Founding Partner
OPTUS

MACQUARIE University

Quantification of Cyber Risk – Risk Categories and Business Sectors

Pavel Shevchenko, Jiwook Jang, Matteo Malavasi, Gareth W. Peters, Georgy Sofronov, Stefan Trück

1 June 2021

EXECUTIVE SUMMARY

This white paper presents analysis of Advisen Cyber Loss dataset (www.advisenltd.com/data/cyber-loss-data/) containing a historical view of cyber events, collected from reliable and publicly verifiable sources. The dataset analyzed in this study comprehends 132,126 cyber events during 2008-2020, affecting 49,496 organizations, with more than 80% of the organizations represented in the dataset residing in the USA. A summary of the findings is provided as follows:

- Currently, data collection and databases on losses from cyber events have an unbalanced recording of samples with the strongest emphasis on developing the US. centric data collection. However, cyber risk is international in nature affecting both commercial and private industry as well as government agencies across all sectors of the economy. Therefore, we advocate that a concerted effort be made to develop an adequate measurement and modelling process for cyber-related risks in the domestic landscape, there is a strong need and utility to be gained by collecting such data specifically for Australia.
- There are many cyber risk classifications, each designed with specific intent, purpose, and which build on pre-existing laws and policies. Enterprises and market participants should adopt the cyber risk classification that best fits their needs; standardisation within sectors makes sense but standardisation across different sectors may be ineffective.
- Over 60% of companies that recorded cyber-related losses have suffered from cyber-attacks more than once in the period 2008-2020. This suggests that governance processes relating to mitigation of such events can significantly be enhanced and that regulation and reporting around best practices as it emerges could help mitigate repeated events of the same nature from reoccurring.
- Losses from cyber related events are heavy-tailed. This means that while the majority of losses is typically relatively small (85% of events cause losses <$2 million), there is a chance for extreme losses, e.g. 5% of losses exceed $10 million, while 1.4% of cyber-related losses even exceed $100 million, and 0.17% of events cause losses >$1 billion.
- There is no distinct pattern or clear-cut relationship between the frequency of events, the loss severity, and the number of affected records. Contrary to assumptions often made in practice, the reported loss databases don't demonstrate a direct proportional relationship between total loss incurred from a cyber event and attributes from the event such as the number of compromised records (data records breached or stolen), the number of employees in a corporation or the number of units of a company affected. This finding shows that all companies, no matter the volume or size of data record can be susceptible to significant incurred loss from cyber events.
- The frequency and severity of the events depend on the business sector and type of cyber threat.
- It is clear that even with the increased scrutiny and increased regulatory guidance the rate of cyber crime has not abated. In fact the frequency of reported cyber-related events has substantially increased between 2008 and 2016 (4,800 reported events in 2008, 16,800 reported events in 2016). Furthermore, the reporting of such events for modelling purposes could be enhanced as there appears to be a significant delay in the reporting of events that needs to be taken into account when drawing conclusions on the risks.
- The most significant cyber loss event category, by number of events, continues to be Privacy - Unauthorized Contact or Disclosure and Data – Malicious Breach. Data related breaches have become increasingly more common since 2008, while Cyber Extorsion, Phishing, Spoofing and other Social Engineering practices also continue to increase, the pace at which malicious breach related events has occurred has now surpassed these other prominent categories of loss event risk type in recent years.
- The heavy tailed nature of cyber loss continues to be present. This is directly observed by the fact that cyber loss are well represented by the expression "one loss causes ruin" adage attributed to heavy tailed loss processes that demonstrate regular variation or power lower severity tail behaviour. As such, in all categories of cyber loss type and in all sectors of the economy it was found that loss severity is often dominated by large individual events. Overall, data breaches have caused the most serious financial consequences in the last four years, while the Information sector, Professional Scientific & Technical Services, and Finance & Insurance have suffered most of the financial damage during the sample period 2008-2020.

INTRODUCTION

Due to the digitalisation of business and economic activities via the Internet of Things (IoT), cloud computing, mobile and other innovative technologies, cyber risk is inherent and extreme. Cyber risks refer to any risk of financial loss, disruption to operations, or damage to the reputation of an organisation due to failure of its information technology (IT) systems, as defined by the Institute of Risk Management (IRM). Financial losses from malicious cyber activities result from IT security/data/digital assets recovery, liability with respect to identity theft and data breaches, reputation/brand damage, legal liability, cyber extortion, regulatory defence and penalties coverage and business interruption.

The frequency of malicious cyber activities is rapidly increasing, with the scope and nature dependent on an organisation's industry, size and location. According to the Allianz Global Risk Barometer 2021 (Allianz 2021), cyber incidents (including cybercrime, IT failure/outage, data breaches, fines and penalties) is currently a top-three global business risk. It is therefore critical that corporations and governments focus on IT and network security enhancement. Unless public and private sector organisations have effective cyber security plans and strategies in place, and tools to manage and mitigate losses from cyber risks, cyber events have the potential to affect their business significantly, possibly damaging hard-earned reputations irreparably.

Due to the impact of COVID-19, our business and economic activities will be also accelerated in cyber space, which could significantly increase the frequency and impact of cyber events around the globe, with alarming consequences for public and private sector organisations. Concerns about higher frequency and severity of cyber catastrophes demand a re-examination of quantifying cyber risks. A significant challenge ahead is to model the frequency and severity of individual cyber-related event and it is required greater understanding of the current and emerging risk landscape in cyber space to minimise potentially catastrophic losses from a cyber activity using real data.

The lack of historic data on cyber risk is another challenge to model the frequency and severity of individual cyber-related event. In Australia, it became mandatary for breached organisations to notify their data breaches details in 2019. If more comprehensive data on cyber risk in Australia becomes available, it will allow more effective testing of theoretical models for the frequency and severity of individual cyber-related event. Advisen Cyber Loss dataset is a unique dataset containing a historical view of cyber events, collected from reliable and publicly verifiable sources. The dataset analyzed in this study comprehends 132,126 cyber events from 2008 -2020, affecting 49,496 organizations, with more than 80% of the organizations represented in the dataset residing in the USA.

As the initial step of quantifying cyber risks, we present Australia, United States, European Union's classification of cyber risk categories, together with three other most used classifications in Operational Risk literature. We also examine the cyber security regulation and framework developed in Australia in general, and specifically in the Australian telecommunication sector. The main focus of this white paper is to show what the main features of cyber risk are, by looking at cyber event severity and frequency, using Advisen Cyber Loss dataset. The fact that all cyber risk types are heavy tailed will enable the second phase of the project - dependence analysis as well as further tail asymptotic analysis. Such studies should be interesting for private and public sector organizations dealing with the ongoing challenges and new risk dynamics arising in the cyber space.

CLASSIFICATION OF CYBER RISK EXPOSURES

Cyber risk involves a wide variety of risk factors and touches on nearly every sector in both the public and private domains. This makes the task of classifying cyber risk a challenging and non- unique task. Cyber risk presents many facets, combining technical know-how with behavioral and cultural aspects (Joint Research Center 2018), (Peters, Shevchenko and Cohen 2018), (Joint Research Centre 2019). Cyber crimes and threats are frequent, dynamically changing in nature, their scale is increasing in magnitude, and impact a variety of diverse actors. Cyber crimes affect both the individual personal sphere through events such as loss of data, ransomware attacks, credit card fraud, identity theft to name a few of the many attacks increasingly perpetrated on members of society who are increasingly engaged digitally through applications on multiple platforms such as their smart phones, tablets, computers and cloud

services. Cyber crimes also continue to severely affect organizations from all spheres of business and the public sector including infrastructure such as electricity grids, water grids, government agencies through to private organizations such as retail and investment banks. The nature of these events and attack types will depend on many factors and are often time varying in both sophistication and methods both on a common target and across different targets (Llyod's 2018), (Ponemon 2019), (Rand 2018) (Peters, Shevchenko and Cohen 2018), (NetDiligence 2019), (World Economic Forum 2020). This multidimensional heterogeneity makes defining and classifying cyber risk a non-unique task, to the point where a globally accepted and standardized classification of cyber risk is not available today and instead there are classifications and taxonomies developed which are developed from different industry perspectives (Cebula and Young 2010), (Cebula, Popeck and Young 2014), (CRO Forum 2014), (CRO Forum 2016), (Cyentia Institute 2020). Furthermore, many public and private institutions have tried to produce classifications addressing the most prominent cyber risk aspects relevant to their own stakeholders (National Institute of Standards and Technology 2004), (Joint Research Center 2018), (Joint Research Centre 2019) , (Australian Cyber Security Centre 2020).

Regulatory entities provide cyber risk classifications aimed at various aspects of cyber risk. The classifications analysed in this white paper focus on different aspects of cyber risk management, from pre-emptive preparation and resource allocation, to mitigation strategies and decision making processes. It also worth to mention that law and policy maker propositions often reflect national or communitarian interests and build on pre-existing laws and policies. The regulatory lens of cyber security can be dissected according to national approaches and extranational standards bodies. We will begin with a focus on the Australian perspective for cyber security and then speak more generally about approaches that are being adopted internationally and how Australia's cyber security landscape relates to international initiatives.

Australian Perspectives and Approaches

There are mixed perspectives on the cyber security regulation and preparedness for cyber events in Australia. As discussed in the recent industry review of Norton Rose Fulbright[1] they point out that "...Currently, the regulatory framework for cybersecurity in Australia is haphazard, with no mandatory best practice minimum security standards for businesses and the implications for a cyber attack potentially extending to multiple breaches of corporations, privacy and criminal laws, as well as industry-specific financial, energy, health and telecommunications requirements. With separate regulators – each with their own distinct powers, functions, enforcement priorities and internal pressures – responsible for administering each of those requirements, the potential for inconsistency, red tape and confusion for directors is considerable."

The consequence of such a dispersed approach is perhaps highlighted by the July 2020 Digital Trust Report, brought out by AustCyber which compiled an analysis of the possible scenarios that Australia could face in cyber events. In the report it is estimated that "a four week disruption to digital infrastructure caused by a major cyber attack would cost the Australian economy $30 billion (1.5% of GDP) and 163,000 lost jobs."[2] The report of Norton Rose Fulbright use this assessment to point out that such a figure is so significant as the digital economy in Australia is now contributing $105 billion (5.5% of GDP) to the overall Australian economy in 2019-2020 alone.

It is therefore clear that in order to protect such a key component of the Australian economy there will require a robust framework for regulation and risk management when it comes to national cyber security and commercial cyber security for firms operating in Australia.

There have been multiple fronts that have been developed by numerous government agencies in the past year to address cyber security. This was given particular focus after` the event of a high level incident in Australia involving an alleged state sponsored cyber attack on national agencies in Australia.

As a response the Australian government brought out the Cyber Enhanced Situational Awareness and Response (CESAR) Package on 30 June 2020 [3] which replaces the previous strategy brought out in 2016. As noted on the Australian government webpage associated with the announcement of this new policy guidance for national cyber

[1] (Atkins and Luck 2020)
[2] (AustCyber 2020)
[3] Australian Government Cyber Security Strategy:
www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/BudgetReview202021/CyberSecurityStrategy

security: "The Strategy outlines what the Government sees as the responsibilities of government, business and the community, and actions in relation to each, with the Australian Government to 'focus on critical threats and the most sophisticated actors, while ensuring a baseline of cyber resilience across the economy'."

The new cyber security strategy has a number of key spending components to enhance preparedness and numerous legislative reforms. The summary of these includes, to quote the Australian government's release:

- "positive security obligations for critical infrastructure entities (including, but not limited to, cybersecurity; the framework will take an 'all-hazards' approach) supported by sector-specific standards;
- enhanced cybersecurity obligations for systems of national significance (the subset of entities assessed as being of highest criticality); and
- assistance for entities targeted by cyber attacks, including the ability for the Government to issue directions to entities and in limited circumstances to 'take direct action to protect a critical infrastructure entity or system in the national interest' (the latter has been categorised as a power for ASD to 'hack back'[4])."

Furthermore, the *SCI Act* currently imposes regulatory obligations on certain entities in the electricity, gas, water and maritime ports sectors, and the telecommunications sector has obligations under similar sector-specific legislation[5]. In addition, it is expected that the proposed amendments will also impose security requirements on other sectors that may include banking and finance, defence private industry, logistics and food resource chains, medical and health sectors, and the transportation industry.

From an industry perspective the new *SCI Act* will require some key actions from the industry sector and the boards operating on Australian listed companies. For instance the analysis of Norton Rose Fulbright highlights the following key takeaways:

- "Directors in all industries and sectors need to be alert to the enhanced cyber threats that extend right across their supply chains and impact on all aspects of their operations in an increasingly digitised business world.
- Directors must ensure that their businesses innovate to keep pace with the technology and resources that criminal networks are themselves putting into novel cyber attacks.
- Directors need to have cyber security as a standing item for proactive consideration at all board meetings, and they should request specific periodic briefings, at least two to three times per year, concentrating on key industry cybersecurity trends, regulatory requirements locally and internationally, modelling on how a cyber attack would impact the business, and the existing cyber capability of the business and avenues for improvement.
- Cybersecurity should also be included as a distinct topic for risk committee investigation and reporting, and directors should ensure that a standalone cyber resilience framework and supporting cyber security program is developed."

It is believed that if directors fail to take these actions as mentioned then they will be at risk of substantial breaches of criminal, privacy and industry regulations currently under development and to be actioned as part of the Cyber Security Strategy, see further discussion in the analysis of Norton Rose Fulbright.

We will also focus specifically on the Australian telecommunications sector and the landscape for cyber security regulations. In the report of Herbert Smith Freehills (HSF)[6]. The telecommunications sector is a particular target of cyber attack as they have core infrastructure for communications and hold large volumes of private user data. As noted in the report of HSF "Telecoms companies face particular cyber security concerns as a result of their interconnected nature and reliance upon international standards in their operations." The example provided is related to mobile phones and the international reliance on the Signaling System 7 SST (North America SS7, UK CCITT7, Germany ZZK-7 etc) protocol which is the standard adopted for international interoperability in telecoms.

The majority of the SS7 protocols are based around the standardization developed by American National Standards Institute[7] (ANSI) and the European Telecommunications Standards Institute[8] (ETSI). There are a few significant deviations from these standards for China and Japan. Furthermore, the Internet Engineering Task Force[9] (IETF) has

[4] https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22media%2Fpressclp%2F7489684%22
[5] https://www.homeaffairs.gov.au/nat-security/Pages/telecommunications-sector-security-reforms.aspx
[6] (Moir, Fitzpatrick and Everett 2020)
[7] https://en.wikipedia.org/wiki/American_National_Standards_Institute
[8] https://en.wikipedia.org/wiki/European_Telecommunications_Standards_Institute
[9] https://en.wikipedia.org/wiki/Internet_Engineering_Task_Force

defined the SIGTRAN[10] protocol suite that implements levels 2, 3, and 4 protocols compatible with SS7. Sometimes also called Pseudo SS7, it is layered on the Stream Control Transmission Protocol[11] (SCTP) transport mechanism for use on Internet Protocol[12] networks, such as the Internet[13].

As discussed in the report of HSF These standards adopted internationally were developed in the 1970's and have been found to contain vulnerabilities that allow calls, texts and location information on handsets to be spied upon knowing only a subscribers phone number. A recent example of this occurred in Germany where attackers were able to exploit vulnerabilities to access bank accounts by intercepting two factor authentication SMS messages.

Other key protocols that will require significant monitoring and potential enhancement of oversight in the new cyber risk policies of Australia include the Border Gateway Protocol (BGP) protocol which is the standardised exterior gateway protocol that was designed to exchange routing and reachability information among autonomous systems and the internet. This protocol has been a source of attack for malware and worms that take over home routers provided by ISPs or take over and redirect DDoS attacks on core internet infrastructure and servers.

It is clear that an Australian SCI Act will require international co-operation to be successful as many of the attacks that target vulnerabilities in a telecommunications network often focus on aspects of international protocols such as SS7 and BGP. Since such standards are defined by international working groups and agencies they naturally require international cooperation to resolve the vulnerabilities.

It is explained in the analysis of HSF that telecommunications companies will be liable for failure to prevent or dampen the effects of attacks exploiting such vulnerabilities in international protocols adopted domestically. They state "Telcos can expect increasing intervention from regulators and governments on cyber issues, including in relation to these protocol vulnerabilities, to the extent these or other cyber issues begin to compromise the integrity or privacy of communications networks. Telcos need to ensure that their pro-active defence and cyber incident response plans adequately address the legal and operational risks as well as the technical response to incidents."

In addition, the ACSC also released their Annual Cyber Threat Report 2019-2020 which established a new categorization applied in Australia based on a three-dimensional approach. Recognizing the importance of Cyber Threats in Australia as surging, fast developing, and adapting to new form of smart working during the COVID-19 pandemic, the ACSC defines a classification based on 6 levels of severity, varying accordingly to 5 macro-categories of cyber-attacks, and 6 macro-categories of affected agents. In principle, it is expected that the magnitude of a sustained disruption of service suffered by a private member of the public differs vastly to the same type of cyber-attack suffered from infrastructure of national importance.

The Australian Cyber Security Centre (ACSC) utilizes a three-dimensional approach and builds a classification system to prioritize responses, identify mitigation practices, categorize incident severity, and allocate resources.

It includes the following cyber-attack categories:

- Sustained disruption of essential services and systems
- Exfiltration or deletion/damage of key sensitive data or intellectual property
- Malware beaconing or other active network intrusion; temporary system or service disruption
- Low level malicious attack – targeted reconnaissance, phishing, non sensitive data loss
- Scanning or reconnaissance

and the following agent categories:

- Members of the public
- Small organizations and sole traders
- Medium sized organizations and schools
- State Government, academia, research and development facilities, large organization, and supply chain
- Federal Government, national infrastructure, and supply chain to center of national intelligence
- National security, Australian essential services, and centers of national intelligence.

[10] https://en.wikipedia.org/wiki/SIGTRAN
[11] https://en.wikipedia.org/wiki/Stream_Control_Transmission_Protocol
[12] https://en.wikipedia.org/wiki/Internet_Protocol
[13] https://en.wikipedia.org/wiki/Internet

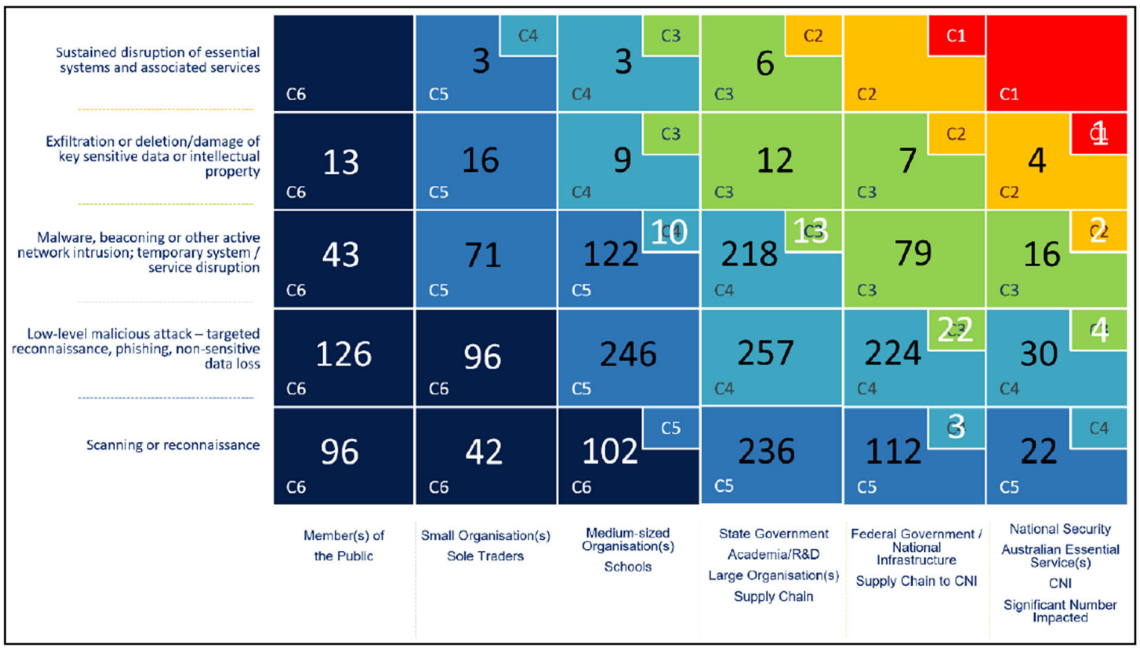

Figure 1: ACSC Cyber Categorisation Matrix. The matrix represents the cyber events recorded by the ACSC during the financial year 2019-2020, divided by cyber categories and agents affected. The colour represents the severity class. Source: (Australian Cyber Security Centre 2020).

International Perspective

United States

A first, broad set of standards, has been laid out by the National Institute of Standards and Technology (NIST) with the "Standards for Security Categorization of Federal Information and Information Systems", which defines standards to assist united states federal agencies in categorize cyber risk related events (National Institute of Standards and Technology 2004). The categories are based on the potential damage on the ability of organizations to carry out their legal responsibilities, their functions and the protection of the individual involved. It is based on three objectives and three levels of potential impact.

Objectives:

- **Confidentiality**: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- **Integrity**: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity
- **Availability**: Ensuring timely and reliable access to and use of information loss of *availability* is the disruption of access to or use of information or an information system

Level:

- Low: The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals
- Moderate: The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals
- High: The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.

The NIST classification aims to evaluate the potential impact of cyber events: cyber events are inspected and classified according to the impact on the three objectives, and the resulting outcomes need to be addressed jointly with vulnerability and threat information in assessing the risk to an organization.

European Union

Currently there is no commonly accepted cyber risk taxonomy among European Union members. Nevertheless, as a result of a two-year consultation process, the European Commission and the Joint Research Center (JRC) have set the ground for a common cyber risk categorization in the EU (Joint Research Center 2018), (Joint Research Centre 2019). The classification roots deeply into the work of the Commission and the JRC and embraces the multidimensional aspects of cyber risk. Having consulted European Cybersecurity Centers of Expertise, the proposed high-level taxonomy is based on three variables:

- **Research domains** represent areas of knowledge related to different cybersecurity aspects. Such domains are intended to cover different areas, including human, legal, ethical and technological aspects.
- **Sectors** are proposed to highlight the need for considering different cybersecurity requirements and challenges (from a human, legal and ethical perspective) in scenarios, such as energy, transport or financial sector.
- **Technologies and Use Cases** represent the technological enablers to enhance the development of the different sectors. They are related to cybersecurity domains covering technological aspects.

The taxonomy proposed by the JRC serves as support in mapping cybersecurity competencies needed in facing cyber threats, and therefore aiding the decision making process before and after cyber threat occurrences.

Other Classifications

More operatively driven definitions of cyber risk categories can be found in various private entities and industry consulting companies. Typically, their interests diverge from those of public and regulatory entities and so do their cyber risk classifications. In this white paper we consider three of the most used classifications in Operational Risk literature.

Chief Risk Officer Forum

Building from the broad definition of the NIST, the Chief Risk Officer Forum (CRO) provides a classification from the perspective of Operational Risk (CRO Forum 2014), (CRO Forum 2016). The CRO defines cyber risk as “any risks emanating from: the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks; physical damage that can be caused by cyber attacks; fraud committed by misuse of data; any liability arising from data use, storage and transfer, and the **availability**, **integrity** and **confidentiality** of electronic information be it related to individuals, companies or governments.” Following this definition, the CRO also provides 4 cyber risk categories:

- System malfunctions
- Data confidentiality breach
- Data integrity
- Malicious activity

Software Engineering Institute

With a similar fundamental approach to the CRO, the Software Engineering Institute bases its cyber risk definition on the NIST, proposing to address cyber risk as “the operational risk to information and technology that have consequences on confidentiality, integrity and availability of information system” (Cebula and Young 2010), (Cebula, Popeck and Young 2014). Placing cyber risk in the realm of operational risk has many advantages. First, it allows to disaggregate cyber risk from other established risk categories, such as market, credit, and legal. Secondly, the commonly used classification from operational risk can be used to categorize cyber risk events. In particular, the Software Engineering Institute proposes that operational cyber risks fall into four categories:

- Actions of people: operational risk characterized by problems caused by the action taken or not taken by individuals in a given situation.
- System and technology failures: operational risk characterized by problematic abnormal or unexpected functioning of technology assets.

- Failed internal processes: operational risk associated with problematic failures of internal processes to perform as needed or expected.
- External events: operational risk associated with events generally outside the organization's control.

Overall, this section has illustrated that classifying cyber-related risks is a challenging and non- unique task. Many public and private institutions have tried to produce classifications addressing the most prominent cyber risk aspects relevant to their own stakeholders. This section has reviewed a variety that combine technical know-how with behavioural and cultural aspects.

In the following section we will use a specific classification proposed by Advisen (https://www.advisenltd.com/), the foremost provider of data, media, and technology solutions for the commercial property and casualty insurance market. The proposed classification distinguishes cyber events based on different cyber risk categories and affected sectors.

QUANTIFICATION OF CYBER RISKS

The Advisen Database

Advisen is the leading provider of data, media, and technology solutions for the commercial property and casualty insurance market. Advisen's proprietary data sets, which include "Cyber Loss Data", "Casualty Dataset", "Private D&O Loss Data", "Public D&O Loss Data" and "Loss Insight", provide detailed collections applicable to applications that focus on large, specialty risks. This white paper analysis focuses primarily on the "Cyber Loss Data" collection where Advisen adopt a granular classification based on the type of cyber risk threat. It comprises 16 cyber risk categories:

- **Privacy – Unauthorized Contact or Disclosure**: cases when personal information is used in an unauthorized manner to contact or publicize information regarding an individual or an organization without their explicit permission.
- **Privacy – Unauthorized Data Collection**: cases where information about the users of electronic services, such as social media, phones, websites, and similar is captured and stored without their knowledge or consent, or where prohibited information may have been collected with or without their consent.
- **Data – Physically Lost or Stolen**: situations where personal confidential information or digital assets have been stored on, or may have been stored on, computer, peripheral equipment, data storage, or printouts which has been lost or stolen, or improperly disposed of.
- **Data – Malicious Breach**: situations where personal confidential information or digital assets either have been or may have been exposed or stolen, by unauthorized internal or external actors whose intent appears to have been the acquisition of such information.
- **Data – Unintentional Disclosure**: situations where personal confidential information or digital assets have either been exposed, or may have been exposed, to unauthorized viewers due to an unintentional or inadvertent accident or error.
- **Identity – Fraudulent Use/Account Access**: identity theft or the fraudulent use of confidential personal information or account access in order to steal money, establish credit, or access account information, either through electronic or other means.
- **Industrial Controls and Operations**: losses involving disruption or attempted disruption to "connected" physical assets such as factories, automobiles, power plants, electrical grids, and similar (including "the internet of things").
- **Network/Website Disruption**: unauthorized use of or access to a computer or network, or interference with the operation of same, including virus, worm, malware, digital denial of service (DDOS), system intrusions, and similar.
- **Phishing, Spoofing, Social Engineering**: attempts to get individuals to voluntarily provide information which could then be used illicitly, e.g. phishing or spoofing a legitimate website with a close replica to obtain account information, or sending fraudulent emails to initiate unauthorized activities (aka "spear phishing").

- **Skimming, Physical Tampering**: use of physical devices to illegally capture electronic information such as bank account or credit card numbers for individual transactions, or installing software on such point-of-sale devices to accomplish the same goal.
- **IT – Configuration/Implementation Errors**: losses resulting from errors or mistakes which are made in maintaining, upgrading, replacing, or operating the hardware and software IT infrastructure of an organization, typically resulting in system, network, or web outages or disruptions.
- **IT – Processing Errors**: Losses resulting from internal errors in electronically processing orders, purchases, registrations, and similar, usually due to a security or authorization inadequacy, software bug, hardware malfunction, or user error.
- **Cyber Extorsion**: Threats to lock access to devices or files, fraudulently transfer funds, destroy data, interfere with the operation of a system/network/site, or disclose confidential digital information such as identities of customers/employees, unless payments are made.

The dataset is also classified based on the following 20 business sectors[14]:

- Agriculture, Forestry, Fishing and Hunting
- Mining, Quarrying, and Oil and Gas Extraction
- Utilities
- Construction
- Manufacturing
- Wholesale Trad
- Retail Trade
- Transportation and Warehousing
- Information
- Finance and Insurance
- Real Estate and Rental and Leasing
- Professional, Scientific, and Technical Services
- Management of Companies and Enterprises
- Administrative and Support and Waste Management and Remediation Services
- Educational Services
- Health Care and Social Assistance
- Arts, Entertainment, and Recreation
- Accommodation and Food Services
- Other Services (except Public Administration)
- Public Administration

We observe that such cyber loss event and business line categories are distinct from those required for Basel II banking Operational Risk practice where the Basel II Accord has seven official Basel II event types across all areas of Operational Risk Loss, including but not exclusively cyber risk losses, as outlined below:

1. Internal Fraud – misappropriation of assets, tax evasion, intentional mismarking of positions, bribery;
2. External Fraud – theft of information, hacking damage, third-party theft and forgery;
3. Employment Practices and Workplace Safety – discrimination, workers compensation, employee health and safety;
4. Clients, Products, and Business Practice – market manipulation, antitrust, improper trade, product defects, fiduciary breaches, account churning;

[14] See (Executive Office of the President Office of Management and Budget 2017)

5. Damage to Physical Assets – natural disasters, terrorism, vandalism;
6. Business Disruption and Systems Failures – utility disruptions, software failures, hardware failures;
7. Execution, Delivery, and Process Management – data entry errors, accounting errors, failed mandatory reporting, negligent loss of client assets.

When working with a taxonomy distinct from that specified in regulation for the banking sector, we note that financial institutions subject to such regulatory reporting requirements will have to consider carefully the mapping exercise to move from the Advisen taxonomy to the Basel II required reporting taxonomy. Furthermore, the standard banking structure under Basel II include 8 level 1 business lines corresponding to:

1. Corporate Finance;
2. Trading and Sales;
3. Retail Banking;
4. Commercial Banking;
5. Payment and Settlement;
6. Agency Services;
7. Asset Management; and
8. Retail Brockerage.

Again, these business lines are largely non-representative of the taxonomy adopted by Advisen which covers a much wider selection of sectors including the financial services. As such, the integration of other cyber loss data collections such as those collected over the last 15 years in the banking industry by consortiums such as ORX should be carefully considered. The great conundrum for modelling and analysing cyber related loss data is that whilst the prevalence of such events and their impact is seemingly growing over time, the access to national, standardised public domain data bases for such loss data is scarce and expensive to obtain. Therefore, generally, data on cyber risk-related events is known to be scarce and expensive to obtain; data on losses linked to cyber risk is even more scarce (Edwards, Hofmeyr and & Forrest 2016), (Eling and Loperfido 2017), (Eling and Wirfs 2019), (World Economic Forum 2020). Moreover, given that a widely accepted cyber risk definition and taxonomy does not exist universally across different sectors subject to different regulatory considerations and bodies, a dataset containing uniform and systematic information on cyber event severity and frequency are hard to find and to work with. With Australia being only in its initial stages of a data collection, a glimpse of what cyber risk is, its characteristics and how it affects various economics sectors can be obtained by looking at Advisen Cyber Loss dataset. Advisen Cyber Loss dataset is a unique dataset containing a historical view of cyber events, collected from reliable and publicly verifiable sources, such as news media, governmental and regulatory sources, state data breach notification sites, and third-party vendors. The dataset analyzed in this study comprehends 132,126 cyber events from 2008 -2020, affecting 49,496 organizations, with more than 80% of the organizations represented in the dataset residing in the USA. It is important to notice also that, given the nature of cyber risk, it is safe to assume that a huge number of events is not recorded. It is well known in fact that enterprises and companies seldom and reluctantly report cyber risk related events to avoid, among other things, a loss of reputation and trust from their counterparties.

Figure 2 illustrates the number of events in the Advisen database by countries. The vast majority of the recorded events happened in the USA, while only a minority of events is recorded for the entire European Union (2.65%) or Australia (0.66%). Given the specific geographic dependence of the data, companies present in the dataset will be categorized according to the North America Industry Classification System (NAIC).

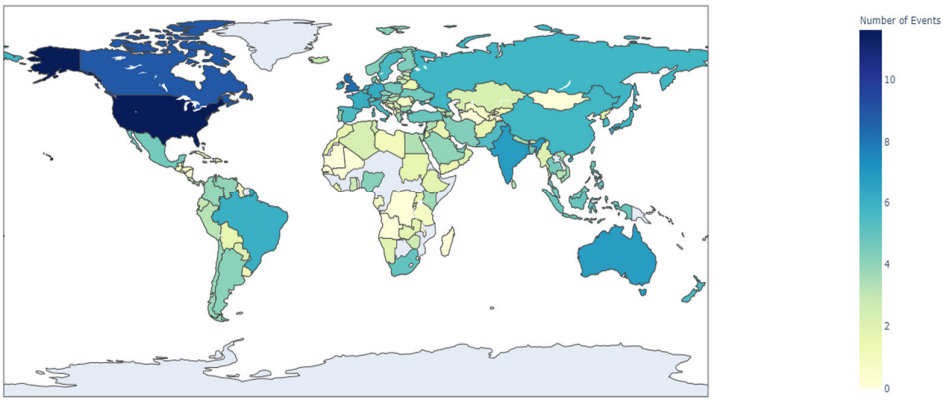

Figure 2: Number of cyber events by country during the period 2008-2020 across all loss categories (note that the number of events is reported on a log scale).

Affected Records, Frequency and Severity of events

In a first step we evaluate the relationship between the frequency and severity of individual cyber-related events and the number of affected records. Figure 3 shows the business sector ranked by frequency and severity of cyber events. Each circle represents a business sector, and its size corresponds to the average number of records affected by a cyber event. Overall, there is no clear-cut relationship between the frequency of events, loss severity, and the number of affected records. The relationship depends also on the business sector and type of cyber threat.

The sectors with the highest average cyber loss are: Information, Manufacturing, Transportation and Warehousing and, Whole Sale Trade. In terms of records affected: Information, Professional, Scientific, and Technical Services, Agriculture, Forestry, Fishing and Hunting, and Accommodation and Food Services. Figure 3 also depicts the fact that monetary losses and the number of records affected vary across business sectors. Business sectors in the top right corner of the graph in Figure 3 share some common features: they exhibit high average loss and high number of events, and a high average number of records affected (the bubbles have larger sizes than the sector in the top left corner of the graph). This seems to indicate that depending on the intrinsic nature of the business sectors, for some sectors there is a connection between a high number of records stolen which translates into high losses, however for other sectors larger number of records doesn't translate into greater losses. For instance, records stolen in sectors such as Mining, Quarrying, Soil and Gas Extraction, Agriculture, Forestry, Fishing and Hunting, and Construction have a lower monetary value than records stolen in Information and Professional, Scientific and Technical Services.

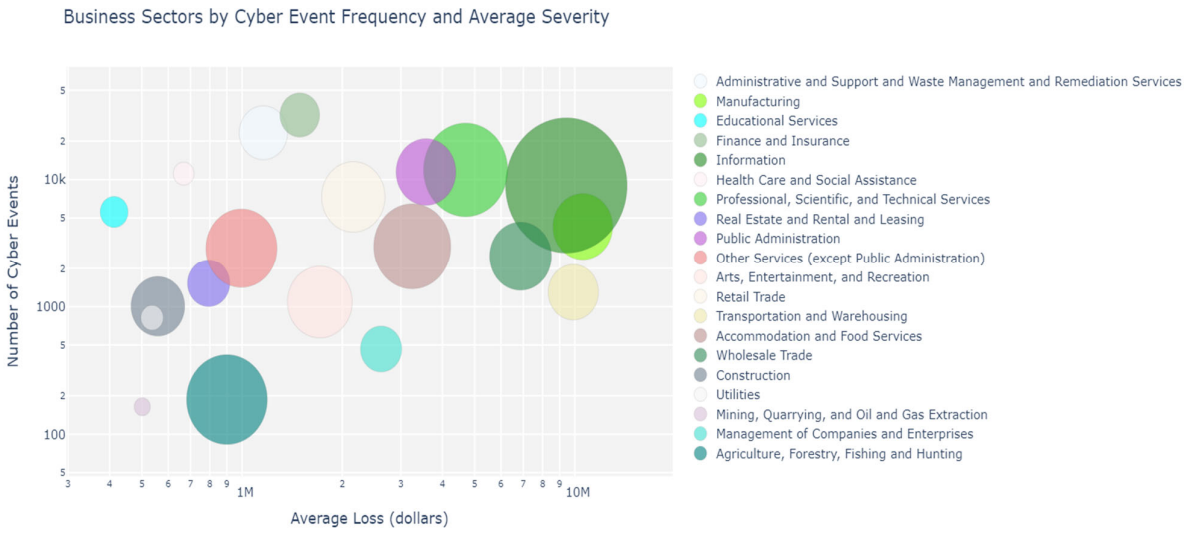

Figure 3: Frequency and severity of individual cyber-related events and the number of affected records (indicated by the size of the circle) across business sectors.

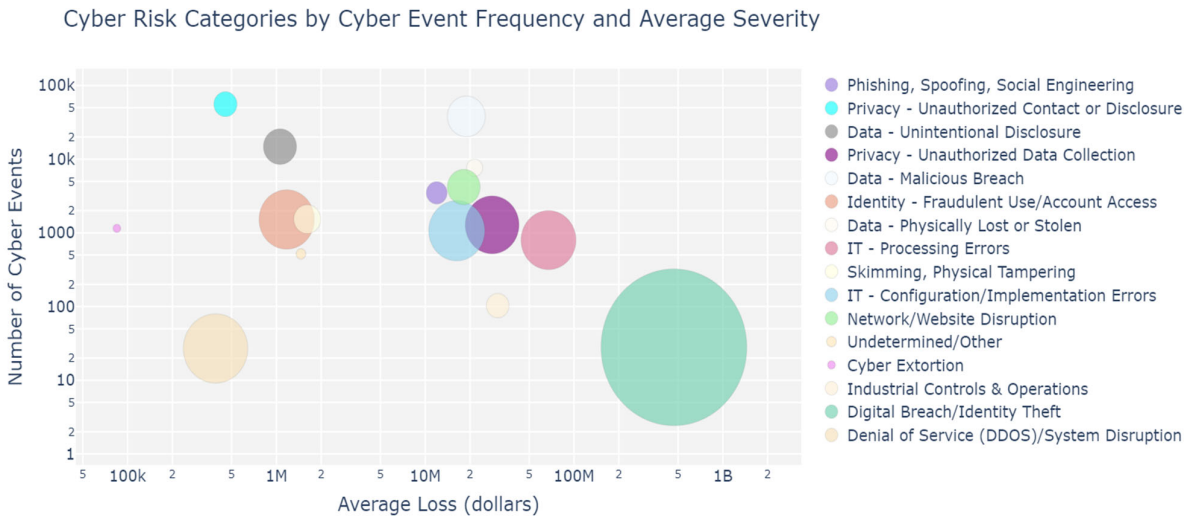

Figure 4: Frequency and severity of individual cyber-related events and the number of affected records (indicated by the size of the circle) across risk categories.

Figure 4 shows the Advisen cyber risk threat types ranked by frequency and average severity. Each circle represents a business sector, and the size of the circle corresponds to the average number of records affected. The cyber risk type with the highest average loss and average number of records affected is **Digital Breach/Identity Theft**. Looking at Figure 4, cyber risk types can be divided into three groups according to their average loss:

1. average loss lower than 2 million dollars: Cyber Extorsion, Denial of Service(DDOS)/ System Disruption, Privacy- Unauthorized Contact or Disclosure, Data-Unintentional Disclosure, Identity Fraudulent Use/Account Access, and Skimming, and Physical Tampering;

2. average loss between 10 million dollars and 100 million dollars: Phishing, Spoofing, Social Engineering, IT-Configuration/Implementation Error, Network/Website Disruption, Data-Malicious Breach, Privacy-Unauthorized Data Collection and IT-Processing Error;
3. average loss greater than 100 million dollars: Digital Breach/Identity Theft.

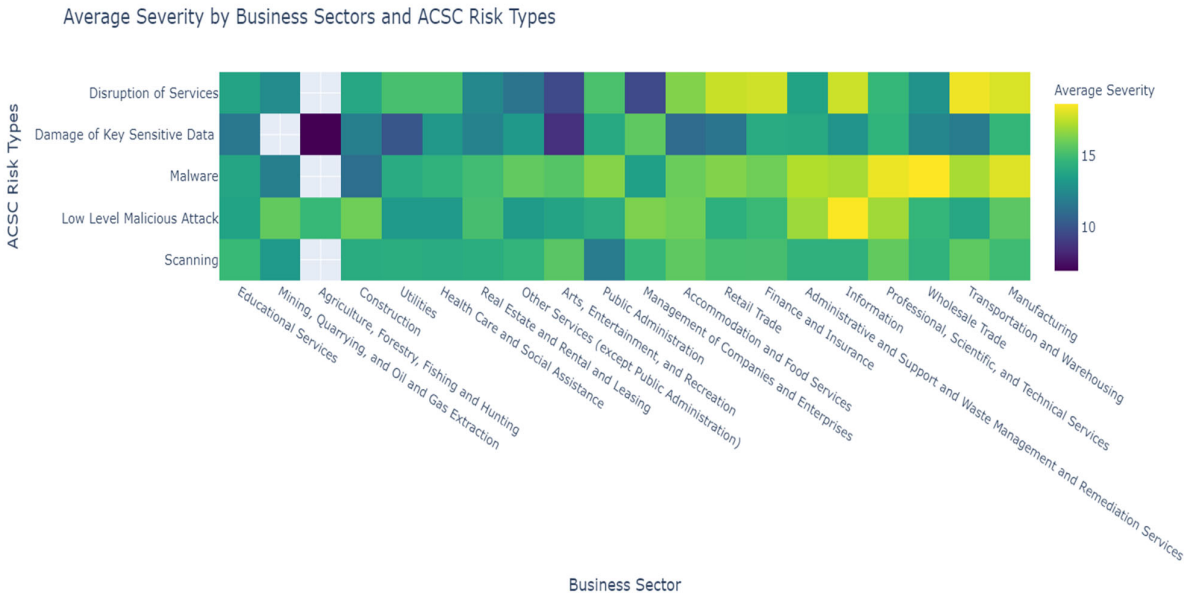

Figure 5: Average severity of cyber-related events by business sectors according to the ACSC classification. Sectors with high average losses show higher average severity in all the ACSC, than those with low overall average losses.

Figure 5 proposes an adapted version of the categorisation matrix by the ACSC, in terms of business sectors and average cyber event severity. Figure 5 illustrates the heterogeneity in the severity of cyber events both for cyber risk type and business sector. In particular, sectors with high average loss in Figure 3 report higher average losses for every ACSC cyber risk type, than those sectors with low average loss in Figure 3. This empirical fact emphasizes the dependence of monetary losses on specific company features, since companies operating in different business sectors have a different business model, a different internal structure and different levels of cyber risk resilience.

The Frequency and Severity of Cyber Events

In the following we examine the frequency and severity. Figure 6 illustrates the distribution of the number of cyber attacks per company between 2008 and 2020. More than 40% of the companies suffered from cyber crimes more than once during this period, with almost 3% of the firms being affected more than 10 times.

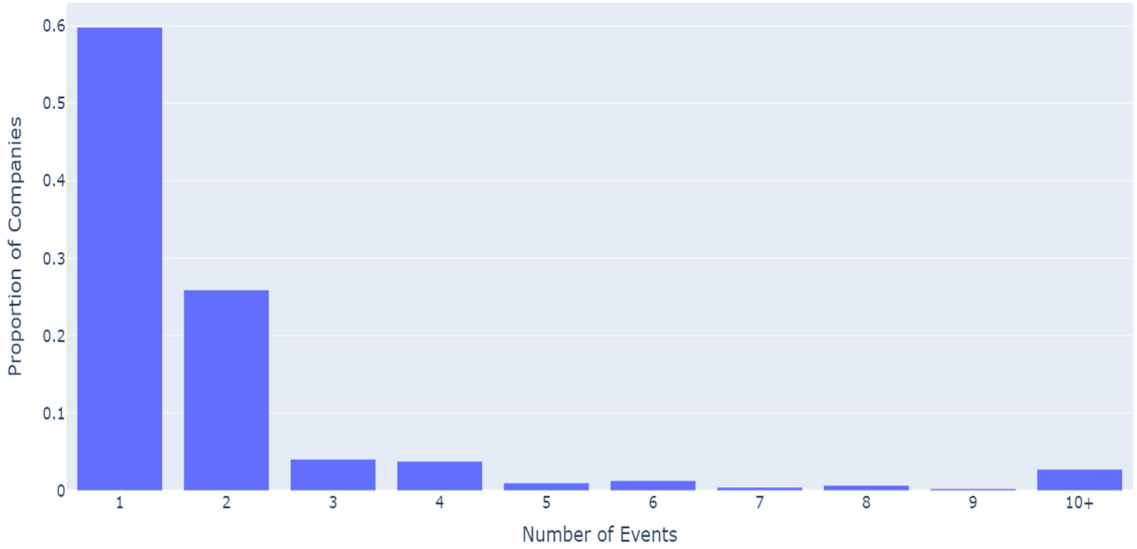

Figure 6: Distribution of the number of cyber-attacks per company.

Figure 6 provides the distribution of the number of cyber-attacks per company. More than 40% of the company experiences more than one cyber attacks between 2008-2020., while almost 3% of the firms were affected more than 10 times by cyber crimes. It is important to note that the dataset contains only information regarding cyber risk related events which have been publicly disclosed, and it would be safe to assume that the real number of events is much higher.

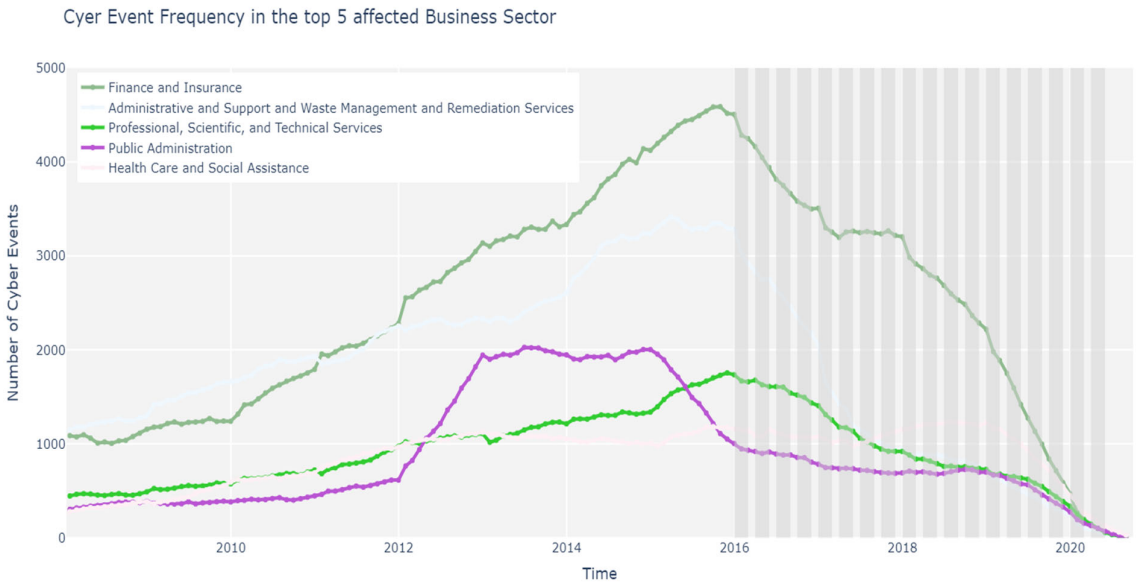

Figure 7: Number of cyber events for the five business sectors that were most affected.

Figure 7 the number of cyber events for the five business sectors that were most affected. We find that the frequency of reported cyber-related events has substantially increased between 2008 and 2016 (4800 reported events in 2008, 16800 reported events in 2016). There is also a significant delay in the reporting of events that needs to be taken into account when drawing conclusions on the risks. As it can be seen from the graph, the number of events appears to be decreasing after 2016 (the period corresponding to the dashed area in the graph). Given that, this declining is consistent across all business sectors, this seems to suggest the presence of a reporting delay, rather than a systematic improvement in cyber threat prevention, detection, and response mechanisms common for every business sector. Such reporting delay can be attributed to numerous factors, such as the reluctance of enterprises and companies to report cyber risk related events, and the data collection procedure employed by Advisen that abide to the United States of America Freedom of Information Act regulation. As a matter of facts, while US domiciled companies have a 60 days window between discovering the data breach and reporting it to affected parties, non-US domiciled entities do not have such strict requirement.

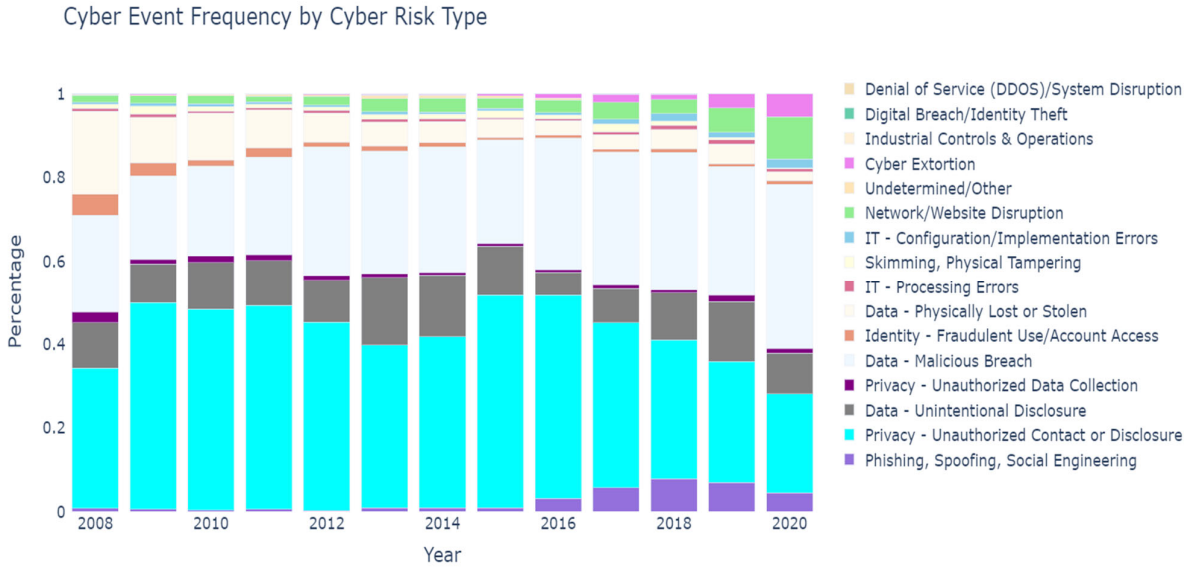

Figure 8: Share of cyber events for different cyber risk types for the period 2008 to 2020. Unintentional Disclosure, Data Malicious Breaches, Network/Website disruption, and Phishing, Spoofing and Social Engineering have become increasingly more common.

Figure 8 illustrates the percentage of events that fall into a specific cyber risk category for the period 2008 to 2020. The figure also illustrates the dynamic nature of cyber risk, with substantially changing shares for different event types. In particular we find that cyber risk categories such as **Data – Unintentional Disclosure**, **Data – Malicious Breaches**, **Network/Website Disruption** have become increasingly more common since 2008. Moreover, in recent years, **Cyber Extorsion** and **Phishing Spoofing and Social Engineering** are on the rise, reflecting the capability of cyber criminals to adapt and create new forms of cyber threats. At the same time, the share of events for the category Data – Physically Lost or Stolen that played a major role in the years 2008-2011 has dropped significantly.

Cyber attacks are time varying in nature, and so are also the root causes of losses. Figure 9 reports the share of total cyber-related losses that can be attributed to the different risk types for each year. Recall that for the frequency of different cyber risk categories we found a relatively clear structure as indicated by Figure 8. However for the severity of events, there is much more heterogeneity in the cyber risk categories across the time period. Nonetheless, we find that losses from **Data-Malicious Breaches** are typically among the highest, while this risk category can also be classified as the most severe risk type over the period 2017-2020. For other years, a high share of losses could be attributed to

Phishing, Spoofing and Social Engineering (2008), Digital Breach/ Identity Theft (2012), Privacy – Unauthorized Data Collection (2013), and Network/Website Disruption (2017).

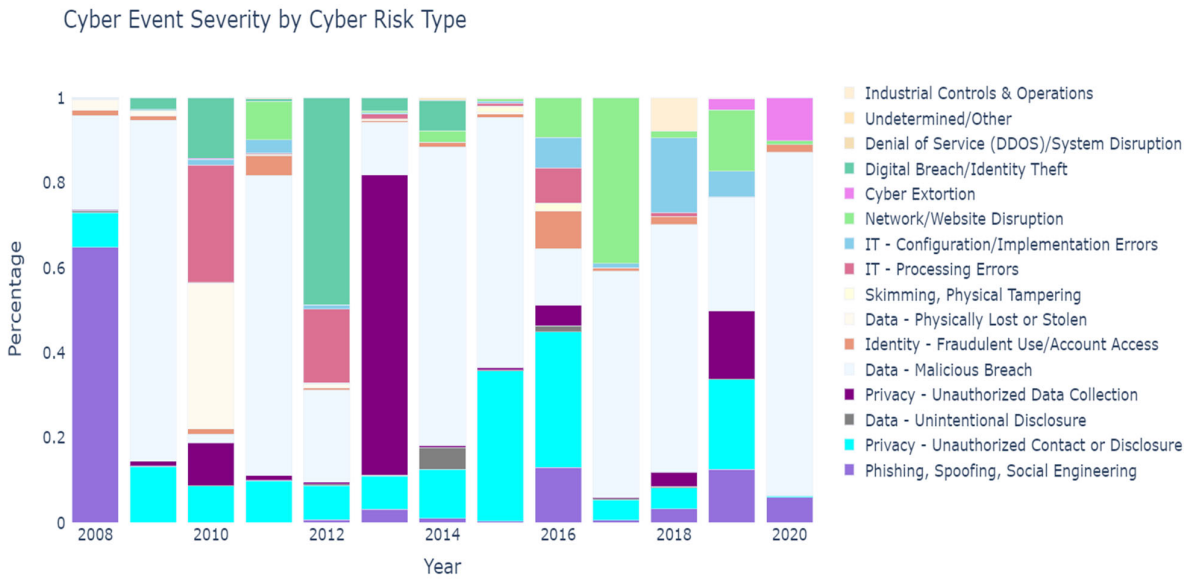

Figure 9: Share of total cyber-related losses that can be attributed to individual risk types for each year 2008-2020.

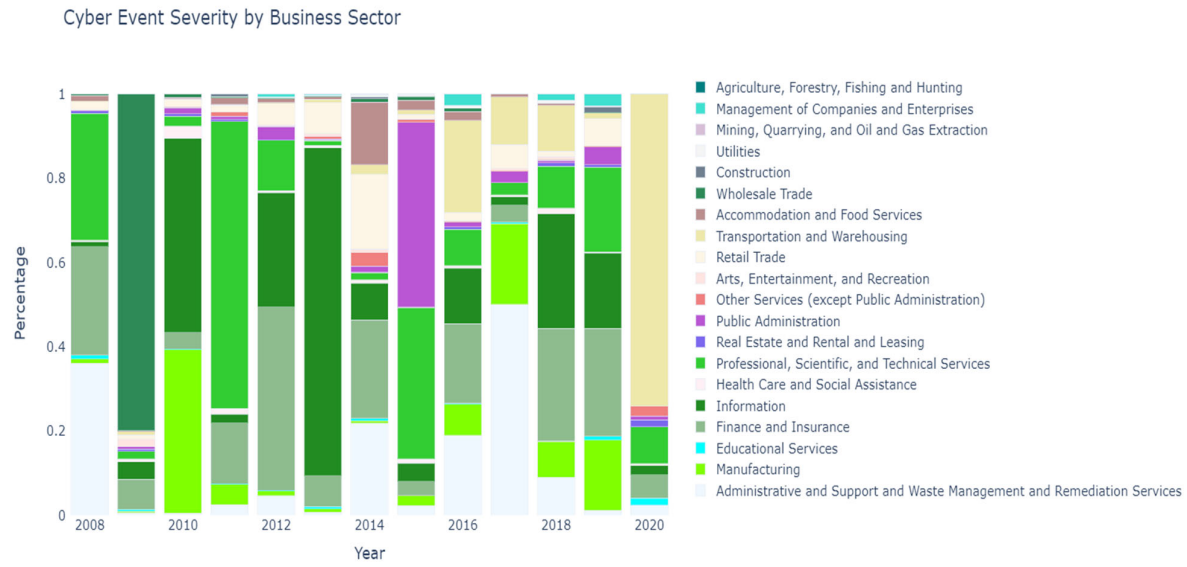

Figure 10: Share of total cyber-related losses that can be attributed to individual risk types for each year 2008-2020. Information, Professional Scientific and Technical Services, are Finance and Insurance are the most affected business sectors.

Not only does the nature of cyber risks change through time, but also companies in different business sectors suffer losses due to cyber events. Figure 10 shows the share of total cyber-related losses that can be attributed to a specific business sector. Our results indicate that the **Information** sector, **Professional Scientific and Technical Services**, and the **Finance and Insurance** sector typically seem to be among the most affected business sectors. However, the Figure also illustrates that other sectors can be heavily affected by cyber events, for example Public Administration in 2015 and Transportation and Warehousing in 2020.

Overall, the frequency and severity of cyber-related losses exhibits a very dynamic and time-varying nature. While the occurrence of events seems to be dominated by have certain risk categories, extreme losses occur in various cyber-risk categories or business sectors. This behaviour also makes it particularly difficult to predict the nature or magnitude of losses from cyber-related events.

The Severity Distribution

Finally, we have a look at the severity distribution of cyber related events across all risk categories and business sectors. Figure 11 shows the historical distribution for the severity of cyber-related event. The figure illustrates that only 15% of events causes losses that were higher than $2.5 million, while only 5% of events resulted in losses greater than $10 million. In Actuarial Science this phenomenon is called “heavy tails” and refers to the characteristic of certain probability distributions to allocate a greater (than the normal distribution) probability to extreme events (the tails). In other words, cyber risk events have a higher probability to produce extreme losses than events whose severity follows a normal distribution. At the same time, for a high fraction of events the losses are quite small, i.e., in the considered database 44% of events cause losses that are smaller than $50,000.

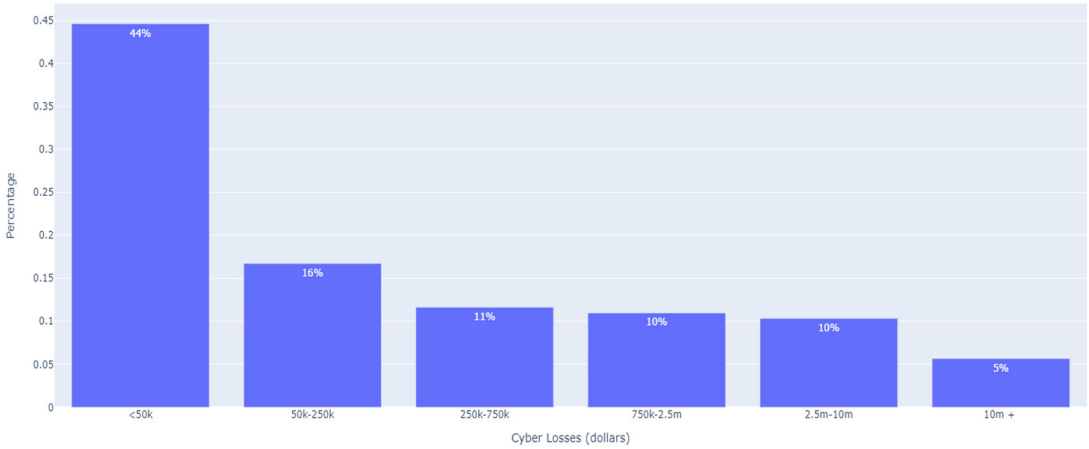

Figure 11: Histogram for severity of cyber-related loss events. Around 15% of events caused a loss that was greater than $2.5 million.

CONCLUDING REMARKS

Based on the discussion on some stylized facts of cyber risk, the following recommendations can be made:

- There exist many cyber risk classifications, each designed with specific intent, purpose, and build on pre-existing laws and policies. Enterprises and market participants should adopt the cyber risk classification that better fits their needs. It would be beneficial for sector specific regulators to continue to develop a working taxonomy and reporting framework specific to the risk profiles and needs of different industry sectors. These should not be unified across all sectors of the economy but tailored to particular sectors to capture the heterogeneous nature of cyber risk data event types and loss behaviour profiles.

- Within a given taxonomy of loss types and business types, there is s strong need to enhance significantly the collection of data on cyber risk, a systematic framework is needed in order to assure consistency and completeness of data. This should include detailed information on the event types, the failure modes that led to the loss events, the components of the loss events broken down into categories such as those utlised by Advisen. Many of these records per category of loss amount are missing or not-reported. The veracity of the data collected also needs to be improved.
- Records affected and monetary losses due to cyber events are both important to understand cyber risk, and reflect different aspects of cyber risk. Database containing cyber risk events should include both.
- The Australian financial system is as only as resilient as its weakest link, therefore more information on frequency and severity of cyber events needs to be shared between companies, insurance sector, government agencies in order to design effective control, prevention and response strategies.
- An effort as to be made in order to increase the awareness of cyber risk, even among small business and entities. Cyber risk can have catastrophic consequences against which, even appropriate insurance policies might not be adequate to cover such losses.
- As cyber losses are currently significantly under insured, there is a potential large exposure under reserved that could amount to tens of billions of dollars. This should be addressed, with maturity of the reporting frameworks and consistency in the loss data collection, insurers will be able to more reliably price and design reproducing insurance contracts to mitigate some of the losses incurred from cyber risk, which in tandem with improving risk governance is a key component of risk transfer for this category of risk. Currently the provided cyber insurance products have grown as a market exponentially, however their scope of coverage is extremely limited and bespoke in nature, making insurance premiums prohibitive to many markets. Consequently, at present, not all losses can be covered by insurance as there are extreme risks that pose a new challenge to the financial viability of insurers
- The dynamically changing nature of cyber risk dictate that enterprises, insurers and government agencies have to constantly update their cyber hygiene practices.

Cyber risk effects are heterogenous and affect different business sectors in different ways. Board members and decision makers should be aware of which cyber risk type the business sector they are operating in is more vulnerable and should act consistently, by adopting all the relevant strategies and procedures.

BIBLIOGRAPHY

Allianz 2021. *Allianz Risk Barometer 2021.* https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html.

Atkins, Scott, and Kai Luck 2020. *The cybersecurity standards set to impact every Australian business and director.* Norton Rose Fulbright. https://www.nortonrosefulbright.com/en/knowledge/publications/5e591584/the-cybersecurity-standards-set-to-impact-every-australian-business-and-director.

AustCyber 2020. "Australia's Digital Trust Report." https://www.austcyber.com/resource/digitaltrustreport2020.

Australian Cyber Security Centre 2020. "Annual Cyber Threat Report." https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-july-2019-june-2020.

Cebula, J. J., M. E. Popeck, and L. R. Young 2014. *A taxonomy of operational cyber security risks version 2.* Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Institute. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=91013.

Cebula, J. L., and L. R. Young 2010. *A taxonomy of operational cyber security risks.* Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Institute. https://apps.dtic.mil/sti/citations/ADA537111.

CRO Forum 2016. "CRO Forum Concept Paper on a proposed categorisation methodology for cyber risk." https://www.thecroforum.org/wp-content/uploads/2016/06/ZRH-16-09033-P1_CRO_Forum_Cyber-Risk_web-2.pdf.

CRO Forum 2014. "Cyber resilience: The cyber risk challenge and the role of insurance." https://www.thecroforum.org/2014/12/19/cyber-resilience-cyber-risk-challenge-role-insurance/.

Cyentia Institute 2020. "Information Risk: Insigth Study." https://www.cyentia.com/iris/.

Edwards, B., S. Hofmeyr, and S. & Forrest 2016. "Hype and heavy tails: A closer look at data breaches." *Journal of Cybersecurity* 2(1): 3-14. https://academic.oup.com/cybersecurity/article/2/1/3/2736315.

Eling, M., and J. Wirfs 2019. "What are the actual costs of cyber risk events?" *European Journal of Operational Research* 3: 272. https://www.sciencedirect.com/science/article/abs/pii/S037722171830626X.

Eling, M., and N. Loperfido 2017. "Data breaches: Goodness of fit, pricing, and risk measurement." *Insurance: Mathematics and Economics Eling, M.; Loperfido, N.* 5: 126-136. https://www.sciencedirect.com/science/article/abs/pii/S0167668716305042.

Executive Office of the President Office of Management and Budget 2017. "North American Industry Classification System." https://www.census.gov/naics/.

Joint Research Center 2018. *European Cybersecurity Centres of Expertise Map.* Publications Office of the European Union. https://publications.jrc.ec.europa.eu/repository/handle/JRC111441.

Joint Research Centre 2019. *A Proposal for a European Cybersecurity Taxonomy.* Publications Office of the European Union. https://publications.jrc.ec.europa.eu/repository/handle/JRC118089.

Llyod's 2018. "Emerging Risk Report." https://www.lloyds.com/~/media/files/news-and-insight/risk-insight/2018/internet-of-things/interconnectedworld2018-final.pdf.

Moir, Andrew, Peter Fitzpatrick, and Miriam Everett 2020. *Managing cyber security risks in the telecommunications sector.* Herbert Smith Freehills. https://www.herbertsmithfreehills.com/latest-thinking/managing-cyber-security-risks-in-the-telecommunications-sector.

National Institute of Standards and Technology 2004. *Standards for Security Categorization of Federal Information and Information Systems.* Federal Information Processing Standards Publication. https://csrc.nist.gov/publications/detail/fips/199/final.

NetDiligence 2019. "Cyber Claims Study." https://netdiligence.com/cyber-claims-studies/.

Peters, G., P. V. Shevchenko, and R. Cohen 2018. *Understanding cyber-risk and cyber-insurance.* Macquarie University Faculty of Business & Economics Research Paper. https://www.mq.edu.au/__data/assets/pdf_file/0007/1137418/understanding-cyber-risk-and-cyber-insurance.pdf.

Ponemon 2019. “Cost of Data Breach Report.” https://www.capita.com/sites/g/files/nginej291/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf.

Rand 2018. “Estimating the Global Cost of Cyber Risk: Methodology and Examples.” https://www.rand.org/pubs/research_reports/RR2299.html.

World Economic Forum 2020. “Cyber Information Sharing: Building Collective Security.” https://www.weforum.org/reports/cyber-information-sharing-building-collective-security.

ABOUT THE AUTHORS

- **Pavel Shevchenko** is a Professor in the Department of Actuarial Studies and Business Analytics and Co-Director of the Centre for Risk Analytics at Macquarie University. Prior to joining Macquarie University in August 2016, he worked at CSIRO Australia (1999-2016) holding the position of a Senior Principal Research Scientist (2012-2016). He has worked in the area of quantitative risk since 1999, leading research and industry projects.
  Email address: pavel.shevchenko@mq.edu.au
- **Jiwook Jang** is an Associate Professor in the Department of Actuarial Studies and Business Analytics at Macquarie University. His research interests include financial and insurance risks, catastrophe insurance modelling, financial/insurance derivatives pricing, stochastic point processes such as Cox process, self-exciting process, and dynamic contagion process.
  Email address: jiwook.jang@mq.edu.au
- **Matteo Malavasi** is a Research Fellow in the Department of Actuarial Studies and Business Analytics at Macquarie University. His research interests are financial mathematics, applied probability, computational methods for economics and finance, and environmental economics.
  Email address: matteo.malavasi@mq.edu.au
- **Gareth W. Peters** is a Chair Professor in Statistics for Risk and Insurance in the Department of Actuarial Mathematics and Statistics at Heriot-Watt University, Edinburgh. He is also an Honorary Professor in the Department of Actuarial Studies and Business Analytics at Macquarie University. He is a renowned researcher in modern data analytics techniques (state-space methodologies, sequential Monte Carlo and Markov chain Monte Carlo methods, machine learning) closely working with insurers and regulators in UK and Europe.
  Email address: g.peters@hw.ac.uk
- **Georgy Sofronov** is an Associate Professor in Statistics and Research Director in the Department of Mathematics and Statistics at Macquarie University. His research interests are focused on change-point detection methods, optimal stopping rules and computational statistics, which include stochastic optimisation algorithms and Markov chain Monte Carlo methods.
  Email address: georgy.sofronov@mq.edu.au
- **Stefan Trück** is a Professor of Business Analytics, the Co-Director of the Centre for Risk Analytics at Macquarie University, and has been awarded a 2020 ARC Future Fellowship. He is a leading international expert in risk management, financial econometrics and business analytics, including the fields of energy and commodity markets, credit and operational risk management, the analysis of systemic risks, and the economics of climate change.
  Email address: stefan.trueck@mq.edu.au

ACKNOWLEDGEMENTS

This research has been conducted within the Optus Macquarie University Cyber Security Hub and funded by its Risk Management, Governance and Control Program.

Founding Partner
OPTUS

MACQUARIE University

OPTUS MACQUARIE UNIVERSITY

Cyber Security Hub

CRICOS Provider 00002J

This white paper is part of an insight and knowledge-sharing series from the Optus Macquarie University Cyber Security Hub.

The Cyber Security Hub relies on a network of experts across business, government and higher education. It promotes an interdisciplinary understanding of cyber security by bringing together technology, business, legal, policy, security intelligence and psychology perspectives.

The Cyber Security Hub offers a range of services and collaborative opportunities. This includes professional education, hosting events to promote up-to-date knowledge, publishing key insights and updates, and working with partners on their business challenges.

If your organisation would benefit from being a part of a cross-sector network and have a greater understanding of the complex issues surrounding cyber security, please contact us to discuss opportunities for collaboration at cybersecurityhub@mq.edu.au

For more information visit mq.edu.au/cyber-security-hub