyber criminals have become increasingly sophisticated. For insurers, cybersecurity incidents can harm the ability to conduct business, compromise the protection of commercial and personal data, and undermine confidence in the sector. The IAIS has noted that the level of awareness of cyber threats and cybersecurity within the insurance sector, as well as supervisory approaches to combat the risks, appear to vary across jurisdictions.

2. These factors prompted the IAIS to consider the area of cybersecurity in the insurance sector, including the involvement of insurance supervisors in assessing and promoting the mitigation of cyber risk.

3. While many of the most widely publicised cybersecurity incidents involving consumer data have affected retailers, companies in the financial services sector, including insurers, have been victimised as well.

4. All insurers, regardless of size, complexity, or lines of business, collect, store, and share with various third-parties (e.g., service providers, intermediaries, and reinsurers) substantial amounts of private and confidential policyholder information, including in some instances sensitive health-related information. Protection of the confidentiality, integrity, and availability of insurers' data is of fundamental importance. Information obtained from insurers through cyber crime may be used for financial gain through extortion, identity theft, misappropriation of intellectual property, or other criminal activities. Inadvertent or intentional eExposure of private data can potentially result in severe and lingering harm for the affected policyholders, as well as reputational damage to insurer sector participants. Similarly, malicious cyber attacks against an insurer's critical systems may impede its ability to conduct business.

5. In 2015, the IAIS surveyed its Members on their perceptions of insurance industry cyber risk, their involvement as regulators in combating cyber threats, and supervisory approaches to cybersecurity that are in useused or under development. Members' responses to the survey have provided input to this paper. Other inputs include consultations with various Members, insurers, cybersecurity professionals, and other experts, as well as literature cited in this paper. Additional resources are presented in Annex III.

6. The objectives of this Issues Paper are to raise awareness for insurers and supervisors of the challenges presented by cyber risk, including current and contemplated supervisory approaches for addressing these risks. As an Issues Paper, it provides background, describes current practices, identifies examples, and explores related regulatory and supervisory issues and challenges. This paper focuses on cyber risk to the insurance sector and the mitigation of such risks. It, but does not cover IT security risks more broadly, cyber insurance (insurers' selling or It also does not specifically address insurers' underwriting that type of insurance productof cyber risk (i.e., cyber insurance), or risks arising from cybersecurity incidents involving supervisors, which are important topics but not within the scope of this Issues Paper.

7. The paper is intended to be primarily descriptive and is not meant to create supervisory expectations. Nevertheless, the paper may shed light on the need for additional, more specific IAIS material to support supervisors in addressing cyber risk.

II. The Cyber Risk Landscape

8. There is no standardised definition of the term "cyber risk." The CRO Forum has broadly described "cyber risk" to mean: "Any risks that emanate from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks. It also encompasses physical damage that can be caused by cybersecurity incidents, fraud committed by misuse of data, any liability arising from data storage, and the availability, integrity and confidentiality of electronic information − be it related to individuals, companies, or governments."[1] Similarly, a working group of the Committee on Payments and Market Infrastructures and the International Organization of Securities Commissions has described cyber risk as follows: "The combination of the probability of an event occurring within the realm of an organisation's or person's information assets, computer and communication resources and the consequences of that event for an organisation or person."[2]

9. Various terms are used to describe adverse outcomes arising from cyber risk. These include "cyber attack," defined by the U.S. Federal Financial Institutions Examination Council (FFIEC) as: "attempts to damage, disrupt, or gain unauthorised access to a computer, computer system, or electronic communications network. An attack, via cyberspace, targeting an enterprise's use of cyberspace, for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment or infrastructure; or destroying the integrity of the data or stealing controlled information."[3] Relatedly, a "cyber incident" is defined by the FFIEC as "actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system or the information residing therein."[3]

10. In this paper, the phrase "cybersecurity incident" is used generally to include both cyber attacks and cyber incidents.

11. In its 2015 Global Risk Report, the World Economic Forum identified technological risks, in the form of data fraud, cybersecurity incidents, or infrastructure breakdown, as among the top ten risks facing the global economy.[4] Cyber risk was~~has been~~ identified as the fourth largest risk among surveyed insurers (and first among U.S. and U.K. insurers) in a 2015~~recent~~ report on industry perceptions of risk.[5]

[1] CRO Forum, *The Cyber Risk Challenge and the Role of Insurance,* paragraph 3 (December 2014), *available at* http://www.thecroforum.org/cyber-resilience-cyber-risk-challenge-role-insurance/.

[2] Committee of Payment and Market Infrastructure and International Organization of Securities Commissions, *Consultative Paper – Guidance on Cyber Resilience for Financial Market Infrastructures* (November 2015), *available at* http://www.bis.org/press/p151124.htm.

[3] FFIEC, *Cybersecurity Assessment Tool Glossary* (June 2015), *available at* http://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_App_C_Glossary_June_2015_PDF5.pdf.

[4] World Economic Forum, *Global Risks 2015* (2015), *available at* http://www3.weforum.org/docs/WEF_Global_Risks_2015_Report15.pdf.

[5] PWC and Centre for the Study of Financial Innovation, *Insurance Banana Skins 2015: The CSFI Survey of the Risks Facing Insurers,* paragraph 1 (July 2015), *available at* http://static1.squarespace.com/static/54d620fce4b049bf4cd5be9b/t/55dde0fce4b0dff05004146c/1440604412304/2015+Insurance+Banana+Skins+FINAL.pdf.

12. One insurer, Allianz, has identified the following top trends in the cyber risk landscape:[6]

- Increasing interconnectivity and "commercialisation" of cyber-crime driving greater frequency and severity of incidents, including data breaches;
- Data protection legislation will toughen globally. More notifications and significant fines for data breaches can be expected in the future;
- Business interruption (BI), intellectual property theft and cyber-extortion risks are increasing. BI costs could be equal to – or exceed – breach losses; and
- Vulnerability of industrial control systems poses significant threat.

13. For context, the remainder of this section of the Issues Paper outlines recently published data concerning the types, frequency, severity, and costs of cybersecurity incidents.

Types of Cybersecurity Incidents

~~14.~~ Cybersecurity incidents happen in a variety of ways, exemplified by the different ways that data breaches, the most reported type of cybersecurity incident, occur.[7] In a 2015 report,[8] Verizon concluded that most data breaches arose from one or more of the following causes~~as follows~~:

~~15. 28.5 percent of confirmed data breaches arose from~~ point-of-sale intrusions;

~~16. 18.8 percent from~~ crimeware (any form of malware used for criminal purpose);

~~17. 18.0 percent from~~ cyber espionage;[9]

~~18. 10.6 percent from~~ insider misuse; and

~~19. 9.4 percent from~~ web application attacks.

~~20.~~14. The remainder of cybersecurity incidents arose from miscellaneous errors, physical theft or loss, payment card skimmers, or distributed denial of service. These cybersecurity incidents, while often linked to data breaches, might also result in other forms of loss (e.g., theft of intellectual property).

~~21.~~15. Cyber extortion, usually accomplished through a form of crimeware known as "ransomware," is an increasingly common cybersecurity incident "in which hackers infiltrate computers belonging to a business or an individual, encrypt the data thereon, and then demand a payment to decrypt it."[10] Certain types of ransomware are very effective, and victims of such attacks cannot retrieve data without paying ransom unless they have made a backup copy of the

[6] Allianz Global Corporate & Specialty, *A Guide to Cyber Risk* (September 2015).

[7] Data breaches are "security violations in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorised to do so." *See*, *e.g.*, U.S. Department of Health and Human Services, Administration for Children and Families, *Information Memorandum: ACYF-CB-IM-15-04* (1 July 2015), *available at* http://www.acf.hhs.gov/programs/cb/resource/im1504.

[8] Verizon, *2015 Data Breach Investigations Report*, page 32 (2015).

[9] Cyber espionage is defined as: "Unauthorised spying by computer. The term generally refers to the deployment of viruses that clandestinely observe or destroy data in the computer systems of government agencies and large enterprises." PC Magazine, "Encyclopedia," *available at* http://www.pcmag.com/encyclopedia/term/64376/cyber-espionage.

[10] Devlin Barrett, "Paying Ransom to Hackers Stirs Debate," *Wall Street Journal* (9 November 2015).

data stored on media not subject to the ransomware attack.[11] ~~It has been reported that the ransom demanded generally is relatively low – usually between $200 and $10,000.~~[12]

Frequency, Severity, and Cost of Cybersecurity Incidents

~~22.~~16. The frequency of cybersecurity incidents is increasing. In the fall of 2014, the PricewaterhouseCoopers (PwC) annual global information security survey of corporate executives, which included 9,700 participants, reported that almost 43 million detected cybersecurity incidents occurred during the previous year – the equivalent of 100,000 attacks per day and a 48 percent increase over the number of incidents reported in the 2013 survey.[13] The number of cybersecurity incidents reported to the 2015 PwC survey increased by a further 38 percent year over year.[14] Moreover, the number of unreported or undetected cybersecurity incidents is likely far higher. Attacks through malware are increasingly prevalent:[15] it has been reported that, across all organisations globally, five malware attacks occur every second of every day, although not all are successful.[16]

~~23.~~17. Cybersecurity incidents occur at companies of all sizes. Small businesses, however, may be particularly vulnerable. In a 2015 survey by NetDiligence, for example, responding businesses with less than $50 million in revenues reported the most incidents (29 percent), followed closely by businesses with less than $2 billion in revenue (25 percent).[17]

~~24.~~18. The severity of data breaches, the most reported form of cybersecurity incident, varies by jurisdiction. Among the countries and organisations covered by a report from the Ponemon Institute (Ponemon), the average number of records lost or stolen per data breach ranges from approximately 19,000 to nearly 30,000, with the United States, India, and countries from the Arabian region experiencing the highest averages.[18]

---

[11] *Ibid.*

[12] ~~*Ibid.*~~

[13] PwC, *Managing Cyber Risk in an Interconnected World: Key Finding from The Global State of Information Security Survey 2015*, paragraph 7 (September 2014), *available at* https://www.pwc.ch/de/dyn_output.html?content.void=57078&collectionpageid=8240&containervoid=46459&comefromcontainer=true.

[14] PwC, *Turnaround and Transformation in Cybersecurity: Key Findings from The Global State of Information Security Survey 2016*, paragraph 2 (September 2015), *available at* http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html.

[15] "[Malware is] designed to secretly access a computer system without the owner's informed consent. The expression is a general term (short for malicious software) used to mean a variety of forms of hostile, intrusive, or annoying software or program code. Malware includes computer viruses, worms, Trojan horses, spyware, dishonest adware, ransomware, crimeware, most rootkits, and other malicious and unwanted software or programs." FFIEC, *Cybersecurity Assessment Tool Glossary*.

[16] Verizon, *2015 Data Breach Investigations Report*, page 21. The Verizon report notes that ~~M~~many of these malware attacks are stopped by "controls like firewalls, intrusion detection systems (IDS)/intrusion prevention systems (IPS), spam filters, etc."

[17] Net Diligence, *2015 Cyber Claims Study*, page 22 (2015).

[18] Ponemon Institute, *2015 Cost of Data Breach Study: Global Analysis*, page 8 (May 2015). 350 companies representing the following 11 countries participated in the study: United States, United Kingdom, Germany, Australia, France, Brazil, Japan, Italy, India, United Arab Emirates, Saudi Arabia, and Canada. Participating organisations experienced data breaches ranging from a low of approximately 2,200 to slightly more than 101,000 compromised records. As described in the next section, the "per record" cost of responding to data breaches also varies by country.

~~25.~~ 19. Cybersecurity incidents are also costly. The Center for Strategic and International Studies and McAfee, for example, have estimated that cyber crime costs the global economy more than $400 billion every year.[19]

~~26.~~ 20. Recently, Lloyd's and the University of Cambridge Centre for Risk Studies released a report analysing the financial losses associated with a hypothetical cyber attack on the U.S. power grid. The report predicted total losses of between $243 billion and more than $1 trillion, with insured losses of between $21.4 billion and $71.1 billion, depending on the severity of the power outage.[20]

~~27.~~ 21. Ponemon has concluded that the global average cost of a data breach in 2014 was $3.79 million, with a global average cost of $154 for each lost or stolen record. These costs vary geographically. For example, the average cost per record in the United States was $217, whereas the cost was $56 per record in India. Costs also varied by industry, with health-related firms ($363/record), education firms ($300/record), pharmaceutical firms ($220/record), and financial firms ($215/record) having the highest average costs associated with breaches. The retail industry's average cost per breached record has increased dramatically year-over-year, from $105/record in 2014 to $165/record in 2015.[21]

~~28.~~ 22. According to Ponemon, these costs can be viewed as falling into one of four categories: (i) detection and escalation; (ii) notification; (iii) ex-post response; and (iv) lost business. In 2013, 2014, and 2015, lost business – which includes unexpected customer turnover, reputation losses, and decreased goodwill – was the largest cost component associated with data breaches.[22]

[19] Center for Strategic and International Studies and McAfee, *Net Losses: Estimating the Global Cost of Cybercrime* (June 2014), *available at* http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf.

[20] Lloyd's of London, *Emerging Risk Report: Business Blackout – The Insurance Implications of a Cyber Attack on the U.S. Power Grid* (July 2015), *available at* https://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf. The report (which assumes that the U.S. Terrorism Risk Insurance Act would not be triggered) notes that the insured loss figures carry uncertainty of $5 billion or more due to ambiguities surrounding coverage and exclusions under various lines of business, e.g., property and all risk covers.

[21] Ponemon Institute, *2015 Cost of Data Breach Study: Global Analysis*, pages 1, 2, and 9 (May 2015). These results are based on a Ponemon survey of companies experiencing breaches of fewer than approximately 100,000 records.

[22] Ponemon Institute, *2015 Cost of Data Breach Study: Global Analysis*, paragraph 17 (May 2015).

III. Cyber Threats to the Insurance Sector

~~29.~~23. In general, the insurance sector faces cyber risk from both internal and external sources, including through third parties~~is vulnerable to cyber incidents~~. Insurers collect, process, and store substantial volumes of data, including personally identifiable information. Insurers are connected to other financial institutions through multiple channels, including investment, capital raising, and debt issuance activities. Insurers execute mergers and acquisitions and other changes in corporate structure that may affect cybersecurity. Insurers outsource a variety of services, which may increase, or in some cases decrease, exposure to cyber risk.

Examples of Cybersecurity Weaknesses Involving Insurers Recently Observed by IAIS Members

Missing or Incomplete Overview of the IT-Landscape

While all insurers should have an inventory of IT hardware and licensed software, even those maintaining such records on a current basis may not recognise the data flow between those IT systems, applications, and components. If data flows exist between systems with high levels of protection and systems with lower security levels, cyber criminals may be able to gain access to otherwise secure systems.

Inadequate Control Process Regarding User Privileges

There are typically two types of problems associated with user identity management: (1) the failure of controls within the allocation process of user rights, i.e., allowing users to have higher system privileges than warranted; and (2) the failure to recognise when an account no longer needs certain system privileges. Both types of failures could lead to insider abuse and exposure to cyber risks. Software products which can perform identity management checks on an automated basis are available.

Improper Access to Superuser Accounts

Direct employee access to “superuser” accounts (accounts with privilege levels far beyond those appropriate for most users) without sufficient controls presents risks to insurers. First, if a hacker gained access to any of the accounts held by the employees with access to the superuser account, the hacker could effectively control the entire system through the superuser account (including hiding criminal acts by modifying or deleting log files or by disabling detection mechanisms). Second, common use of superuser accounts could lead to unintended errors affecting the entire system.

~~30.~~24. Potential adverse consequences resulting from insurance sector cybersecurity incidents may include, for example: loss or corruption of confidential or sensitive business, consumer, or third-party data; disruption of business; physical loss (e.g., damage to hardware); financial loss; and reputational damage. Some of these ~~Potential adverse consequences of insurance sector cybersecurity incidents~~ are highlighted below.

Loss of Confidential Data

~~31.~~25. Personally identifiable information collected and stored by insurers, including personal health information of policyholders and, in some cases, of third parties, may include names, birthdates, social security numbers, street and email addresses, medical identification numbers, and employment data such as income. Private health records may be particularly valuable on black markets as tools for extortion, fraud, and identity theft, making insurers that collect such information high-value targets for criminals.

~~32.~~26. For commercial policyholders, insurers may collect sensitive business information that could be valuable to corporate and foreign spies. In the case of ~~certain lines such as~~ cyber insurance products, for example, insurers may possess information about a policyholder's network security controls and other cyber resilience information that could be valuable to hackers and other cyber criminals. Further, loss of confidential information could harm valuable intellectual property rights of a policyholder.

Disruption of Business~~Operations~~

~~33.~~27. Not all cybersecurity incidents involve data breaches; some cyber attacks can result in disruption to normal business operations. The cybersecurity incident on Sony Pictures, for example, was reported to have destroyed the company's entire network, including emails, telephone directories, voicemails, and business records such as contract templates.[23] Such a malicious attack on an insurer could result in significant harm to the firm and substantial recovery costs.

Reputational Damage~~Loss~~

~~34.~~28. The foundation of the insurance business is policyholder trust: trust that the information collected by insurers will be protected, and trust that claims will be paid out in a timely way when appropriate. If an insurer suffers a data breach, which exposes confidential policyholder information, that trust may be shaken. Similarly, if an insurer were to suffer a cybersecurity incident that rendered it unable to make timely claims payments or otherwise interrupted its operations, that trust may also be shaken. The reputational risk could extend to the insurance sector as a whole and adversely affect the confidence of consumers, policyholders, investors, rating agencies, and business partners.

[23] Amanda Hess, "Inside the Sony Hack," *Slate* (22 November 2015), *available at* http://www.slate.com/articles/technology/users/2015/11/sony_employees_on_the_hack_one_year_later.html.

IV. Examples of Cybersecurity Incidents in the Insurance Sector

~~35.~~29. The insurance sector has experienced a variety of cybersecurity incidents in recent years, including well-publicised data breaches at several U.S. health insurers. Some examples of these cybersecurity incidents are provided below.

~~36.~~30. In 2015, Anthem Blue Cross Blue Shield and Premera Blue Cross experienced data breaches in which credit card data and personally identifiable information, including health data, were compromised.[24] The breaches potentially exposed the personal information of up to 91 million policyholders – as many as a quarter of the people in the United States.[25] The insurers had to react swiftly to mitigate reputational damage and to minimise litigation costs, although it is currently unknown how much loss the insurers will ultimately incur due to this breach.

~~37.~~31. In another recent U.S. example, a data server operated by the state of North Dakota was compromised, potentially exposing a range of personal information related to workers compensation claimants – including 43,000 Incident Reports and 13,000 Payroll Reports that had been filed online by workers and employers. Reportedly, medical information and claim files were not exposed, but data at risk was said to include individuals' names, social security numbers, birth dates, descriptions of injury, descriptions of incidents, names of employers, and employer addresses.[26]

~~38.~~32. A group of cyber extortionists known as the "DD4BC" has been targeting a range of firms including financial institutions in Europe, Australia, Canada, and the United States with threats of distributed denial-of-service (DDoS)[27] attacks in order to extort money from them. DD4BC has demanded ransoms of varying amounts, to be paid in bitcoins (crypto-currency), threatening to launch DDoS attacks unless the target pays the ransom by a specified deadline. Two German insurance groups experienced this type of attack in mid-2015, receiving threats of a DDoS-attack on company web servers unless they paid 40 bitcoins. The insurers refused, as they assessed the extortionists would have caused only minor damage in those instances, but these incidents could have been far more serious if the attacks had concentrated on more critical systems~~intra-company connections~~.

~~39.~~33. In 2015, penetration testing performed by the internal audit team of an insurer in France found that unauthorised access to accounting tools had occurred. Although in this instance there were no further consequences, this cybersecurity incident could have had a substantial impact not only on the company but also on partners, service providers, and policyholders.

~~40.~~34. As a reminder that cybersecurity incidents can also include acts by insiders, an internal fraud was identified in 2012 in a French mutual insurance company. This fraud, resulting from an

[24] Anthem, Inc., *Statement Regarding Cyber Attack Against Anthem*, *available at* https://www.anthem.com/health-insurance/about-us/pressreleasedetails/WI/2015/1813/statement-regarding-cyber-attack-against-anthem; Premera Blue Cross, *Premera Targeted by Cyberattack* (17 March 2015), *available at* peter.cooke@bis.org.

[25] NAIC, *Cybersecurity Breach Response HQ*, *available at* http://www.naic.org/index_security_breach.htm.

[26] North Dakota Workforce Safety & Insurance, *Cyber-Attack on State Server May Impact WSI Information* (July 2015), *available at* https://www.workforcesafety.com/news/news-item/cyber-attack-on-state-server-may-impact-wsi-information.

[27] In a DDoS attack, an adversary directs a flood of illegitimate service requests to overwhelm the targeted computer or network in an attempt to make the resource unavailable to intended users, thereby seizing control of multiple systems by infecting them with malware. See Committee on Payments and Market Infrastructures and International Organization of Securities Commissions, *Consultative Paper – Guidance on Cyber Resilience for Financial Market Infrastructures* (November 2015), *available at* http://www.bis.org/press/p151124.htm.

internal data theft on a replicated environment with sensitive client information, led to a case of identity theft and false claims.

~~41.~~35. In the Netherlands, an insurer was recently subject to the so-called "CEO hack," a specific form of phishing cyber attack.[28] Pretending to be the CEO of a major and well-known commercial customer of the insurer, the criminals tried to persuade employees of the insurer to transfer money into a certain account. The criminals had apparently researched certain operational details of the insurer.

~~42.~~36. A recent report from PwC identified several additional cybersecurity incidents experienced by insurers in multiple jurisdictions, including attacks against personal lines, travel, health, and marine insurers.[29]

[28] This type of cyber attack has been observed as an emerging threat. See, e.g., U.S. Federal Bureau of Investigation, "Business E-Mail Compromise - An Emerging Global Threat," (28 August 2015), *available at* https://www.fbi.gov/news/stories/2015/august/business-e-mail-compromise/business-e-mail-compromise.

[29] PwC, *Under the Lens: Threats to the Insurance Sector* (November 2015).

V. Insurer Cyber Resilience

43.37. The varied challenges presented by cyber risk should be met with a broad response by insurers. Appropriately high-level management attention is a necessity, as is an effective governance structure able to understand, prevent, detect, respond to, and address cybersecurity incidents. In addition, a well-functioning risk management programme consistent with cyber resilience best practices should be in place and verified through supervisory review. As described below, this level of response is consistent with the Insurance Core Principles.

44.38. To be effective, cybersecurity needs to be addressed at all levels of an institution and with respect to relevant third-party arrangements. Generally, an effective cyber risk management programme includes ongoing process and control improvements, incident management procedures such as response and disaster recovery, appropriatestate-of-the-art network policies and procedures, rigorous management and control of user privileges, secure configuration guidance, appropriate malware protection procedures, consistent control of removable media usage, monitoring of mobile and home working procedures, and ongoing awareness and educational initiatives for all personnel.

45.39. For example, It is generally recognised that best practices for cyber resilience include:[30]

- Governance

  Together with the engagement and commitment of the Board and Senior Management, a proper cyber resilience framework contributes to the mitigation of cyber risk. For example, Senior Management should include an official with access to the Board, who is responsible for developing and implementing the cyber resilience framework, such as a Chief Information Security Officer.

- Identification

  Identification means identifying thosecritical business functions and processes that should be protected against compromise. Information assets (including sensitive personal information) and related system access should be part of the identification process. Regular reviews and updates are key factors, as cyber risk is constantly evolving and "hidden risks" can emerge. Connected entities are part of the whole picture; significance of the risks they pose is not necessarily proportionate to criticality of the particular service. For example, the well-known cyber attack against retailer Target involved entry via a ventilation service provider.[31]

- Protection

  Controls should be in line with leading technical standards. Resilience can be provided by design. Continued strong IT controls contribute to protection. Comprehensive protection

[30] U.S. National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity* (February 2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf; FFIEC, Cybersecurity Assessment Tool (June 2015), *available at* https://www.ffiec.gov/cyberassessmenttool.htm; Committee on Payments and Market Infrastructures and International Organization of Securities Commissions, *Consultative Paper – Guidance on Cyber Resilience for Financial Market Infrastructures* (November 2015), *available at* http://www.bis.org/cpmi/publ/d138.pdf .

[31] SANS Institute, *Case Study: Critical Controls that Could Have Prevented Target Breach* (5 August 2014), *available at* http://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412.

entails protecting interconnections and other means of access to insider and outsider threats to the institution. When designing protection, the "human factor" should be taken into consideration. Therefore, training is also an essential part of the safety net against cyber risk. Controls should be in line with leading technical standards, as strong IT controls contribute to protection. ~~The same degree of IT controls should be ensured for outsourced activities.~~

- Detection

  Continuous and comprehensive cybersecurity monitoring is essential for detection of potential cyber incidents~~Comprehensive cybersecurity monitoring is essential, and should include third party providers, because detection goes hand in hand with continuous monitoring~~. Performing security analytics also helps to detect and mitigate cyber incidents.

- Response and Recovery

  It is not always possible to detect or prevent cyber incidents before they happen, even with the best processes in place. For this reason, incident response planning is of great importance. Resumption of services (if interrupted) should be achieved within a reasonable timeframe, depending on the impact of the incidents and the criticality of the service. Contingency planning, design, and business integration as well as data integrity (also in the case of data sharing agreements) are key enablers for fast resumption. To make contingency planning effective, it should be subject to regular testing. Steps to prevent contagion can mitigate further risks. A disclosure policy should be in place in order to enhance crisis communication. Last but not least, forensic readiness is essential for deep dive investigations. Business continuity planning should consider these elements.

- Testing

  Testing programmes, vulnerability assessments, scenario-based testing, penetration tests, and red team tests are cornerstones in the testing phase. Cybersecurity testing should be included when systems are specified, developed, and integrated.

- Situational Awareness

  Awareness contributes to the identification of cyber threats. Accordingly, the establishment of a threat intelligence process helps to mitigate cyber risk. In this regard, insurers should consider participating~~e~~ in established information sharing initiatives.

- Learning and Evolving

  Insurers should continually revaluate the effectiveness of cybersecurity management. Lessons learned from cyber events and cyber incidents contribute to improved planning. New developments in technology should be monitored.

VI. Applicability of Insurance Core Principles to Cybersecurity

~~46.~~40. While the Insurance Core Principles (ICPs) do not specifically address cyber risk and cyber resilience, they provide a general basis for supervisors to address the insurance sector with respect to cyber risk and cyber resilience by requiring the management of significant risks and related internal controls~~.~~.

~~47.~~41. The ICPs that may be most relevant for the supervision of cyber risk in the insurance sector include:[32]

- ICP 7 (Corporate Governance)
- ICP 8 (Risk Management and Internal Controls)
- ICP 9 (Supervisory Review and Reporting)
- ICP 19 (Conduct of Business)
- ICP 21 (Countering Fraud in Insurance)

And, particularly regarding information exchange and supervisory cooperation, the following ICPs are relevant as well:

- ICP 3 (Information Exchange and Confidentiality Requirements)
- ICP 25 (Supervisory Cooperation and Coordination)
- ICP 26 (Cross-border Cooperation and Coordination on Crisis Management).

ICP 7 - Corporate Governance

~~48.~~42. ICP 7 was revised in November 2015. Under this ICP, insurers are expected to be able to demonstrate the effectiveness of systems and controls and corporate governance framework. The Guidance for this ICP states: "It is the Board's responsibility to ensure that the insurer has appropriate systems and functions for risk management and internal controls and to provide oversight to ensure that these systems and the functions that oversee them are operating effectively and as intended." Identifying and addressing cyber risk ~~to the insurance sector~~ should be an integral part of the risk management of an insurer.

ICP 8 - Risk Management and Internal Controls

~~49.~~43. ICP 8 was revised in November 2015. This ICP requires an insurer to have, as part of its overall corporate governance framework, effective systems of risk management and internal controls, including effective functions for risk management, compliance, actuarial matters, and internal audit.

~~50.~~44. ICP 8 Guidance lists a minimum set of categories that the risk management system should cover. With respect to cyber risk, the Guidance is relevant as it refers to "operational risk management," "conduct of business," and "other risk-mitigation techniques." In addition, the Guidance states that the risk management system should take into account all reasonably foreseeable and relevant material risks, including current and emerging risks.

~~51.~~45. The Guidance also describes typical components of an effective internal control system. Under the "policies and processes" that are listed as one of these components, the Guidance describes such internal control system as having "appropriate controls for all business processes

[32] Other ICPs, such as ICPs 16 (Enterprise Risk Management for Solvency Purposes) and 18 (Intermediaries), may also be relevant.~~(Insert a footnote on ICPs 16 and 18.)~~

and policies," including "critical IT functionalities," "access to databases" and to "IT systems by employees." This clearly encompasses cyber risk.

~~52.~~46. In addition, the Guidance calls for sufficient resources for control functions, including appropriate IT/management information systems.

~~53.~~47. Finally, ICP 8 Guidance states that the internal audit function should provide independent assurance to the Board and Senior Management in respect of matters including capacity and adaptability of the IT architecture to provide accounting, financial, and risk reporting information in a timely manner.

~~54.~~48. When entering into or revising an outsourcing arrangement, the Board and Senior Management should consider how the insurer's risk profile and business continuity will be affected by the outsourcing. This can apply to service provider's governance, risk management, and internal controls with respect to cyber risk.

ICP 9 - Supervisory Review and Reporting

~~55.~~49. ~~This~~ ICP 9 addresses the general processes and procedures supervisors should have in place with respect to supervisory review and reporting. These processes include analysing the supervisory framework for review and reporting, to ensure that it pays due attention to the evolving nature, scale, and complexity of risks which may be posed by insurers and of risks to which insurers may be exposed. Under this ICP, the supervisory framework should require an insurer to report promptly any material changes or incidents that could affect the insurer's condition or customers. As part off-site monitoring and on-site inspection supervisors should obtain sufficient information to assess and analyse the risks to which an insurer and its customers are exposed, and should review the effectiveness of the insurer's management of the risks. ICP 9 is currently under review.

ICP 19 - Conduct of Business

~~56.~~50. The requirements for the conduct of insurance business include provisions relating to privacy protection under which insurers and intermediaries are allowed to collect, hold, use, or communicate personal information of customers to third parties.

~~57.~~51. ICP 19 requires insurers and intermediaries to have policies and procedures for the protection of private information on customers. The Guidance describes a number of measures to ensure privacy protection and prevent security breaches, focusing on prevention of the misuse or inappropriate communication of personal information to third parties.

ICP 21 – Countering Fraud in Insurance

~~58.~~52. Under ICP 21, supervisors require that insurers and intermediaries take effective measures to deter, prevent, detect, report, and remedy fraud in insurance. Fraud in insurance may occur through cyber incidents. ICP 21 is currently under review, in part to consider whether it should be revised to address cyber risk more directly.

ICP 3, ICP 25, and ICP 26 - Information Sharing and Supervisory Cooperation

~~59.~~53. ICP 3 (Information Exchange and Confidentiality Requirements) is relevant because given the nature of cyber risk, it is possible that more than one jurisdiction would be involved in the identification, management, and mitigation of such risks. ICP 3 is currently under review.

~~60.~~54. The ability to share information with other jurisdictions – as set out in ICP 25 (Supervisory Cooperation and Coordination) – is an important tool for supervisors given the potential for a cyber incident to have cross-border impact. The ability of Supervisors to act quickly to identify, manage, and mitigate risks will be enhanced by having an efficient mechanism for information sharing. Such mechanisms might include bilateral or multilateral memoranda of understanding, such as the IAIS Multilateral Memorandum of Understanding (the global standard for information sharing among insurance supervisors), or other cooperation agreements, such as those established, for example, in relation to supervisory colleges. In addition, the IAIS survey results described in this paper suggest that most jurisdictions may benefit from sharing regulatory and supervisory initiatives pertaining to cybersecurity, notably on issues such as cyber education and training, and treatment of cyber risk with respect to outsourcing. ICP 25 is currently under review.

Examples of Cybersecurity Work of Other Global Financial Sector Standard Setting Organisations

Committee on Payments and Market Infrastructures (CPMI) and International Organization of Securities Commissions (IOSCO)

In November 2015, the Joint Working Group on Cyber Resilience of CPMI and IOSCO released the consultative paper, "Guidance on Cyber Resilience for Financial Market Infrastructures."[33] This guidance aims to enhance the ability of financial market infrastructures (FMIs) to prevent cyber attacks, respond rapidly and effectively to them, and achieve faster and safer recovery objectives. When finalised, the guidance will not establish additional standards for FMIs beyond those already set out in the Principles for Financial Market Infrastructures (PFMI) but aims to elaborate on the PFMI.[34]

Basel Committee of Banking Supervision (BCBS)

In October 2014, the BCBS published "Review of the Principles for the Sound Management of Operational Risk,"[35] which reviews implementation of the Principles for the Sound Management of Operational Risk published in 2011.[36] The report addresses the operational risk management practices of 60 systemically important banks, and observes that some banks have developed scenarios concerning catastrophic events, such as cyber attack.

~~61.~~55. Under ICP 26 (Cross-border Cooperation and Coordination on Crisis Management), the supervisor cooperates and coordinates with other relevant authorities such that a cross-border crisis involving a specific insurer or group can be managed effectively. Accordingly~~Where cyber risk has crystallised~~, it is expected that supervisors would~~should~~ cooperate and coordinate with other relevant authorities in respect of ~~so that~~ a cross-border crisis involving the cybersecurity of a specific insurer or group ~~can be managed effectively, in accordance with ICP 26 (Cross-border~~

[33] *Available at* http://www.bis.org/press/p151124.htm.

[34] CPMI and IOSCO, *Principles for Financial Market Infrastructures* (April 2012), *available at* http://www.bis.org/cpmi/publ/d101a.pdf.

[35] *Available at* http://www.bis.org/publ/bcbs292.htm.

[36] *Available at* http://www.bis.org/publ/bcbs195.htm.

~~Cooperation and Coordination on Crisis Management)~~. Advance planning for timely and consistent coordination and management of a cross-border crisis (including policy measures, crisis response decisions, and external communications) is a component of effective crisis management. ICP 26 is currently under review.

~~62.~~56. Further IAIS material specific to this area may be useful to help supervisors implement consistent and sound supervisory practices, and to help insurers implement appropriate cybersecurity practices.

VII. Supervisory Response to Cyber Risk

~~63.~~57. This section considers the role of supervisors, includes a summary of the 2015 survey of IAIS Members on combatting cyber risk, and provides examples of ongoing and evolving supervisory responses to cybersecurity issues.

~~64.~~58. The mission of the IAIS includes developing and maintaining fair, safe, and stable insurance markets for the benefit and protection of policyholders. Within this context, insurance supervisors have a role in addressing risks (including cyber risk) that could pose threats to the safety and stability of, and confidence in, insurance markets, and that could compromise policyholders.

~~65.~~59. The supervisor can address cyber risk through appropriate regulation and the supervisory process. Supervisory areas that may have particular relevance for cyber risk and cyber resilience include:

- The security of private information held by insurers and intermediaries;
- Financial crime undertaken through cyber means; and
- Business continuity and disaster recovery planning – for individual insurers and intermediaries and potentially for the insurance sector as a whole.

~~66.~~60. In addition, cross-border and cross-sectoral supervisory cooperation may be important for addressing cyber risk, as the issue is global in nature.

IAIS Survey on Cyber Risk and Supervisory Practices

~~67.~~61. During January and February 2015, the IAIS conducted a survey of its Members to gain insight about current supervisory approaches to cyber risk. Specifically, the survey was intended to assist the FCTF in understanding Members' perception of cyber risk, their involvement in combating cyber threats, and the supervisory approaches that are used or are under development in this area. Approximately 30 Members responded. Based on the survey responses received, supervisory practices and views on cybersecurity vary widely among IAIS Members. Following are some notable trends observed from the survey responses. A summary of the survey results is provided in Annex I.

~~68.~~62. Most respondents indicated that they have established or will establish regulatory or supervisory requirements for insurers' corporate governance with respect to cybersecurity. Although many of the survey respondents have not yet defined specific cybersecurity provisions, they expect that insurers will cope with cyber risk under broader regulatory and supervisory requirements, i.e., through enterprise risk management activities, particularly through IT risk assessments. In addition, some of the survey respondents reported adherence to relevant standards, notably the ISO standard for information security management,[37] as well as the National Institute of Standards and Technology (NIST) framework for improving infrastructure.[38] A few respondents have published cybersecurity guidelines applicable to financial institutions.

[37] The ISO 27000 standards help organisations keep information assets secure. ISO/IEC 27001 is the standard that provides requirements for an information security management system. International Organization for Standardization, *ISO/IEC 27001 - Information Security Management*, *available at* http://www.iso.org/iso/home/standards/management-standards/iso27001.htm.

[38] NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (12 February 2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

~~69.~~63. Yet, cyber resilience did not appear to be perceived as a regulatory priority for most survey respondents. Reasons given include the current stage of IT development, the lack of specific regulatory requirements for cyber resilience, and reliance on insurers' self-assessments. Furthermore, most survey respondents appeared to have limitations on staff with responsibility for and expertise in cybersecurity monitoring and supervision.

~~70.~~64. The survey results indicated that there are a variety of supervisory approaches to cyber resilience. For example, some respondents assess the nature and scale of cyber risk faced by an insurer through on-site inspections. Some expect to adopt holistic self-assessment exercises or thematic inspections focusing on cyber resilience of insurers. Others do not focus specifically on cyber risk but may assess cybersecurity as part of a business continuity plan or risk management framework of an insurer. Also, a minority of the respondents define the type or severity of cyber incidents that an insurer needs to report to its supervisory authority, while the majority of respondents have no specified requirements for notification, and a few rely on annual audit reports.

~~71.~~65. Although the number of survey responses was limited, the answers from responding Members and other information described in this report demonstrates that there is no uniform practice among IAIS Members with respect to supervision concerning cybersecurity.

Examples of Supervisory Responses to Cyber Risk

~~72.~~66. In addition to survey responses, certain IAIS members provided examples of some cyber risk initiatives undertaken in Member jurisdictions, including, in some instances, public—private cooperation and market-wide approaches. These examples are described below.

~~73.~~67. ***France***. L'Autorité de Contrôle Prudentiel et de Résolution (ACPR) categorises supervision related to cyber risk under Information System (IS) control. The ACPR established the following four criteria for cybersecurity supervision: (1) Confidentiality: Information is accessible only to those who are authorised to access. Information is protected throughout its lifecycle; (2) Integrity: Stored data is accurate and consistent. There is no need for alteration among data records; (3) Availability: Information is accessible by authorised persons at the right time with the right performance; and (4) Auditability: Access to IS, attempts to access IS, or activities in IS are logged and stored. The logged files must not be modified or deleted. With these criteria, the ACPR looks into the following areas: governance; identification, and assessment of IS risks; responses to IS risks; and, evaluation of controls, risk management, and follow-up activity.

~~74.~~68. ***Germany***. The supervisory examination of the management of cyber risk is usually performed through on-site inspections. The exact procedure depends on the size and risks of the particular undertaking and on the size of the team of supervisors. For smaller undertakings, the Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) addresses this aspect in the context of risk management. For larger undertakings, it often arranges a meeting focused on information security issues. During such a meeting, the team discusses those aspects of cybersecurity and IT risk management which are of high importance. Further areas of cybersecurity may be addressed when taking a closer look at other IT related aspects such as the software development process or identity management.

~~75.~~69. ***European Union***. The proposal for a Directive[39] concerning measures to ensure a high common level of network and information security across the Union was put forward by the European Commission in 2013. On 7 December 2015, the European Parliament and the Council reached an agreement on the Commission's proposed measures to increase online security in the EU. This Directive is the first piece of European legislation on cybersecurity. Its provisions aim to make the online environment more trustworthy and, thus, to support the smooth functioning of the EU Digital Single Market. The new rules will: (1) improve cybersecurity capabilities in Member States; (2) improve Member States' cooperation on cybersecurity; and (3) require operators of essential services in the energy, transport, banking and healthcare sectors, and providers of key digital services like search engines and cloud computing, to take appropriate security measures and report incidents to the national authorities.[40]

~~76.~~70. A proposed regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data entered into force on 24 May 2016~~will be put to a vote by Parliament as a whole in 2016~~ and ~~if adopted will~~shall be applicable from 25 May~~in~~ 2018.~~.~~[41] This text includes security incident notification provisions relating to personal data and empowers national data commissioners to impose significant fines.

~~77.~~71. ***Netherlands***. One of the deliverables from thematic investigations by the central bank of the Netherlands (the De Nederlandsche Bank, or DNB), is to provide individual financial institutions with a benchmark with which they are compared in each sector (e.g., insurers, banks, and pension funds) based on results of investigations. Individual financial institutions can see where they are positioned compared to the average for each sector. This applies to cyber risk management.

~~78.~~72. The DNB also supervises large international insurers jointly with supervisors of other jurisdictions. A number of joint research projects for supervision of such groups have been conducted. In addition, during investigations, two groups of people from different supervisory authorities have worked together in one team. Through such cooperation, the DNB intends to obtain insight into management of cyber risk within insurance groups. Moreover, some units within a group provide services internally for multiple group entities while the individual group entities may be subject to separate financial regulations applicable in each jurisdiction. The DNB intends to obtain better insight into such units from a perspective of the entire group through such work. Good examples of this type of supervisory cooperation include supervision focusing on group-wide asset management and IT systems.

[39] Proposal for a Directive on Measures to Ensure a Common High Level of Network Security and Information in Union – 2013/048 (called SRI or NIS).

[40] European Commission, *Network and Information Security Directive: co-Legislators Agree on the First EU-wide Legislation on Cybersecurity* (9 December 2015), *available at* http://ec.europa.eu/digital-agenda/en/news/network-and-information-security-directive-co-legislators-agree-first-eu-wide-legislation.

[41] The European Parliament and the Council of the European Union, *Regulation 2016/679 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) (4 May 2016),~~European Parliament, New Data Protection Standards to Ensure Smooth Police Cooperation in the EU (17 December 2015),~~ *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN ~~http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fTEXT%2bIM-PRESS%2b20151217IPR08122%2b0%2bDOC%2bXML%2bV0%2f%2fEN&language=EN~~.

Private Sector Information Sharing Initiatives in the Netherlands

In the Netherlands, the central bank (De Nederlandsche Bank, or "DNB") has found that insurers recognise the danger presented by cyber risk and are willing to cooperate with one another. The Dutch Association of Insurers currently has two active working groups in the field of IT risks and a separate consultation group made up of insurer IT directors. The two working groups work respectively on information security (IS) and Business Continuity Management (BCM). In these two groups, specialists from the largest insurers exchange information about their experiences, what they are doing, and how to learn from each other. The working groups meet three to four times per year. The DNB has given presentations to both groups and observed that the information exchange process still has room for improvement. For example, information about attacks on insurers could be shared more extensively.

~~79.~~73. ***Singapore***. The Monetary Authority of Singapore (MAS), together with the Association of Banks in Singapore ("ABS"), organises an industry-wide exercise triennially to enable financial institutions to practice and improve coordination with key government partners to minimise the impact of a crisis arising from a cybersecurity incident. Exercise Raffles IV, the 2014 exercise, saw some 141 financial institutions, including banks, finance companies, insurance companies, asset management firms, and securities and broking houses participate in a half-day exercise that tested participants' response to a massive cybersecurity incident on the financial industry. Financial institutions and market infrastructures faced a combination of simulated cybersecurity incidents, including theft of information; compromise of financial institutions' core systems; ATM outages, disruptions in online services; and website defacement. The simulated attacks required financial institutions to assess the impact of the attacks on the institutions' businesses in five broad categories: customer, reputational, regulatory and legal, financial, and operational.[42]

~~80.~~74. ***United Kingdom***. The UK financial authorities[43] have undertaken a number of projects to understand and seek to mitigate cyber risk. In 2005, 2007, and 2009, the UK financial authorities undertook projects to benchmark the operational resilience of the UK financial sector.[44] In 2012, the authorities responded to increasing cyber threats and feedback from the sector and focused on developing smaller, more targeted surveys to delve deeper into the theme of technology and cyber resilience. This led to a desk-top exercise in 2013 to test the wholesale banking sector's response to a sustained and intensive cyber attack.[45]

~~81.~~75. The Financial Policy Committee (FPC) recommended that HM Treasury, collaborating with relevant government agencies and the other financial authorities, should work with the core UK financial system and its infrastructure to put in place a programme of work to improve and test resilience to cyber risk. In response, the authorities issued a cyber-risk management questionnaire to core UK firms and themes from this survey have been used to identify areas for future work. Based on this assessment, the capabilities needed to address cyber risk can usefully be divided into three categories: defensive capabilities, recovery capabilities, and effective governance. The resulting programme of work is set around four themes: (1) enhancing

[42] Association of Banks in Singapore, "Financial Sector Tests Response to Cyber Attacks in Fourth Industry-wide Business Continuity Exercise" (21 November 2014), *available at* http://abs.org.sg/docs/library/mediarelease_20141121.pdf.

[43] Prior to 1 April 2013, the financial authorities were the Bank of England, the Financial Services Authority, and HM Treasury.

[44] Bank of England: http://www.bankofengland.co.uk/financialstability/fsc/Pages/bcinformation.aspx.

[45] *Ibid.*

understanding of the threat to the financial sector; (2) strengthening work to assess the sector's current resilience to cyber risk; (3) developing plans to test the resilience of the sector; and, (4) improving the sharing of information.

~~82.~~76. In June 2015, the FPC recommended further that the Bank of England, the Prudential Regulatory Authority (PRA), and the Financial Conduct Authority (FCA) should work with firms at the core of the UK financial system to ensure that they complete CBEST tests (a framework to test for cyber vulnerabilities) and adopt individual cyber resilience action plans. The Bank, the PRA, and the FCA should also establish arrangements for CBEST tests to become one component of regular cyber resilience assessment within the UK financial system. In August 2015 the PRA and FCA began a project to assess the resilience of the insurance sector.[46]

Additional Supervisory and Cooperative Measures in the United Kingdom

The UK government views cyber attacks as a highest-level risk to national security, alongside terrorism threats. Accordingly, it has set up a number of initiatives to help prevent cyber attacks, including.

- Cyber Essentials[47] – a basic cybersecurity hygiene standard launched in 2014 to help organisations protect themselves against common cyber attacks
- A National Cyber Crime Unit within the National Crime Agency
- A Cyber Information Sharing Partnership to allow Government and industry to exchange information on cyber threats[48]
- A single reporting system for people to report financially motivated cyber-crime through Action Fraud,[49] a UK National Computer Emergency Response Team (CERT) to improve national co-ordination of cyber incidents[50]
- A new Cyber Incident Response scheme in Government Communications Headquarters to help organisations recover from a cyber attack
- A network of Centres of Excellence for Cyber Security Research within UK universities in 2013, to help provide reliable and up to date research and academic prowess.

[46] Prudential Regulation Authority, Bank of England: http://www.bankofengland.co.uk/pra/Documents/about/insuranceletter100815.pdf.

[47] Government of the United Kingdom, Department for Business, Innovation & Skills and Cabinet Office, *Guidance – Cyber Essentials Scheme* (April 2014), *available at* https://www.gov.uk/government/publications/cyber-essentials-scheme-overview.

[48] Government of the United Kingdom, Cabinet Office, Department for Business, Innovation & Skills, Foreign & Commonwealth Office and National Security and Intelligence, *Policy Paper – 2010 to 2015 Government Policy: Cyber Security* (February 2013), *available at* https://www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace/supporting-pages/establishing-a-cyber-security-information-sharing-partnership.

[49] Action Fraud is the UK's national fraud and internet crime reporting centre. Information *available at*: http://www.actionfraud.police.uk/about-us.

[50] CERT-UK (https://www.cert.gov.uk/) is the UK National Computer Emergency Response Team, formed in March 2014 in response to the *National Cyber Security Strategy* (November 2011), *available at* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf).

~~83.~~77. ***United States***. There are several initiatives and programmes in the United States that focus on the cyber resilience of the financial sector, including insurers. These include, but are not limited to, the following.

~~84.~~78. Financial and Banking Information Infrastructure Committee. The United States Department of the Treasury serves as chair of the Financial and Banking Information Infrastructure Committee (FBIIC), which is a committee of 18 federal and state financial regulators and related organisations, including the Board of Governors of the Federal Reserve System and state insurance regulators. FBIIC was chartered to focus on: (1) improving coordination and communication among financial regulators; (2) enhancing the resiliency of the financial sector; and (3) promoting public-private partnership. Treasury coordinates U.S. financial sector cybersecurity efforts through the FBIIC. To fulfil its mission, FBIIC: (1) identifies critical infrastructure assets, along with their locations and potential vulnerabilities, and prioritises their importance to the financial system of the United States; (2) establishes secure communications capability among the financial regulators and protocols for communicating during an emergency; and (3) ensures that sufficient staff at each member organisation have appropriate security clearances to handle classified information and to coordinate in an emergency.[51]

79. Federal Sanctions Power. On 1 April 2015, the President ~~Obama~~ signed Executive Order 13694, *Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities*. This Executive Order authorises the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, to impose sanctions on individuals or entities that engage in certain significant malicious cyber-enabled activities.[52]

~~85.~~80. NIST Framework. The Framework for Improving Critical Infrastructure Cybersecurity (NIST Framework) was released by the U.S. National Institute of Standards and Technology in February 2014. The NIST Framework was created through collaboration between industry and government, and sets out a voluntary, prioritised, flexible, repeatable, and cost-effective approach to managing cybersecurity.[53] Although originally created for applicability to critical infrastructure (i.e., essential services that underpin the U.S. economy, security, and health), the NIST Framework was also designed to be used by firms of all sizes and from all sectors and jurisdictions. Authorities in the United States continue to promote widespread adoption of baseline cybersecurity best practices through the use of the NIST Framework with the aim of broadening the understanding of cyber risk and improving collective cybersecurity.[54]

~~86.~~81. FFIEC Cybersecurity Assessment Tool. Although designed specifically as a voluntary self-assessment tool for banks, the Cybersecurity Assessment Tool (Assessment) developed by the U.S. Federal Financial Institutions Examination Council (FFIEC)[55] in 2015 provides a logical

[51] Financial and Banking Information Infrastructure Committee: https://www.fbiic.gov/index.html.

[52] Executive Office of the President, *Executive Order: Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities* (1 April 2015), *available at* https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m.

[53] NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (12 February 2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[54] White House, *Administration Efforts on Cybersecurity: The Year in Review and Looking Forward to 2016* (2 February 2016), *available at* https://www.whitehouse.gov/blog/2016/02/02/administration-efforts-cybersecurity-year-review-and-looking-forward-2016.

[55] The FFIEC is a formal U.S. interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by certain U.S. banking regulators. See FFIEC's website: http://www.ffiec.gov/.

approach to cyber risk management, aspects of whichthat could be considered by other financial institutions, including insurers. The Assessment is designed to provide financial institutions within its purview with a "repeatable and measurable process" to inform Senior Management and Boards of Directors of the institutions cyber risk and cybersecurity preparedness.[56] The Assessment can be used to: (1) identify factors contributing to and determining the institution's Inherent Risk Profile, or its overall cyber risk; (2) assess the institution's Cybersecurity Maturity in five separate domains, and whether that cybersecurity preparedness is aligned with the institution's Inherent Risk; and (3) identify specific risk management practices or controls that are needed to improve cybersecurity.

[56] Federal Financial Institutions Examination Council (FFIEC), *Cybersecurity Assessment Tool Glossary* (June 2015), *available at* http://www.ffiec.gov/cyberassessmenttool.htm#tool.

Additional Federal Supervisory and Cooperative Measures in the United States

Cyber Information Sharing. In December 2015, the President signed into law the Cyber Information Sharing Act of 2015 (CISA), which establishes a system for private companies to voluntarily share cybersecurity threat information with federal agencies. Companies that share such information receive specific liability protections. Personally identifiable information not directly related to a threat must be removed prior to sharing the data.[57]

National Cybersecurity Plan. On 19 February 2016, the President ~~Obama~~ directed Executive Department agencies to implement a Cybersecurity National Action Plan (CNAP) that takes near-term actions and puts in place a long-term strategy to enhance cybersecurity awareness and protections, protect privacy, maintain public safety as well as economic and national security, and empower Americans to take better control of their digital security. In addition to establishing the Commission on Enhancing National Cybersecurity to develop a roadmap for future actions, CNAP calls on health insurers and healthcare stakeholders to take significant steps to enhance their data stewardship practices and ensure that consumers can trust that their sensitive data will be safe and secure.[58]

Financial Services Information Sharing and Analysis Center. The Financial Services Information Sharing and Analysis Center (FS-ISAC) was established by the private sector to share threat, vulnerability, and incident information, including anonymised reporting from member institutions and several public authorities. Membership in FS-ISAC is recommended by several agencies, including the FFIEC, its member agencies, Department of Homeland Security, and the Department of the Treasury. Homeland Security Presidential Directive 7 (2003) established the role of the federal government in providing sanitised threat and vulnerability information to FS-ISAC and private sector entities operating critical infrastructure, assisting critical infrastructure protection through public/private partnerships, and the coordinating role of Treasury related to response to incidents affecting financial services critical infrastructure.[59] In addition, private critical infrastructure firms in the financial services sector formed the Financial Services Sector Coordinating Council (FSSCC) to coordinate critical infrastructure protection activities for the financial sector, including incident response and related information sharing.[60] Insurers are involved in both the FS-ISAC and the FSSCC.

~~88.~~83. National Association of Insurance Commissioners (NAIC) Cyber Initiatives. The NAIC is pursuing several initiatives in response to emerging cyber threats. State insurance regulators serve on the FBIIC and on the Cybersecurity Forum for Independent and Executive Regulators, where they work with Federal regulators to develop best practices and discuss common approaches to cybersecurity challenges. In late 2014, the NAIC formed the Cybersecurity (EX) Task Force to coordinate insurance regulators' efforts to address cybersecurity issues. Shortly after its formation, the Task Force established 12 *Principles for Effective Cybersecurity Insurance Regulatory Guidance*, which set forth a framework for regulators to evaluate efforts by insurers,

[57] Consolidated Appropriations Act, 2016, Pub. L. 114-113 (Dec. 15, 2015).

[58] White House Press Release, *Fact Sheet: Cybersecurity National Action Plan* (9 February 2016), *available at* https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

[59] Financial Services Information Sharing and Analysis Center (https://www.fsisac.com/about).

[60] Financial Services Sector Coordination Council for Critical Infrastructure Protection and Homeland Security (https://www.fsscc.org/eweb/startpage.aspx).

producers, and other regulated entities to protect consumer information.[61] These principles were revised and adopted by the NAIC Executive/Plenary Committee in June 2015. The Task Force then developed the *Cybersecurity and Identity Theft Coverage Supplement* for insurer financial statements to gather financial performance information about insurers writing cybersecurity coverage. The revised supplement was adopted by the NAIC Executive/Plenary Committee in August 2015 and filings began in the first quarter of 2016.[62] The Task Force is also working with the NAIC's Information Technology Examination Working Group and the Market Conduct Examination Standards Working Group to develop and updated protocols for inclusion as guidance in the Financial Condition Examiners Handbook and Market RegulationConduct Examiner Handbooks, respectively, as cyber threats continue to evolve. Financial Examination revisions included in the 2016 Handbook are beingand will be used for examinations with an effectiveas of date of 31 December 2015. Finally, the Task Force also developed the NAIC *Roadmap for Consumer Cybersecurity Protections* to describe protections the NAIC believes consumers are entitled to from insurance companies, agents, and other businesses when these entities collect, maintain, and use personal information.[63] First adopted by the Task Force in October 2015, the Roadmap was adopted by the NAIC Executive/Plenary in December 2015. These protections will be incorporated into updates of relevant NAIC model laws and regulations, as well as into a new "Insurance Data Security Model Law" that was exposed in March 2016, and which may be considered for adoption later in 2016.

89.84. Role of the U.S. State Supervisor. In general, in the event of a breach at a domestic insurer, the lead state may use its regulatory authority in the following ways: (1) coordinate calls with the insurer to determine: when breach took place; who is affected by such breach and, using that information, determine which regulators need to be informed of this impact on state residents; and, how notifications will be made to affected individuals (e.g. mail, email, newspaper ads, etc.); (2) ensure that appropriate actions are taken by the insurer in response to the breach (e.g., identity theft protection, etc.); (3) communicate with state/federal regulators as appropriate; and (4) determine if a targeted exam is necessary/appropriate and, if so: coordinate selection of vendor to perform cybersecurity exam; coordinate the execution of the examination procedures; determine the scope of work using Financial Condition Examiners Handbook concepts where appropriate; communicate the results of the exam; and, determine if regulatory action is necessary. Relevant state insurance regulators have joined multi state market conduct examinations following insurer data breaches, looking into, among other things, the details of the breaches, the insurers' responses to the breaches, and the financial impact of the breaches on both policyholders and the insurers.

90.85. New York Department of Financial Services. In November 2015, the New York Department of Financial Services (DFS) issued a letter to the members of the FBIIC indicating that it is considering a new cybersecurity regulation for financial institutions. The letter sets forth key regulatory proposals that the DFS is considering as part of those regulations and invites feedback. Among other provisions, the potential regulations would require financial institutions to adopt written cybersecurity policies and procedures overseen by a designated Chief Information

[61] NAIC, *Principles for Effective Cybersecurity: Insurance Regulatory Guidance* (April 2015), *available at* http://www.naic.org/documents/committees_ex_cybersecurity_tf_final_principles_for_cybersecurity_guidance.pdf.

[62] NAIC, *Cybersecurity and Identity Theft Insurance Coverage Supplement* (June 2015), *available at* http://www.naic.org/documents/committees_ex_cybersecurity_tf_related_cyber_id_theft_ins_suplement.pdf.

[63] NAIC, *Roadmap for Cybersecurity Consumer Protections* (December 2015), *available at* http://www.naic.org/documents/committees_ex_cybersecurity_tf_related_roadmap_cybersecurity_consumer_protections.pdf

Security Officer (CISO) on: (1) information security; (2) data governance and classification; (3) access controls and identity management; (4) business continuity and disaster recovery planning and resources; (5) capacity and performance planning; (6) systems operations and availability concerns; (7) systems and network security; (8) systems and application development and quality assurance; (9) physical security and environmental controls; (10) customer data privacy; (11) vendor and third-party service provider management; and (12) incident response, including by setting clearly defined roles and decision making authority. Moreover, institutions would be required to implement and maintain policies and procedures to ensure the security of sensitive data or systems that are accessible to, or held by, third party service providers, and the policies and procedures would be required to include internal requirements for minimum preferred terms to be included in contracts with third-party service providers addressing information security risks. Further, the CISO would be required to submit to the DFS an annual report, reviewed by the Board, assessing the cybersecurity programme and the cyber risk to the institution. The New York initiative remains at the proposal stage.

VIII. Conclusion

~~92.~~87. Cyber risk presents a growing challenge for the insurance sector, and one which, under the ICPs, supervisors are obliged to address. Insurers collect, store, and manage substantial volumes of confidential personal and commercial information. Because of these reservoirs of data, insurers are prime targets for cyber criminals who seek information that later can be used for financial gain through extortion, identity theft, or other criminal activities. In addition, because insurers are significant contributors to the global financial sector, interruptions of insurers' systems due to cybersecurity incidents may have far-reaching implications.

~~93.~~ The insurance sector faces cyber risk from both internal and external sources, including ~~Insurers are vulnerable to cybersecurity incidents via internal systems and~~ through interconnections with third parties.

~~94.~~88. Insurance sector cybersecurity incidents may result in severe and lingering harm for the policyholders affected and significant legal, regulatory, and operational costs, including reputational damage. Moreover, the insurance sector as a whole may be affected by a loss in public trust. Because of the growing frequency and severity of cybersecurity incidents on all commercial entities, cyber resilience must be achieved by all insurers, regardless of size, specialty, domicile, or geographic reach.

~~95.~~89. The global scale of cyber risk dictates the need to address these risks on a global basis, exemplified by ongoing work at the international level, including by financial sector standard-setting bodies such as CPMI and IOSCO. Effective cross-border cooperation and coordination is an important component of the supervisory response to cyber risk.

~~96.~~90. Insurance supervisors have an important role in enhancing cyber resilience in the insurance sector. The nature of cyber risk requires increased scrutiny by supervisors and increased cooperation and information sharing, with appropriate safeguards, between and among the private and public sectors to enhance cyber resilience.

~~97.~~91. Although the ICPs do not explicitly address cyber risk or cyber resilience, the terms of the principle statements and accompanying standards and guidance encompass all of the issues presented by these risks. Accordingly, the ICPs provide a general basis for supervision of the insurance sector with respect to cybersecurity. Moreover, consistent with its mandate, in 2016-17 the FCTF will be investigating whether – and if so, how – ICP 21 should be extended to specifically address elements of cybersecurity.

~~98.~~92. There is a diversity of sophistication on cyber-related issues among IAIS Members ~~and insurers~~. Some insurance supervisors have taken meaningful steps to address the cyber resilience of insurers under their jurisdiction. However, based on the results of the 2015 IAIS survey on cyber risk, among other indications, the degree to which supervisors prioritise cyber risk and the tools available to address such risks varies across the globe.

~~99.~~93. Given past experience and forecasted trends, cyber risks and the impact of cyber incidents will continue to grow. Supervisors should seek to increase their understanding of cyber risk and their supervisory capabilities concerning the insurance sector's cyber resilience. Such supervisory focus might appropriately include, but should not be limited to, insurers' awareness of cyber risk and cyber resilience, and insurers' development and implementation of policies, procedures, and technology to increase cyber resilience, including the implications of outsourcing and other third-party connections on cyber resilience.

~~100.~~94. The IAIS will monitor initiatives and issues related to cyber risk as they continue to evolve. Additional IAIS supporting material addressing cyber resilience best practices in line with the ICPs may be helpful for supervisors and insurers. In this regard, in accordance with its mandate the FCTF recommends that the IAIS consider following this Issues Paper with one or more Application Papers further exploring these topics. It has identified, in particular, that guidance for supervisors on cybersecurity would be useful for the following facets of the insurance sector: (1) examination practices for supervisors; and (2) risk management practices for insurers.

Annex I

Summary of Responses to IAIS Survey

Over January-February 2015, the FCTF conducted a survey of IAIS Members on the subject of cyber crime. The survey was intended to assist the Task Force in understanding Members' perception of the risks, their involvement in combating cyber threats, and the supervisory approaches that are used or are developing in this area. Approximately 30 Members responded. This section provides major points from the responses, set out in accordance with the main themes of the survey.

Regulatory and Supervisory Context

i) Cyber risk is considered within the scope of operational risk and is addressed within IT regulatory frameworks, either through operational risk guidelines or specified IT standards. In general, respondents considered cyber threats to be increasing within their jurisdiction. However, the majority did not perceive cyber resilience to be a regulatory priority. Some of the factors for not prioritising cyber resilience included the current stage of development of their own insurance sector, the lack of a regulatory framework, and reliance on insurers' self-assessments.

Supervisory Expectations

ii) Some authorities provided feedback assuming their regulatory frameworks that are expected to be updated in near future are already in place while others described how their regulatory frameworks addressing operational risk or IT risk address cyber risk. In general, most survey respondents expect to include governance requirements within their own cyber regulatory framework, particularly regarding roles in respect of the three lines of defence.[64] However, responses in other areas, such as monitoring cyber incidents or staff training and awareness, cast doubt on whether these areas are being addressed within the cyber regulatory framework.

iii) For example, while more than half of the respondents indicated that they monitor a project of an insurer, including its deliverables and action plans, to remediate root causes of cyber incidents, others indicated that they do not have a specific framework to monitor projects addressing cyber incidents. Some authorities, however, indicated that if they identify any weaknesses of an insurer in dealing with a cyber incident during an on-site visit or on other occasions, they will assess and monitor follow-up actions of the insurer to address those weaknesses and its progress.

Supervisory Review and Assessment

iv) Certain survey respondents had no staff specifically devoted to cybersecurity surveillance, whereas a few have experienced teams of IT specialists that continuously receive training on cybersecurity issues. Between these extremes, most survey respondents appeared to have limitations on the number of staff with responsibility for cybersecurity monitoring.

[64] Commonly observed practices in the industry for sound risk governance three lines of defence often rely on three line of defence – (i) business line management, (ii) an independent corporate operational risk management function and (iii) an independent audit review. For example, see Basel Committee of Banking Supervision, *Sound Practices for the Management and Supervision of Operational Risk* (June 2011).

Governance

v) Two-thirds of survey respondents confirmed that they check whether periodic reporting to the Board and Senior Management on cyber risk and control assessments takes place. The same proportion reported that they verify the audit function's validation of the cybersecurity framework. A little over half of respondents confirmed that supervisors review the alignment of cyber risk management with the organisational strategy.

Cyber Risk Control Environment

vi) Half the survey respondents appeared to have regulatory provisions and supervisory practices in place to evaluate insurers' cyber risk control environment. However, many of them have not defined specific cybersecurity provisions, but rather follow cyber threats through risk management activities and particularly through IT risk assessments. A few respondents rely on periodic audit reports to monitor insurers' cybersecurity surveillance, while others include cybersecurity provisions as part of licensing requirements.

Threat and Vulnerability Risk Management

vii) A third of survey respondents clearly indicated that they assess insurers' management of cyber risk, including insurers' usage of software security tools. Around the same proportion confirmed that they keep up to date with recent developments on management of cyber risk. For those which do not follow such practices, some indicated that they only expect to be informed when insurers are subject to major cyber threats, while others rely on insurers' internal audit reports supported by conclusions from external IT specialists.

Addressing Cybersecurity Incidents

viii) Over two thirds of the respondents have no specific requirements for notifying authorities of cyber incidents. A few authorities nevertheless expect to be informed by insurers of any incidents that have significant impact on policyholders under regulatory requirements to protect personal information or with respect to major operational risk incidents, or they expect to be informed by another government agency that is responsible for information protection in general, but not directly reported by insurers. There is clearly scope to further develop the collection of statistics on the number of cybersecurity incidents.

ix) Also, over half of the respondents indicated that they monitor how an insurer follows up a cyber incident, including its deliverables and action plans, to remediate root causes of cyber incidents. A few others indicated that if they identify any weaknesses of an insurer in dealing with a cyber incident through an on-site visit, they will assess and monitor follow-up actions of the insurer to address the weaknesses.

x) Further, with respect to business continuity related to cyber incidents, a large majority of respondents indicated that they assess the effectiveness of insurers' business continuity plans after a cyber incident. Approaches vary among the respondents. Several look into a business continuity plan or a crisis management framework from a broader perspective where cyber resilience is part of the plan or framework.

Supervisory Measures

xi) Although the majority of respondents indicated that there is no regulatory requirement specifically addressing cyber risk, most of them indicated that there are a number of supervisory measures available. These included a letter of warning, an additional reporting request, a remediation plan, fine, or suspension of business. Over half of survey respondents reported not having used supervisory enforcement measures to address weaknesses and deficiencies in insurers' cybersecurity practices, over the past five years.

Supervisory Approaches and Other Initiatives to Address Cyber Risk

xii) Supervisory approaches vary for a number of reasons, including the priority given to cybersecurity initiatives as compared to other risk categories. Supervisory approaches also differ depending on the level of maturity of insurers' IT and telecommunications infrastructures. It should be noted that guidelines and other documents referred to in this section are considered to be of potential benefit to most jurisdictions, although there could be others of similar or even better level of detail and clarity. Bearing this in mind, the observed approaches have been subdivided into the following sections:

xiii) *Compliance with Standards.* Survey results clearly indicated that most jurisdictions associate cybersecurity with standards compliance. Though cybersecurity practices are continuously evolving, certain standards are relevant and applicable to most organisations. One such standard is ISO 27001, an international norm with the objective of providing requirements for sound information system security management.[65] More specifically related to cybersecurity is the "framework for improving critical infrastructure" published by the U.S. National Institute of Standards and Technology (NIST),[66] which focuses on using business drivers to guide cybersecurity activities and considers cybersecurity risks as part of an organisation's risk management processes.

xiv) *Guidelines and on-Site Inspections.* A few survey respondents noted having published guidelines specific to cybersecurity. For example, the U.S. NAIC has published principles for effective regulatory guidance specific to the insurance industry. In other cases the guidelines have been conceived to be applicable to all kind of organisations, such as the U.K.'s "Cyber Essentials" scheme, while others are specific to financial institutions, as in the case of OSFI's cyber self-assessment guide in Canada, or ASIC's cyber resilience health check in Australia.

xv) Even though most jurisdictions have only developed best practices documents, a few jurisdictions are already in the process of implementing updated examination frameworks, such as the one being developed by the New York State Department of Financial Services.

65. International Organization for Standardization, *ISO/IEC 27001 - Information Security Management*.

66. NIST, *Framework for Improving Critical Infrastructure Cybersecurity*.

Annex II

Glossary of Terms

Definitions of some of the key terms used in the paper are as follows:[67]

Cyber attack	Attempts to damage, disrupt, or gain unauthorised access to a computer, computer system, or electronic communications network. An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment or infrastructure; or destroying the integrity of the data or stealing controlled information.[68]
Cyber incident	Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system or the information residing therein.[69]
Cyber risk	Any risks that emanate from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks. It also encompasses physical damage that can be caused by cybersecurity incidents, fraud committed by misuse of data, any liability arising from data storage, and the availability, integrity and confidentiality of electronic information − be it related to individuals, companies, or governments.[70]
Cyber resilience	The ability to anticipate, absorb, adapt to and/or rapidly recover from disruption caused by a cyber attack or cyber incident.[71]
Cybersecurity	The term refers to strategies, policies, and standards encompassing the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resilience, and recovery activities, and policies regarding the security of an insurer's operations.[72]

[67] In providing these definitions, it is recognised that there is limited standardisation and hence alternative definitions for some terms can be found in other sources.

[68] Federal Financial Institutions Examination Council (FFIEC), *Cybersecurity Assessment Tool Glossary* (June 2015), *available at* http://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_App_C_Glossary_June_2015_PDF5.pdf.

[69] *Ibid.*

[70] CRO Forum, *The Cyber Risk Challenge and the Role of Insurance* (December 2014), *available at* http://www.thecroforum.org/cyber-resilience-cyber-risk-challenge-role-insurance/.

[71] Committee of Payment and Market Infrastructure and International Organization of Securities Commissions, *Consultative Paper – Guidance on Cyber Resilience for Financial Market Infrastructures* (November 2015), available at http://www.bis.org/press/p151124.htm.

[72] *Ibid.* Consistent with the definition used in the consultative paper.

Cybersecurity incident	In this paper, the phrase "cybersecurity incident" is used generally to capture both cyber attacks and cyber incidents.
Cyber threat	A circumstance or event with the potential to intentionally or unintentionally exploit one or more system vulnerabilities ~~in an insurer's systems~~ resulting in a loss of confidentiality, integrity, or availability.[73]
Data breaches	Security violations in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen, or used by an individual unauthorised to do so.[74]
Malware	Malware is designed to secretly access a computer system without the owner's informed consent. The expression is a general term (short for malicious software) used to mean a variety of forms of hostile, intrusive, or annoying software or programme code. Malware includes computer viruses, worms, Trojan horses, spyware, dishonest adware, ransomware, crimeware, most rootkits, and other malicious and unwanted software or programmes.[75]
NIST framework	National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, February 2014.[76]

[73] *Ibid.* Consistent with the definition used in the consultative paper.

[74] U.S. Department of Health and Human Services, Administration for Children and Families, *Information Memorandum: ACYF-CB-IM-15-04* (July 1, 2015), *available at* http://www.acf.hhs.gov/sites/default/files/cb/im1504.pdf.

[75] FFIEC, *Cybersecurity Assessment Tool Glossary*.

[76] *Available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

Annex III

Further Reading

Atlantic Council, *Beyond data breaches: global interconnections of cyber risk* (April 2014)

Committee on Payments and Market Infrastructures, *Cyber Resilience in Financial Market Infrastructures* (November 2014), *available at* http://www.bis.org/cpmi/publ/d122.pdf.

Committee on Payments and Market Infrastructures and International Organization of Securities Commissions, *Principles for Financial Market Infrastructures: Assessment Methodology for the Oversight Expectations Applicable to Critical Service Providers* (December 2014), *available at* http://www.bis.org/cpmi/publ/d123.htm.

Council of Europe, *Convention on Cybercrime* (November 2001), *available at* http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

Deborah Bodeau and Richard Graubart, "Cyber Resiliency Assessment: Enabling Architectural Improvement," *MITRE Technical Report MTR120407* (May 2013), *available at* http://www.mitre.org/publications/technical-papers/cyber-resiliency-assessment-enabling-architectural-improvement.

European Commission, "Cyber Security," *Special Eurobarometer 390* (July 2012), *available at* http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf.

Angelia Herrin, "Meeting the Cyber Risk Challenge," *Harvard Business Review* (27 November 2012), *available at* https://hbr.org/webinar/2012/12/meeting-the-cyber-risk-challen.

International Cyber Security Protection Alliance, "Project 2020 -Scenarios for the Future of Cybercrime," *available at* https://www.icspa.org/wp-content/uploads/2015/03/ICSPA_Project_2020_-_Scenarios_for_the_Future_of_Cybercrime.pdf.

International Telecommunication Union and United Nations Educational, Scientific and Cultural Organization, Broadband Commission for Digital Development, *The State of Broadband 2012: Achieving Digital Inclusion for All* (September 2012), *available at* http://broadbandcommission.org/documents/bb-annualreport2012.pdf.

International Telecommunication Union, "Cybersecurity Guide for Developing Countries," *available at* http://www.itu.int/ITU-D/cyb/publications/2009/cgdc-2009-e.pdf.

International Organization for Standardization, *ISO 31000: 2009, Risk management -- Principles and guidelines* (November 2009), *available at* http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43170.

- *ISO/IEC 27005:2011, Information technology – Security techniques – Information security risk management* (June 2011), *available at* http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56742.

- *ISO/IEC 27032:2012, Information technology – Security techniques – Guidelines for cybersecurity* (July 2012), *available at* http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44375.

- *ISO/IEC 27000:2016, Information technology - Security techniques -- Information security management systems - Overview and vocabulary* (February 2016), *available at* http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=66435.

International Organization of Securities Commissions, *Mechanisms for Trading Venues to Effectively Manage Electronic Trading Risks and Plans for Business Continuity*, (December 2015), *available at* http://www.iosco.org/library/pubdocs/pdf/IOSCOPD522.pdf.

Information Systems Audit and Control Association, *Control Objectives for Information and Related Technology*, *available at* http://www.isaca.org/COBIT/Pages/default.aspx.

Organisation for Economic Co-operation and Development, *Future Global Shocks, Improving Risk Governance* (September 2011), *available at* http://www.oecd.org/governance/48329024.pdf.

- *Cybersecurity Policy Making at a Turning Point, Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy* (2012), *available at* http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf.

- *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines* (April 2011), *available at* http://www.oecd-ilibrary.org/science-and-technology/the-evolving-privacy-landscape-30-years-after-the-oecd-privacy-guidelines_5kgf09z90c31-en.

- "Information security and privacy," *available at* http://www.oecd.org/sti/ieconomy/informationsecurityandprivacy.htm.

Rohini Tendulkar, "Cyber-crime, securities markets and systemic risk," *Joint Staff Working Paper*, International Organization of Securities Commissions Research Department and World Federation of Exchanges, (July 2013), *available at* http://www.iosco.org/research/pdf/swp/Cyber-Crime-Securities-Markets-and-Systemic-Risk.pdf.

SANS Institute, *CIS Critical Security Controls - Version 6.0* (January 2013), *available at* http://www.sans.org/critical-security-controls/.

Securities Industry and Financial Markets Association, *Principles for Effective Cybersecurity Regulatory Guidance* (October 2014), *available at* http://www.sifma.org/issues/item.aspx?id=8589951691.

UK National Computer Emergency Response Team, *Cyber-security risks in the supply chain* (February 2015), *available at* https://www.cert.gov.uk/resources/best-practices/cyber-security-risks-in-the-supply-chain/.

United Nations, *Creation of a global culture of cybersecurity, Resolution 57/239 adopted by the General Assembly* (January 2003), *available at* http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf.

United Nations Interregional Crime and Justice Research Institute, *Profiling Hackers* (November 2008), *available at* http://www.unicri.it/news/article/0811-4_hackers.

United Nations Office on Drugs and Crime, *Comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector* (February 2013), *available at* http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

U.S. Securities and Exchange Commission, Division of Corporation Finance, *CF Disclosure Guidance: Topic No. 2, Cybersecurity* (October 2011), *available at* http://www.sec.gov/about.shtml.

World Economic Forum, *Building Resilience in Supply Chains* (January 2013), *available at* http://www3.weforum.org/docs/WEF_RRN_MO_BuildingResilienceSupplyChains_Report_2013.pdf.

- *Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience* (May 2012), *available at* http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf.

- *Partnering for Cyber Resilience – Towards the Quantification of Cyber Threats* (January 2015), *available at* http://www3.weforum.org/docs/WEFUSA_QuantificationofCyberThreats_Report2015.pdf.