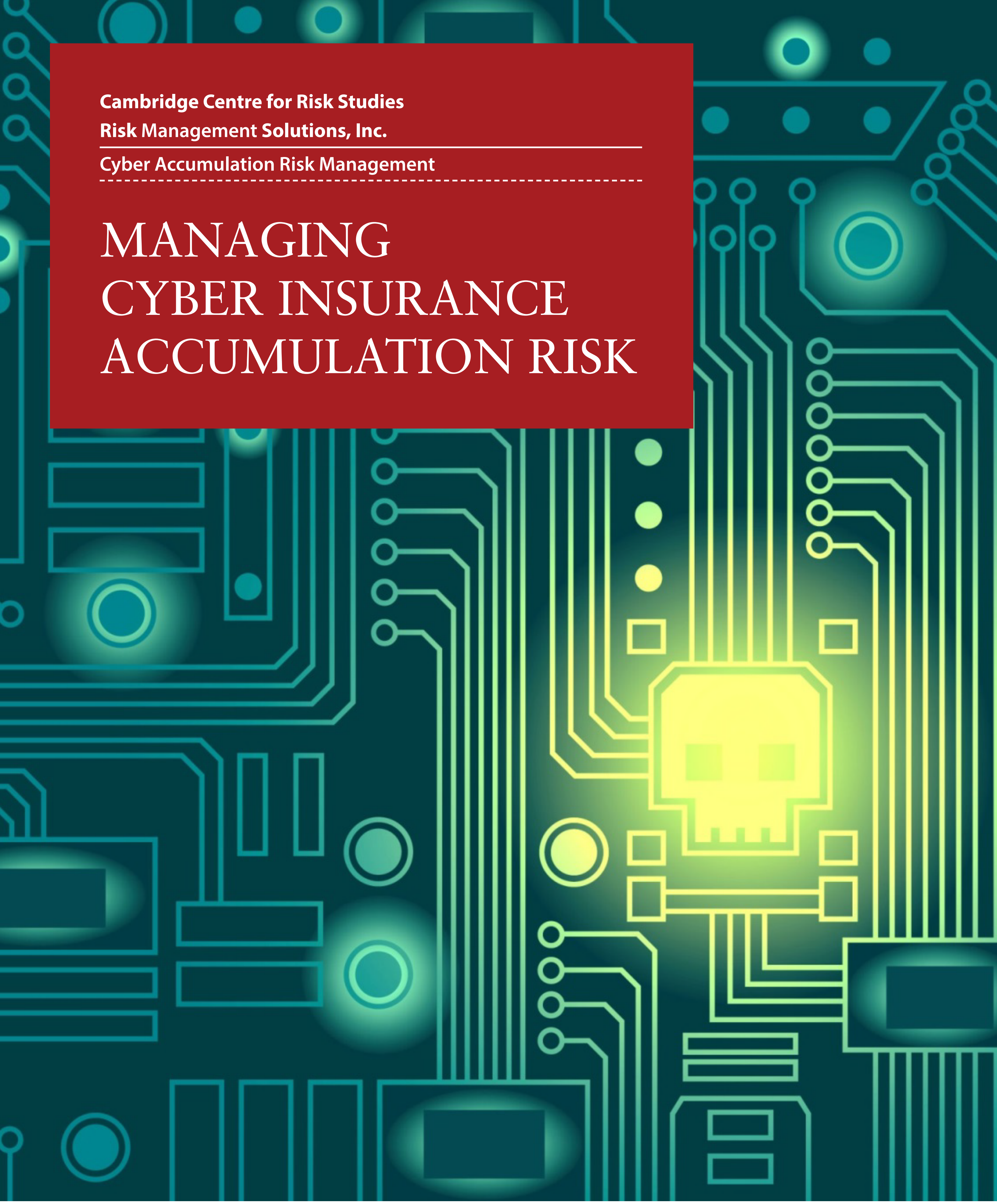


Cambridge Centre for Risk Studies
Risk Management Solutions, Inc.

Cyber Accumulation Risk Management

MANAGING CYBER INSURANCE ACCUMULATION RISK

Centre for
Risk Studies

UNIVERSITY OF CAMBRIDGE
Judge Business School

RMS

Risk Management Solutions, Inc.
Cambridge Centre for Risk Studies
February 2016

Risk Management Solutions, Inc. acknowledges the generous support provided for this research by the following organisations:

Aon Benfield

Axis Capital

Barbican Insurance Group

MS Amlin Plc.

Sompo Canopius Re

RenaissanceRe

Talbot Underwriting

XL Catlin

The views contained in this report are entirely those of the research team of Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, and do not imply any endorsement of these views by the organisations supporting the research.

This report describes hypothetical scenarios developed as accumulation stress tests for risk management purposes. They do not constitute predictions or forecasts of what is likely to happen.

Managing Cyber Insurance Accumulation Risk

Table of Contents

Report citation:

Risk Management Solutions, Inc.; 2016; Managing Cyber Insurance Accumulation Risk; report prepared in collaboration with and based on original research by the Centre for Risk Studies, University of Cambridge.

Risk Management Solutions, Inc.

Cyber Development Team

Dr Andrew Coburn, *Senior Vice President*
Peter Ulrich, *Senior Vice President*
Rob Savage, *Director, Application and Platform Product Management*
Tom Harvey, *Product Manager, Emerging Risk Innovation*
Dr Gordon Woo, *Catastrophist*
Pooya Sarabandi, *Senior Director, Model Development*
Simon Arnold, *Technical Architect, Integration Services*
Edwina Glennie, *Senior Consultant, Management Consulting*
Chris Vos, *Analyst*, *Management Consulting*

Cambridge Centre for Risk Studies

Cyber Research Team

Simon Ruffle, *Director of Technology Research and Innovation*
Éireann Leverett, *Senior Risk Researcher*
Dr Andrew Skelton, *Research Associate*
Jennifer Copic, *Research Assistant*
Siobhan Sweeney, *Risk Fellow*
Ali Rais-Shaghagi, *Research Assistant*
Viktorija Kasaite, *Research Assistant*
Dr Scott Kelly, *Research Associate*
Professor Daniel Ralph, *Academic Director*
Dr Michelle Tuveson, *Executive Director*
Dr Louise Pryor, *Risk Researcher*
Tamara Evan, *Coordinating Editor*

Development Partner Teams

Aon Benfield; Jon Laux, *Senior Consultant, Inpoint Strategy*; Ed Messer, *Specialty Catastrophe Management*; Meredith White, *Director, Catastrophe Modelling*

AXIS Capital; William Fischer, *Chief Underwriting Officer, Axis Re*; Stefan Habereder, *Chief Risk Officer, Axis Re;* Peter Kiernan, *Executive Vice President & Regional President, Axis Re Bermuda;* John Colello, *Executive Vice President Axis Re New York*; Loic Grandchamp, *Vice President Axis Re*; Dan Draper, *Chief Risk Officer, Axis Insurance*; Paul Miskovich, *Senior Vice President, AXIS Insurance*; Dr Katarzyna Kacprzak, *Risk Management Analyst, Axis Re Europe*

Barbican Insurance Group; Geoff White, *Underwriting Manager, Cyber, Technology and Media*; Matt Waller, *Cyber, Technology and Media Underwriter*

MS Amlin Plc.; David Singh, *Group Underwriting Exposure Manager*; Jean-Bernard Crozet, *Head of Underwriting Modelling*; Paul Western, *Head of Casualty Underwriting*

Sompo Canopius Re.; Marek Shafer, *Head of Cat Management*; Chiara Ball, *Political Risk and Terrorism Analyst*; Jeremy Hyne, *Underwriter*; Tim Spencer, *Head of Research*

RenaissanceRe; Jim Maher, *SVP & Chief Risk Officer - US*; James Riley; *AVP, Specialty*; Stephen Burke, *VP, Chief Information Security Officer*

Talbot Underwriting; Russell Bean, *Head of Financial Institutions*; Jahangez Chaudhery, *A&H Class Underwriter*; Charity Bare, *Head of Risk Management*; Ben Kiely, *Exposure Management Analyst*

XL Catlin; Vinita Saxena, *SVP, Enterprise Risk Management*; Kelly Bellitti, *Cyber Actuary, Professional Lines*; Lisa Hansford-Smith, *Cyber, Tech & Media Underwriter*

Foreword

Our society is undergoing a profound digital transformation. As critical exposures become data, commerce electronic, and assets interconnected systems, the key personal, business and economic risks are increasingly cyber in nature. Cyber-related insurance, while currently modest, has the potential to be a fundamental driver of growth for the global re/insurance industry. And while an opportunity, the digital transformation also poses challenges; as businesses and stakeholders throughout society increasingly make mitigating cyber threats a top priority, the industry needs to adapt to remain relevant. An engaged and vital cyber insurance market will not only be good for the industry but will also ensure a more resilient economy.

At RMS, we understand there are many challenges to overcome to realize this vision. One key challenge is accumulation. To allocate the capital needed to provide the necessary coverages, and do so in scale, the industry needs to understand the correlation space for this new class of exposure. We know we can write earthquake exposures in both Japan and California with the confidence that the same event will not impact all these exposures at once. We know to be wary of writing two industrial risks along the same river basin, and the role flood defenses play in mitigating loss. With cyber risks, the contours of systemic accumulation are not as clear.

To develop a framework for multi-line cyber accumulation, we have partnered with several re/insurers and with Cambridge Centre for Risk Studies to explore a number of new modelling strategies to help measure and constrain cyber risk. In this report, we describe our work to analyze cyber loss processes, develop scenarios and modeling parameters, and define exposures. This initiative is an important first step, and we are committed to the long-term pursuit of the research and development program to provide the industry with the models and tools to better quantify, grow and manage this important risk.

With best regards,

Hemant Shah

Hemant Shah

Co-founder and CEO, Risk Management Solutions, Inc.

Executive Summary

This report sets out a complete framework for the assessment and understanding of cyber insurance accumulation risk management. It presents the key concepts in the RMS Cyber Accumulation Management System, a software system for exposure reporting and scenario analytics.

The development of this framework has been supported by a group of forward-thinking insurance companies whose representatives have worked with the research and development teams of RMS, Inc. and the University of Cambridge Centre for Risk Studies to tackle the complex problem of cyber accumulation. The teams have worked together to combine insurance market knowledge with specialist cyber research to address this problem.

The starting point of the framework is a review of the current cyber insurance market, to identify a practical approach to tracking the coverages and product components that are being offered across the market.

Cyber Exposure Data Schema

We present a schema to structure the data that should be captured in an insurer's cyber accumulation management system. The design of the Cyber Exposure Data Schema benefited from consultation with many practitioners across the cyber insurance market and with a number of industry organisations. The Cyber Exposure Data Schema provides a segmentation of the cyber insurance market by enterprise size and business sector that aligns with market demand and cyber risk, together with key aggregation attributes, such as breach of privacy potential and loss potential from internet failure and IT counterparties. It provides an exposure classification that can be monitored and routinely reported. This data standard enables companies wanting to share or transfer risk to provide data to each other in a consistent format, which should help expand risk data interchange across the market.

Accumulation is a function of the cyber insurance coverages provided. We explicitly identify the categories of coverage to identify loss potential in a portfolio. This can extend beyond affirmative cyber products to potential silent exposures in 'all risks' policies covering property and casualty without explicit cyber exclusions.

Changing Cost Landscape for Cyber Risk

We discuss how the cyber compensation landscape is changing, and the legislative and litigation trends that are changing the costs of cyber claims. We provide a structure for stress testing the assumptions about the cost components of future claims as part of good practice in accumulation risk management.

Five Cyber Loss Processes

The various coverages in affirmative cyber insurance products can be triggered by a number of different cyber loss processes. We identify five key cyber loss processes that have the potential to cause widespread and correlated losses and show how these map to common coverage categories. These form the key models of cyber accumulation stress test scenarios. We set out a framework for analysing these cyber loss processes, for understanding the main concepts that drive the loss processes, that have the potential to cause correlated loss across many insured accounts, and that constitute a cyber catastrophe.

We explain each of the loss processes, develop the controlling metrics that underlie the incidents – and the potential extremes – and define a specific severity scale for each loss process. These severity scales are an important new contribution to the management of cyber risk, providing a link between the underlying cyber loss process and the insurance claims payouts.

Frequency-Severity Distributions of Loss

An important concept that frames the models of cyber loss process is the definition of a frequency-severity distribution of loss: claims incurred in a single year. In some cases these can be calibrated to background occurrence rates from claims experience. The definition put forward by this report provides a framework for stressing the occurrence rate and severity of claims that could arise from an extreme cause of correlated loss across the entire portfolio. This framework is consists of accumulation scenarios, developed as hypothetical narratives with variants of extreme but plausible increases in the frequency-severity incidence of each one.

Cyber Data Exfiltration

Systemic release of confidential customer records from many corporate enterprises

Accumulation Stress Test Scenario: **Leakomania**

Three rare 'zero-day' vulnerabilities provide a criminal gang with the capability to scale data exfiltration attacks across thousands of companies. Billions of confidential data records are leaked in a few months, more than the total number of confidential data records leaked in the past ten years.

Denial-of-Service Attack

Attacks to disable websites and disrupt online business activity across multiple companies

Accumulation Stress Test Scenario: **Mass DDoS**

Hacktivists build the largest distributed denial-of-service capability yet seen and target it at capitalist corporate websites to disrupt e-commerce. They generate DDoS traffic at many multiples of the most extreme peak rates seen on the internet, which is concentrated on insured businesses.

Cloud Service Provider Failure

A large number of companies have business operations disrupted by losing cloud-based functionality when a major cloud service provider company suffers a disruption

Accumulation Stress Test Scenario: **Cloud Compromise**

A technical error leads to an outage at a leading cloud service provider, causing its customers to lose service for many hours until they are gradually reconnected. The outage is on a scale never experienced by a commercial CSP, in terms of proportion of their customers affected and reconnection times.

Financial Transaction Cyber Compromise

Theft of large sums in cyber attacks on multiple enterprises that carry out financial transactions

Accumulation Stress Test Scenario: **Financial Transaction Interference**

A coordinated cyber heist operation on many financial services companies to syphon funds from transactions, obtain cash from ATMs, and carry out insider trading using stolen information. It is carried out on a scale that is orders of magnitude larger than any known cyber theft to date.

Cyber Extortion

Many companies are held to ransom by hackers disabling IT functionality to obtain payoffs

Accumulation Stress Test Scenario: **Extortion Spree**

Hackers graduate from personal computer ransomware to create a sophisticated system of encrypting SME business corporate servers. They attack large numbers of enterprises, and demand high ransom payments, on a scale far beyond anything seen even in the PC environment to date.

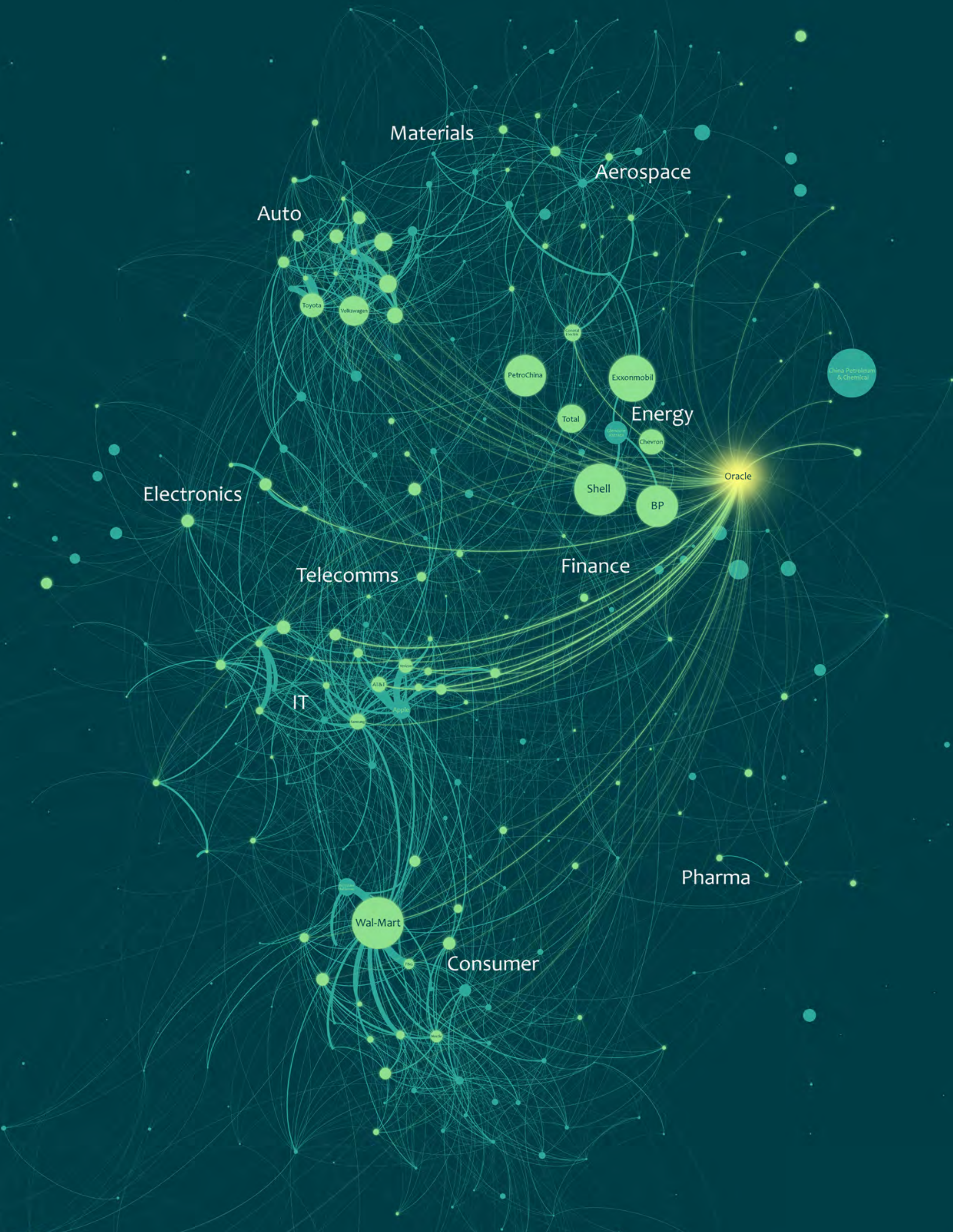
Portfolio Specific Loss Estimation

Insurers can apply these accumulation scenarios to their own portfolios using the data schema and the RMS Cyber Accumulation Management System to model the loss to their portfolio. This enables routine monitoring of accumulation risk, and allows a company to set their risk appetite on an informed basis.

It is important to consider several different types of loss processes in monitoring accumulation risk. The most common concern of cyber insurers – data exfiltration losses – may not pose the greatest catastrophe potential. Companies that are focused on the small and medium-sized enterprise sectors will want to consider their accumulation exposure to different types of cyber loss processes than those that concentrate on premier enterprises. These scenarios and loss processes also have significantly different impacts on different business sectors, so portfolios with different sectoral mixes will find they have different risk profiles.

Expanding Capacity Safely

We have laid out an approach to monitoring and managing cyber accumulation risk. We believe that it provides a framework for companies to assess their own risk appetite for cyber, and will prove a useful tool for analysing diversification and exploring loss potential. We hope that it will enable insurers to gauge their loss potential with more information than they had previously, and to develop strategies for safely expanding their capacity in the cyber insurance market.



"Systemic Cyber Threats", the world's largest commercial companies and their trading relationships, showing the systemic linkages through major software providers, using Oracle as an example; *created by Dr Andrew Skelton*

Managing Cyber Insurance Accumulation Risk

1 Accumulation Management and Cyber Risk

Market surveys suggest that demand for cyber insurance significantly exceeds the capacity currently provided by the insurance industry.

The primary reason that most insurers give for being cautious about expanding capacity is the accumulation risk posed by cyber. Cyber is a relatively young threat with a short history of claims experience, which demonstrates that the risk is constantly changing and evolving. Media reports are full of individual cases of major data breaches or cyber attacks on high-profile technology targets. The main fear is that the cyber threat is inherently scalable – a single malicious email can reach hundreds of thousands of company recipients with one click of a mouse. Cyber risk is clearly systemic – it is spread through interconnectivity: the internet, communications, and internal and external networks. These connections are neither obvious nor easily tracked.

It is difficult for insurers to assess the potential for a major cyber incident to trigger losses in many of their insureds at the same time. There have been a number of very large claims from individual companies, but there has not yet been a truly systemic cyber 'catastrophe event' that has triggered large numbers of companies to make major claims on their cyber insurance policies. Assessing the Probable Maximum Loss (PML) from a peril is a key determinant for an insurance company to set their risk appetite. This needs to incorporate how severe the risk may be, together with some indication of how unlikely that scenario is to occur. Without an ability to set a PML, the insurer is obliged to play safe and assume that their entire limit is at risk from a single event, which restricts their capacity and the efficiency of utilising risk capital.

PMLs for other insurance lines from conventional perils have been established from experience and analytics. With property insurance and the potential for large losses from many individual insureds, geographical proximity provided a first-order accumulation management technique: buildings that were far enough apart not to be impacted in the same explosion, or later on, in the same hurricane wind field, earthquake attenuation zone, or flood catchment area, were unlikely to suffer a correlated loss from the same event.

With cyber insurance, the underlying potential correlation that could cause thousands of insured companies to have a loss from the same cause is not as intuitive. Identifying this needs domain subject matter expertise combined with a risk analytics framework that extrapolates evidence-based information to potential scenarios. The RMS, Inc. and Cambridge Centre for Risk Studies cyber risk development team has progressed proven techniques from previous studies to identify key accumulation management issues.[1]

This report provides a framework for understanding and managing accumulation risk for cyber insurance. It introduces a number of new and important concepts for quantifying accumulation risk. This report:

- Sets out the data requirements that a company needs to track and monitor its potential accumulations from cyber insurance
- Identifies the insurance coverage categories that are most susceptible to systemic cyber events
- Defines five key cyber loss processes that are drivers of accumulation risk
- Proposes severity scales, frequency incidence distributions, and modelling frameworks for each of the five cyber loss processes
- Sets out the exposure landscape of corporate purchasers of cyber insurance, and the issues and characteristics of the insureds that are key in assessing accumulation risk

[1] The development team for this project has published previous scenarios of hypothesised cyber catastrophes, including Sybil Logic Bomb (Cambridge (2013)) and Lloyd's Business Blackout (Lloyd's (2015)).

- Considers the loss costs that arise from these processes and identifies the trends and determinants of future costs including the legal liability landscape, and the processes of dealing with cyber events
- Proposes and describes an accumulation management scenario for each of the five cyber loss processes that can be considered plausible but severe, and explains the constraints on severity and influences on the likelihood of these scenarios

2 Cyber Insurance Exposure Data Schema

Managing cyber accumulation in a portfolio of insured policies requires a specific data structure to record the attributes of exposure that could potentially correlate. This has been identified as a general need across the insurance market, including the United States, Europe, and most of the emerging markets for cyber insurance.

During the course of this project, the development team has worked with the client development partners, together with a number of insurance industry organisations, and many of the leading practitioners writing cyber insurance to develop a Cyber Insurance Exposure Data Schema, through several iterations of published consultation rounds and industry feedback. This has been published as a companion paper to this report:

Cambridge Centre for Risk Studies and Risk Management Solutions, Inc.; 2016; Cyber Insurance Exposure Data Schema v1.0; Cyber Accumulation Risk Management working paper.

The schema provides a specification for structured information records in a database, to capture cyber insurance exposure in a way that can be standardized across insurance industry participants, to:

a) Provide a standardized approach to identifying, quantifying and reporting cyber exposure

b) Facilitate risk transfer to reinsurers and other risk partners, and risk sharing between insurers

c) Provide a framework for exposure-related dialogues for risk managers, brokers, consultants and analysts

d) Enable companies and other analysts and vendors to develop their own cyber accumulation risk management analytics

The Cyber Exposure Data Schema has been adopted in the RMS Cyber Accumulation Management System and incorporated into the design of the RMS accumulation scenarios and other risk management tools.

A company that reviews its own cyber insurance exposure using the schema can:

- Report exposure aggregates by different types of coverage and potential loss characteristics to a level of granularity that can inform risk appetite decisions
- Estimate losses from scenarios or other types of risk models to the exposure recorded in the database
- Identify insurance policies that may have ambiguity in whether they would pay out in the event of a cyber incident, enabling companies to take action to clarify silent or affirmative covers
- Enable companies to share or transfer information about exposures in a consistent and standardized format for use in risk transfer transactions, benchmarking exercises, and regulatory reporting

Exposure is defined at sufficient granularity to allow risk models and scenarios to apply loss assumptions to subsets of exposure, which can be identified as accumulation categories. These may be one or a combination of coverages offered in policies, enterprise size, business sector, geographic region and jurisdiction, companies with exposure to their cloud service providers, exposure to internet access risk, data exfiltration potential, and other cyber risk attributes identified in the schema.

2.1 Cyber Insurance Market Practice Overview

It is important that any proposed exposure data schema fits current practice, is aligned with practical issues of implementation, and reflects the main priorities for the business user. The schema is based on an extensive review of cyber insurance market practice – current activities and common products and processes in the offerings of cyber insurance, and the exposures and business priorities of companies that write cyber insurance.

The cyber market practice review included extensive interviews with representatives from different sectors of the cyber insurance market, including underwriters, exposure managers and analysts, primary insurers in the U.S., London and European markets, reinsurers, intermediaries, advisors and management consultants, and collaboration with compilers of insurance market information. It includes a compilation of public domain documents describing the insurance product offerings currently offered in the market, confidential internal documents provided under non-disclosure by a number of market participants, and an extensive review of published reports, market studies, and literature.[2]

2.2 Cyber Exposure in the Insurance Market

Cyber exposure – i.e. insurance policies that could trigger claims in the event of a cyber attack –can be categorised into the following four categories:

A) **Affirmative Standalone Cyber Cover**: Specific policies for data breach, liabilities, property damage and other losses resulting from information technology failures, either accidental or malicious. This is generally known as cyber liability insurance cover (CLIC) and includes:

- Standalone policies being offered for cyber liability insurance cover (CLIC);
- Technology errors and omissions (E&O) liability insurance, available as a specific insurance product for the providers of technology services or products to cover both liability and other loss exposures.

B) **Affirmative Cyber Endorsements:** Cyber endorsements that extend the coverage of a traditional insurance product, such as commercial general liability, to cover cyber-induced losses, typically privacy breaches.

C) **Silent Cyber Exposure – Gaps in Explicit Cyber Exclusions:** There are a range of traditional policies, such as commercial property insurance, that have exclusion clauses for malicious cyber attacks, excepting certain nominated perils such as: Fire; Lightning; Explosion and Aircraft Impact (FLEXA). These policies have exposure to a cyber attack if one of the nominated perils were triggered to cause a loss, however unlikely this might be.

D) **Silent Cyber Exposure – Policies without Cyber Exclusions:** Many insurance lines of business incorporate ‘All Risks’ policies without explicit exclusions or endorsements for losses that might occur via cyber attacks. Insurance business sectors that may contain silent cyber exposure include: property; casualty; energy; marine; aviation; aerospace; specialty; auto; personal lines; terrorism; and war and political risk.

The Cyber Exposure Data Schema provides a categorization of coverage by types of cyber-induced loss for use across all of these areas of exposure and enables insurers to flag cyber exposures in the policies they write.

Identifying silent cyber exposures entails a review of the contractual language, clarification of perils, and coverage areas provided in the policies in an insurance company’s portfolio. Many companies currently identify ambiguities and silent cyber exposure in coverage areas and, where possible, move the insured to affirmative cyber cover.

[2] Examples of market review literature are included as recommended reading at the end of this report.

2.3 Coverages Provided in Affirmative Cyber Insurance

At least 35 insurers currently offer products for standalone affirmative cyber liability insurance.[3] To support the development of a Cyber Exposure Data Schema, the key categories of loss coverage were examined for a large sample of insurance products on the market. Coverage analysis was carried out on 26 products – i.e. two-thirds of the products currently estimated to be on the market. This identifies 19 primary categories of coverage that are provided in one product or another in the market today. These 19 cyber loss coverage categories, defined in Table 2.1, form a key part of the data structure to manage accumulation risk.[4]

The coverage categorization can be treated as hierarchical, with each category capable of being further subdivided into component parts if required. It is fairly typical for coverage to be sublimited by some of these coverage categories – i.e. insurance policies will identify limits, retentions, and other contractual conditions for this category of coverage separately from the others, combined with an overall limit and policy terms for the total policy. To quantify cyber exposure effectively, these main categories of coverage need to be identified in the policies and products being offered in a cyber insurance portfolio.

2.3.1 Wide Variation in Coverage

Coverage provided by insurance products currently on the market varies widely. The industry has not converged on a single standard product. In the 26 insurance products reviewed, almost no two products have exactly the same number and types of coverages in their offering. The number of our categories of cyber coverages in these products ranges from 3 to 12, with an average of just over 7.

The coverage types that are most common across the market are shown in Table 2.2. The primary focus of most products is for breach of privacy events, data and software loss, and incident response costs. Almost all of the affirmative products offer these, reflecting a focus on risks from the compromise of Information Technology (IT) systems. Coverage for physical damage, injury, and environmental consequence are some of the least common offered, illustrating that cyber threats to Operational Technology (OT), the control systems for physical processes, are less well recognized and in demand than IT threats.

Accumulation management requires monitoring the insurance exposure to these coverages. Insurers should quantify their total limits by these categories and monitor them routinely. Each insurer may be offering a product that includes a set grouping of these coverages, so that all of their accounts may have the same collection of coverage categories. However, the schema enables other coverages to be considered, and other products that may include a different grouping of covers can then be included and accumulations monitored across multiple products in the same portfolio. The sublimits for individual coverage categories can be captured, and differentiated from coverages that are included in the total policy limit. Total limits and exposures for each and all of the loss coverages can be monitored with this data structure.

This provides one level of granularity for exposure monitoring. There are a number of different types of cyber loss processes that may trigger one of more of these coverages, but having explicit identification of the key categories of coverage is an important management requirement.

2.4 Cyber Underwriting and Risk Selection Practices

Each company has its own set of data attributes that it monitors and uses to manage its cyber risk. In some cases, these attributes are confidential and viewed as a competitive advantage. A number of companies are partnering with cyber security specialists to provide insights into risk selection and in some cases to provide incident response services and security advice to insureds.

[3] Advisen and PartnerRe (2014)

[4] The coverage categorization of the Cyber Exposure Data Schema extends and reframes a cyber loss categorization scheme published by a government and insurance industry study developed by a steering group of 15 insurance companies and several industry organizations and government agencies. Marsh & UK Government (2015).

Table 2.1: Cyber Insurance Loss Coverage Categorization in Cyber Insurance Exposure Data Schema

v1.0 Code	Cyber Loss Coverage – Primary Category	Lloyd's Min Recommended	1st party	3rd party	Description
1	**Breach of privacy event**	Security Breach of Privacy	1st		The cost of responding to an event involving the release of information that causes a privacy breach, including notification, compensation, credit-watch services and other third party liabilities to affected data subjects, IT forensics, external services, and internal response costs, legal costs.
2	**Data and software loss**	Replacement of Lost Data and Software	1st		The cost of reconstituting data or software that have been deleted or corrupted.
3	**Network service failure liabilities**	Security Breach of Privacy		3rd	Third-party liabilities arising from security events occurring within the organisation's IT network or passing through it in order to attack a third-party.
4	**Business Interruption**	Business Interruption	1st		Lost profits or extra expenses incurred due to the unavailability of IT systems or data as a results of cyber attacks or other non-malicious IT failures.
5	**Contingent Business Interruption**	Business Interruption		3rd	Business interruption resulting from the IT failure of a third party, such as a supplier, critical vendor, utility, or external IT services provider.
6	**Incident response costs**	Security Breach of Privacy	1st		Direct costs incurred to investigate and close the incident to minimise post-incident losses. Applies to all the other categories/events.
7	**Regulatory and defence coverage**	Regulatory Fines	1st		Covers the legal, technical or forensic services necessary to assist the policyholder in responding to governmental inquiries relating to a cyber attack, and provides coverage for fines, penalties, defence costs, investigations or other regulatory actions where in violation of privacy law, and other costs of compliance with regulators and industry associations. Insurance recoveries are provided where it is permissible to do so.
8	**Liability – Product and Operations**	Liability		3rd	Third party liabilities arising in relation to product liability and defective operations.
9	**Liability – Technology Errors & Omissions**	Tech E&O / Programming ENO		3rd	Coverage for third party claims relating to failure to provide adequate technical service or technical products including legal costs and expenses of allegations resulting from a cyber attack or IT failure.
10	**Liability – Professional Services Errors & Omissions**	Liability		3rd	Coverage for third party claims relating to failure to provide adequate professional services or products (excluding technical services and products) including legal costs and expenses of allegations resulting from a cyber attack or IT failure.
11	**Liability – Directors & Officers**	Liability	1st		Costs of compensation claims made against the individual officers of the business, including for breach of trust or breach of duty resulting from cyber-related incidents and can result from alleged misconduct, or failure to act in the best interests of the company, its employees, and its shareholders.
12	**Multi-media liabilities (defamation and disparagement)**	Liability	1st	3rd	Cost for investigation, defence cost and civil damages arising from defamation, libel, slander, copyright / trademark infringement, negligence in publication of any content in electronic or print media, as well as infringement of the intellectual property of a third party.
13	**Financial theft & fraud**	Extortion	1st		The direct financial loss suffered by an organisation arising from the use of computers to commit fraud or theft of money, securities, or other property.
14	**Reputational damage**	Reputational Damage / Public Relations	1st		Loss of revenues arising from an increase in customer churn or reduced transaction volumes, which can be directly attributed to the publication of a defined security breach event.
15	**Cyber extortion**	Extortion	1st		The cost of expert handling for an extortion incident, combined with the amount of the ransom payment.
16	**Intellectual property (IP) theft**	Replacement of Lost Data and Software	1st		Loss of value of an IP asset, expressed in terms of loss of venue as a result of reduced market share.
17	**Environmental damage**	Physical Damage	1st		Cover for costs of clean up, recovery and liabilities associated with a cyber induced environmental spill or release.
18	**Physical asset damage**	Physical Damage	1st		First-party loss due to the destruction of physical property resulting from cyber attacks.
19	**Death and bodily injury**	Bodily Injury		3rd	Third-party liability for death and bodily injuries resulting from cyber attacks.

Table 2.2: Most Common Cyber Loss Coverages Included in Cyber Insurance Products on the Market

v1.0 Code	Cyber Coverage	% of Products Offering this Cover (Sample of 26)
1	**Breach of privacy event**	92%
2	**Data and software loss**	81%
6	**Incident response costs**	81%
15	**Cyber extortion**	73%
4	**Business interruption**	69%
12	**Multi-media liabilities (defamation and disparagement)**	65%
7	**Regulatory and defense coverage**	62%
14	**Reputational damage**	46%
3	**Network service failure liabilities**	42%
5	**Contingent Business Interruption**	33%
9	**Liability – Technology Errors & Omissions**	27%
10	**Liability – Professional Services Errors & Omissions**	23%
13	**Financial theft & fraud**	23%
16	**Intellectual property (IP) theft**	23%
18	**Physical asset damage**	19%
19	**Death and bodily injury**	15%
-	**Cyber terrorism**	12%
11	**Liability – Directors & Officers**	13%
8	**Liability – Product and Operations**	8%
17	**Environmental damage**	4%

Underwriting processes are even more disparate and varied across the industry than coverage offerings. Table 2.3 shows a listing of attributes, though not an exhaustive list, gathered from a review of cyber underwriting processes in the market.[5] There is a wide range of opinion on the relative importance of these factors. In one survey of insurers underwriting cyber insurance less than a quarter of the 73 respondents agreed on any of the attributes as the most important in underwriting cyber risks.[6] It is difficult to standardize these factors across the industry and the Cyber Exposure Data Schema does not attempt to do so. Companies are encouraged to create their own user defined variables in their accumulation management systems for their preferred risk factor data that is not incorporated in the schema.

Only some of these underwriting risk factors are important for accumulation management. It is obviously important that an insurer's portfolio of risks is written profitably, and that the companies it insures are not poor risks. Insurers select the companies that they underwrite on the basis of how likely the companies are to make a claim, particularly when capacity is limited. The quality of an underwritten portfolio, in terms of the ratio of premium income to claims paid, is an important dynamic in the business proposition of all insurance, and is a particular focus of building up claims experience in an emerging class of business such as cyber. However, the attributes that define the potential for many correlated losses to occur across a portfolio of insureds are significantly distinct from risk selection attributes, while sharing several of them. The portfolio management of exposure accumulation is a different process and requires a different system than the process of underwriting and tracking their claims experience against their risk selections.

[5] Underwriting and risk selection practices were reviewed by compiling cyber insurance policy application forms, interviewing selected cyber underwriters, and cyber insurance underwriting market practice reviews by others, for example Verisk (2014); CRO Forum (2014); Airmic (2012);

[6] Verisk (2014).

Table 2.3: Examples of Attributes of a Company's Cyber Risk Used in Cyber Insurance Underwriting or Risk Selection

1. Company Activities and Profile

- Business sector and activities
- Company financials
- Size of company (revenue)
- Number of employees
- Historical experience of cyber events
- Business dependency on IT
- Enterprise transacts with general public
- Online trading volume

2. Risk Management Processes and Security Culture

- Enterprise Risk Management Philosophy
- Incident response plan
- Regulatory and PCI compliance
- Chief Information /Chief Privacy Officer
- Procedures for employee termination
- Remote access procedures
- Staff awareness and training on IT security

3. Confidential Records and Data Assets

- Types of records and confidential data held
  - *PII - personally identifiable information*
  - *PCI - payment card information*
  - *PHI - personal health information*
  - *CCI - commercially confidential information, trade data and secrets*
  - *IP - intellectual property*
- Volumes of records and data stored, including average and maximum
- Data shared with third party or cloud provider
- Intellectual property
- Encryption practices of confidential records

4. IT Network Configuration and Storage Security

- Structure, size, and configuration of network
- Operating systems and main systems
- Firewall: type; updating and testing
- Sizing of firewalled separate data storage compartment
- Network security system software and provider
- Cloud service provider
- Listing of major suppliers/vendors of software or system components
- Processes for patching vulnerabilities

5. IT and Data Transfer Security Practices

- Number of IT Staff
- In-house and outsourced IT services
- Anti-virus systems and suppliers
- Cyber security testing procedures and audits
- Cyber incident response plan
- Mobile device security, tablets, smartphones
- USB controls
- Email protocols and email security system
- Backup processes and recovery
- Laptop encryption and security
- Password management and change processes

6. Other Underwriting Procedures

- Operational Technology (OT) Security
- Hardware assessments
- External security audit or penetration tests
- Wide range of other questions and assessments

Most insurance companies have separate systems for underwriting and accumulation risk management across the portfolio.

This analysis and report focuses on accumulation management – to assess the potential for a portfolio of policies to suffer high losses through correlated events.

2.5 Cyber Exposure Data Schema v1.0

The Cyber Exposure Data Schema provides a standardized minimum set of information to augment existing information about the policy details, account holder, relationship history, insurance structure limits and retentions, contractual terms and conditions, value, and financial information.

For full details, refer to the published companion white paper to this report. A brief summary is provided here.

In addition to the cyber loss coverage categories in the policy, as discussed above, the schema provides recommended data categories and formats for the attributes of the company being insured:

2.5.1 Geographical Jurisdiction

To manage cyber accumulations by geographical market, accounts are identified by the jurisdiction that determines pay outs and regulatory attitudes to cyber loss. This is by country, recorded using two letter ISO 3166 codes (Alpha-2 code) that uniquely define each country of the world.

2.5.2 Cyber Peril Coding

Recognising the cause of loss through a peril code helps to identify cyber activity that relates to insurance policy wordings and loss types, for example compatibility with Lloyd's risk codes in the London Market:[7]

- **Cyber Security Data and Privacy Breach** – First and third-party claims from a data breach (or threatened breach) where no physical damage has occurred (equivalent to Lloyd's risk code 'CY').
- **Cyber Security Property Damage** – First and third-party claims from physical property damage due to a breach of security event (equivalent to Lloyd's risk code 'CZ')

2.6 Enterprise Size

Attributes of the company being insured for cyber includes identification of unique insured enterprises, so that any aggregation of accounts, potentially from multiple sources, will identify the legal entities covered.

Size of enterprise is an important accumulation and segmentation concept for the cyber market. Most writers of cyber insurance differentiate at least large companies from small-and-medium-enterprises (SMEs).

Size of organization is an exposure differentiator, as well as a risk factor for some of the key cyber loss processes, such as data exfiltration. The number of employees in a company makes it more likely that one of them may succumb to a malicious trick or fail to carry out a security procedure.

The annual **revenue of a company** is an important determinant of potential losses, targeting by external agents, quantity of business interruption potential, and the scale and sophistication of its likely IT infrastructure and other risk factors.

Accumulation management and segmentation of risk by company size is important, not only because these markets have different requirements and insurance purchasing activity, but because loss potential, concentration risk, and diversification potential is determined by this categorization.

Table 2.4 provides the segmentation of enterprises by their sizing for use in cyber accumulation risk management, with banding based on definitions used in U.S. Census Bureau for statistics of US businesses. Application in other countries requires different revenue thresholds.

The 'Premier' group of companies represents the largest enterprises in that market, for example the Fortune 1000 companies in the United States, listed public companies that are complex international organisations.

Table 2.4: Size of Enterprises for Use in Cyber Accumulation Management (U.S. Categorization)

	Number of Employees		Revenue	
	Typical Min	Typical Max	Typical Min	Typical Max
Premier	>2000		>US$3 B	
Large	500	2,000	$40 M	$3 B
Medium	100	500	$10 M	$40 M
Small	20	100	$2 M	$10 M

2.7 Business Sector

Market segmentation for cyber is also commonly reported by business sector, and this is important for exposure management, market development, and for the risk characteristics of companies in those sectors.

Table 2.5 provides a high-level business sector classification that incorporates most of the terminology and classes in common use in the cyber insurance market and that encompasses the main activity sectors in the economy and segmentation used in statistical reporting and analysis.

[7] Lloyd's (2015) *Lloyd's Risk Codes Guidance and Mappings.*

Two of the key sectors, Information Technology and Financial Services, are each further subdivided into three subsectors. This reflects the importance of these sectors as key markets for purchasing cyber insurance, and where additional granularity is required by cyber insurance practitioners. Other sectors could similarly be subdivided in future versions of the schema.

Classifications of enterprises operating in the economy can be made extremely granular. Most industry classification codes are hierarchical, and can be increasingly subdivided. North American Industrial Coding System (NAICS) is the system preferred by most of the companies who operate a coding system of this type, with SIC being a second but less common practice. We recommend that companies capture the NAICS code for their policy-holders, and that the published schema includes conversion tables from NAICS (and concordance to convert from SIC) to the cyber accumulation categories for each business sector in Table 2.5.

2.8 Cyber Risk Attributes

The Cyber Exposure Data Schema captures a manageable number of cyber risk attributes to explore potential loss from a number of the key cyber coverage categories.

Not all insurers currently receive these details from their insureds, or capture them in their exposure management systems, but these are proposed as desirable data for accumulation management.

2.8.1 Breach of Privacy Potential

Number and type of confidential records held by an enterprise that could potentially be lost if it were breached, including:

- Personally Identifiable Information (PII)
- Payment Card Information (PCI)
- Personal Health Information (PHI)

2.8.2 BI Potential from Internet Failure

To identify the potential for systemic correlated loss arising from an outage of the internet on the business activity of the insureds, for each account the schema captures the estimated business interruption value per hour if internet connectivity is lost.

2.8.3 BI Potential from IT Counterparty: Named Cloud Service Provider(s)

To identify the potential for systemic correlated loss arising from the failure of a shared Cloud Service Provider (CSP), for each account the schema captures the estimated business interruption value per hour of outage from named CSPs (top three used by the policyholder).

2.8.4 BI and Financial Loss Potential: Named Payment System Provider(s)

To identify the potential for systemic correlated loss arising from the compromise of a common financial transaction system provider, for each account the schema captures the monthly transaction volumes with named payment system providers (top three used by the policyholder).

Table 2.5: Business Sector Classification for Managing Cyber Accumulation Risk

V1.0 Code	Business Sector	Description
1	**Information Technology**	
1.1	**IT - Software**	Companies involved in the design, development, documentation, and publishing of computer software
1.2	**IT - Hardware**	Companies engaged in manufacturing and/or assembling computers (mainframes, personal computers, workstations, laptops, and computer servers) and peripheral equipment (e.g. storage devices, printers, monitors etc.)
1.3	**IT - Services**	Companies providing hosting or data processing services (inc. Cloud and streaming services); internet publishing and broadcasting content (inc. social media); internet search portals; services relating to computer systems design, computer facilities management, computer programming services, and computer hardware or software consulting.
2	**Retail**	Retailers to general public, sellers of goods and services both in retail stores and online, wholesalers and distributors.
3	**Financial Services**	
3.1	**Finance - Banking**	Companies engaged in commercial banking, savings institutions, credit unions, credit card issuing, sales financing, mortgage and loan companies and brokers, financial transaction processing, reserve and clearinghouse activities, and central banking.
3.2	**Finance - Insurance**	Direct insurance carriers, reinsurance carriers, and insurance agencies and brokerages.
3.3	**Finance - Investment management**	Companies engaged in investment banking, securities dealing and brokerage, commodity contracts dealing and brokerage, securities and commodity exchanges, investment clubs and venture capital, portfolio management, investment advice, and legal entity funds and trusts
4	**Healthcare**	Companies providing goods and services to treat patients with curative, preventive, rehabilitative, and palliative care.
5	**Business & Professional Services**	Occupations providing specialist business advice and services. Some professional services require holding professional licenses such as architects, auditors, engineers, doctors and lawyers.
6	**Energy**	Companies involved in the exploration, extraction and development of oil or gas reserves, oil and gas drilling, or integrated power firms.
7	**Telecommunications**	Companies facilitating exchange of information over significant distances by electronic means.
8	**Utilities**	The utilities sector contains companies such as electric, gas and water firms and integrated providers
9	**Tourism & Hospitality**	Companies providing services for tourism, travel, accommodation, catering and hospitality
10	**Manufacturing**	Companies making or processing goods, especially in large quantities and by means of industrial machines
11	**Pharmaceuticals**	Pharmaceutical industry develops, produces, and markets drugs or pharmaceuticals for use as medications. Pharmaceutical companies may deal in generic or brand medications and medical devices.
12	**Defence / Military Contractor**	Defence industry comprises government and commercial industry involved in research, development, production, and service of military materiel, equipment and facilities
13	**Entertainment & Media**	Enterprises involved in providing news, information, and entertainment: radio, television, films, theatre
14	**Transportation/Aviation/Aerospace**	Companies facilitating the transportation of goods or customers. The transportation sector is made up of airlines, railroads and trucking companies.
15	**Public Authority; NGOs; Non-Profit**	National or local government agencies, non-governmental and non-profit organizations
16	**Real Estate, Property & Construction**	Companies managing, developing, and transacting property consisting of land and buildings, along with its natural resources such as crops, minerals, or water
17	**Education**	Colleges and universities, independent and unified school districts, student loans and tuition companies
18	**Mining & Primary Industries**	Companies involved in the mining, quarrying, and processing of extracting minerals, coal, ores, main commodities, and natural resources.
19	**Food & Agriculture**	Those involved in the food industry, including production, processing, distribution, and wholesale supply
20	**Other**	

2.8.5 Cyber Security Assessment

There is a wide variety of approaches adopted by insurance companies to select their insureds on the basis of their quality of cyber security hygiene. To respond to requests to capture the importance of security standards at insured enterprises, the data schema includes a cyber risk attribute of cyber security assessment. For use in a standard process of accumulation management that might need to aggregate across different security assessments, the wide variety of approaches to security assessment and scoring systems in use need to be aligned. The schema has capacity for the insurer to use the scoring system or certification standard of their choice, but recommends that they benchmark the scoring system or certification standard to the percentile of the total number of enterprises in that jurisdiction that are expected to qualify for that score, ranked by quality of cyber security. For example "a security score of XX means that this enterprise is in the top 10% of enterprises in the United States, ranked by quality of cyber security". This will enable accumulation management by percentiles of different security quality in the population of enterprises in that jurisdiction.

3 Understanding Cyber Exposure for Accumulation Management

The cyber insurance market – those buying affirmative cyber insurance cover – consists predominantly of the companies that make up the economy, with some public sector and non-profit purchasers. Understanding the landscape of the corporate market, and what that constitutes in terms of exposure, is important in establishing plausible bounds for accumulation and the types of scenarios that could cause plausible but severe correlated losses across a portfolio that represents a selection from the entire population of companies at risk. Many – in fact, most – of these companies are not purchasers of cyber insurance yet. They represent the potential market for cyber insurance.

Developing an optimum strategy for cyber insurance requires managing the levels of accumulation across segmentation sectors of the market, identifying any areas of over-concentration, and ensuring that there is sufficient diversification across the market. Table 3.1 illustrates the cyber accumulation segmentation of the US economy by number of companies in each segment. Insurers should monitor their penetrations into these populations of corporate customers, and manage their potential losses through accumulation scenarios that will impact some of these sectors more than others.

The United States is the largest market for cyber insurance and the largest concentration of geographical exposure. There are around 600,000 companies in the United States of any significant size. The companies in each of these segments have particular characteristics of cyber insurance needs and activities in the digital economy that require risk protection. Smaller companies require different insurance products, coverage packages, pricing structures, and service support than larger ones. Company size determines their appetite for the policy limits they buy, which affects the portfolio of exposure that an insurer has to manage.

Each of the segments, and the companies within it, also vary in terms of market demand for cyber insurance, awareness of their cyber risk, pricing tolerance, and appetite for purchasing protection. Insurers may need to develop specialized expertise to underwrite successfully and profitably in certain sectors.

The 'digital' economy, or 'knowledge' economy, is rapidly growing as a proportion of the corporate output of the economies of advanced countries. The digital economy has its own characteristics and exposure landscape, which is very different from the exposure that makes up the traditional portfolios of property insurers, for example. Property represents the physical 'means of production' in the corporate economy: the assets of factories, commercial office buildings, equipment, and industrial plants that constitute the core resources of traditional business activities over the past few centuries. For many years insurers have helped the manufacturing, industrial, and service economies protect their physical assets from the risk of damage and have developed robust techniques for managing accumulations of insured physical assets, quantifying their concentration risk, and balancing their portfolios to ensure proper diversification against catastrophe losses.

Table 3.1: Total Number of Companies in U.S. by Cyber Accumulation Segmentation

	Premier	Large	Medium	Small	All	% of total
Number of Employees:	>2,000	500-1,999	100-499	20-99		
Revenue:	>$3 B	$40 M-$3 B	$10 M-$40 M	$2 M-$20 M		
Average Annual Revenue:	$14 B	$240 M	$28 M	$11 M		
Business Sector						
Information Technology - Software	11	55	267	1,046	**1,379**	0.2%
Information Technology - Hardware	12	14	61	168	**255**	0.0%
Information Technology - Services	32	395	1,897	7,507	**9,831**	1.6%
Retail	177	2,177	12,645	80,486	**95,485**	16.0%
Financial Services - Banking	44	277	2,201	6,238	**8,760**	1.5%
Financial Services - Insurance	70	254	976	4,061	**5,361**	0.9%
Financial Services - Investment Management	52	205	2,201	2,362	**4,820**	0.8%
Healthcare	47	2,877	15,654	61,702	**80,280**	13.4%
Business & Professional Services	49	4,473	15,757	60,704	**80,983**	13.6%
Energy	58	27	338	1,838	**2,261**	0.4%
Telecommunications	13	43	221	1,013	**1,290**	0.2%
Utilities	89	94	527	2,986	**3,696**	0.6%
Tourism & Hospitality	27	681	6,292	87,155	**94,155**	15.8%
Manufacturing	285	2,119	8,805	40,876	**52,085**	8.7%
Pharmaceuticals	23	34	136	354	**547**	0.1%
Defense / Military Contractor	2	25	27	124	**178**	0.0%
Entertainment & Media	37	407	2,528	15,385	**18,357**	3.1%
Transportation / Aviation / Aerospace	43	896	2,937	13,985	**17,861**	3.0%
Public Authority / NGOs / Non-Profit	0	215	1,558	18,562	**20,335**	3.4%
Real Estate / Property / Construction	28	813	5,592	48,516	**54,949**	9.2%
Education	16	387	2,398	13,372	**16,173**	2.7%
Mining & Primary Industries	4	81	236	759	**1,080**	0.2%
Food & Agriculture	56	283	1,210	5,295	**6,844**	1.1%
Other	0	215	1,558	18,562	**20,335**	3.4%
All	**1,173**	**17,047**	**86,021**	**493,056**	**597,297**	
	0.2%	2.9%	14.4%	82.5%		

In the digital economy, the assets are data, software, content information, skills, communication networks, computing resources, and connections. Insurers who partner with corporate clients to provide insurance protection for these assets have to develop new accumulation management techniques and build up an understanding of diversification and portfolio management that is appropriate to the exposure landscape of the digital economy.

4 Future Cyber Losses and Claims Potential

Accumulation management requires estimating the potential future claims from cyber loss processes. Costs resulting from cyber incidents are themselves not static and are changing over time as new compensation practices, legal landscapes, and regulatory frameworks adapt to cyber threat. Claims experience built up over the past several years may not be a good guide to the future costs of incidents of similar characteristics. Developing a probable maximum loss estimate or a stress test scenario may need to allow for future loss costs per incident that are higher than those of recent times.

First-party costs for a data breach for example may include i) forensic investigation of breach; ii) legal advice; iii) legal consultation costs or ‘breach counsel’ to consult the business regarding statutory requirements; iv) notification costs of communicating breach; v) credit card monitoring for customers.

Third-party costs may include i) legal defence; ii) settlements, damages, judgments; iii) liability including those arising from warranties, breach of contract, product recall and replacement, and indemnification of counter-party losses from their remediation efforts; iv) cost of responding to regulatory enquiries; v) regulatory fines and penalties (including Payment Card Industry fines); vi) cost to settle. In some recent actions, some plaintiffs even seek damages for emotional distress and punitive damages.

Potential lawsuits can be extremely costly to defend and may also require the company to incur other material expenses. The costs of lawsuits and compliance are complicated by a changing regulatory and litigation landscape.

4.1 Changing Regulatory Landscape

The regulatory landscape for cyber risk is changing rapidly, with increasing regulation, penalty payments, duties of notification, and compliance requirements. In the United States 48 states have introduced specific cyber breach regulation, in many cases quite different regulations one to another, sometimes conflicting. Forty-seven states now require prompt notification, sometimes as soon as 15 days, 28 states require reporting to government and the media if the data breach involves more than 500 people, and some states set thresholds for the notice requirement, such as reasonable basis to believe the breach will result in harm. Thirty-six states establish penalties and 11 provide rights of action.[8]

There are also overlapping federal laws. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulates the privacy of personal health data, while the Gramm–Leach–Bliley Act (GLBA) regulates the privacy of financial data, with different requirements and powers of penalty. The Office of Civil Rights resolutions that enforce HIPAA have increased in number over time, from 4,500 in 2004 to 14,000 in 2013, combined with escalating fines, reaching, for example, a fine of $4.8 million imposed on New York and Presbyterian Hospital and Columbia University in May 2014 for failing to secure patient healthcare records of 6,800 individuals (a ‘P3’ event in our data loss severity scale) that accidentally became searchable on the internet from secure servers held on their network.[9]

There are also a number of legislative proposals in progress that are likely to become law in the near future and introduce further changes to response practices and costs for future cyber events, including HR 3696 National Cybersecurity Protection Advancement Act (House Homeland Security Committee); HR 1560 Protecting Cyber Networks Act (House Permanent Select Committee Intelligence); and Cybersecurity Insurance Sharing Act (Senate Select Committee Intelligence).

In the European Union, member states are required to design their own laws within the confines of the EU Directive 95/46/EC. The most serious breaches under this directive attract fines of up to 1 million Euros or 2% of worldwide annual turnover of the company.

The United Kingdom, Australia, Canada, India, Russia, China, and many other nations are also developing their own information security laws and regulations each of which are also likely to result in large fines and penalties.[10]

4.2 Changing Legal and Litigation Landscape

Given the increasing sophistication of cyber attacks and the large settlements attracting significant media attention, there is likely to be an increase in litigation in relation to cyber events around the globe, including class-action lawsuits.

The legal landscape relating to cyber risk is currently disjointed and uncertain. Lawmakers, regulators, and courts across the world are developing rules and new precedents relating to cyber risk on a reactive basis. This has resulted in a patchwork of laws, regulations, case law, settlement trends, and an environment that makes it difficult to estimate future costs that might result from the cyber losses that are likely to occur.

[8] Serfass (2015)

[9] U.S. Department of Health and Human Services (2014)

[10] BakerHostetler (2013)

The outcome of cases is highly variable and depends heavily on the specific language of each insurance policy, the particular state and federal laws in place, and the facts of the claim as well as the court's willingness to find coverage.

The erosion of standard from case law is a concern to lawyers involved in cyber litigation. Historically, data breach suits were dismissed if plaintiffs could not show articulated damages. Recent case law overturned this, allowing a class action to proceed without articulated damages flowing from the breach.[11] This case was settled soon after with monetary awards of $30 per person to individuals whose personal information was stolen but who suffered no articulated damages. The principle was established that it is no longer necessary to demonstrate that the person has suffered damage from a data release, only that their data was released.

There are also changing processes in novel pleading strategies being employed by plaintiffs and the willingness of courts to consider new arguments as well as increasing trends in awarded settlement amounts.

Legal liabilities are part of the insurance coverage for cyber loss in a number of the coverage categories defined in the Cyber Exposure Data Schema, including Breach of Privacy; Regulatory/Defence Coverage; Network Service Failure Liability; Liability (Product and Operations); Liability (Technology Errors & Omissions); Liability (Professional Services Errors & Omissions); Liability (Directors & Officers); Multi-media Liabilities (defamation and disparagement); Intellectual Property Theft; Environmental Damage; Death and Bodily Injury. Claims in relation to many of these insurance liability coverages have significant potential to increase. Due to the uncertain nature of the legal market in relation to cyber incidents, insurance companies are likely to seek to ensure future policies have much more clarity around the exact liability coverage terms and conditions.

A particular area of coverage that is expected to grow in significance in relation to cyber events is liability relating to Directors & Officers, where the duties of senior management to maintain share price and business viability through adequate security protections and contingency planning may become more onerous with cyber events causing damage to the balance sheet and shareholder returns.

Although some of the future changes could cause costs to reduce, managing accumulation risk in an environment of uncertain and changing legislation and litigation means incorporating conservatism into the future loss costs. We recommend that cost forecasts are stressed with conservative estimates of claims costs and liability settlements.

5 Defining Cyber Accumulation Scenarios

Accumulation scenarios assess how much an insurance portfolio might have to pay out in a severe event and help portfolio managers maintain their exposures to be below that risk appetite. Defining a Probable Maximum Loss (PML) for cyber insurance is challenging. The history of claims experience is short, and as the threat is rapidly evolving, even the experience of a few years ago is losing its applicability to the current risk landscape. The systemic nature of cyber risk is apparent, with evidence such as widespread infections of malware in less-secure computer populations, but there has not yet been a truly systemic 'catastrophe' loss – many large claims from their insureds arising from a single cause – experienced by the cyber insurance industry.

Instead the development of accumulation scenarios requires evidence-based assessments of loss potential and an assessment of the realistic constraints to the systemic extent of any loss process. This report proposes a framework and a set of scenarios for use in accumulation risk management.

[11] Resnick v. AvMed, 693 F.3d 1317, 1332 (11th Cir. 2012) cited in Serfass (2015)

Table 5.1: Cyber Loss Processes and Affirmative Standalone Cyber Insurance Coverages

Cyber Loss Process:	Data Exfiltration	Denial-of-Service	Cloud SP Failure	Financial Theft	Cyber Extortion
Accumulation Scenario:	Leakomania	Mass DDoS	Cloud Compromise	Financial Transaction Interference	Extortion Spree
Insurance Coverage Category					
Breach of privacy event	3	1	2	1	1
Data and software loss	3	2	2	1	2
Incident investigation and response costs	1	1	1	1	1
Liabilities	2	2	2	2	1
Financial theft	2		1	3	1
Business interruption	1	3	3	1	2
Cyber extortion	1	2	1	1	3
Intellectual Property (IP) theft	1		1		1
Impact on reputation	2	2	1	2	2

3	Potentially High Impact
2	Potentially Significant Impact
1	Potentially Some Impact
	No Impact Likely

5.1 Cyber Loss Processes

We selected scenarios by considering the different cyber loss processes that have the most potential to impact many of the most common coverage categories being offered in the cyber liability insurance market, as prioritized in Table 2.2, page 12. These loss processes are part of a taxonomy of cyber threats capable of causing disruption to corporate business.

The alignment of cyber loss processes with coverage categories is shown in Table 5.1. The selection ranges across most of the coverages – most processes trigger losses in several categories but some are particularly impactful on specific coverage categories – and there is at least one scenario that impacts each of the most common coverages. These five cyber loss processes are not the only processes that can cause cyber losses, but they cover the primary drivers of loss and provide a framework for generating a variety of accumulation stress tests for a portfolio.

Insurers should consider a variety of accumulation stress tests to avoid over-concentration on a single loss process. Data exfiltration has been the loss process that has been an understandable focus for cyber insurance risk management but several other loss processes have the potential for similar size losses. The insurance exposure is defined by the coverages being offered so for accumulation risk management it is prudent to consider a variety of ways that those coverages could trigger extreme levels of payouts.

Each of these cyber loss processes is a particular technique or mode of attack that occurs today in companies and triggers insurance claims on cyber policies. The detailed study of each of these five processes constitutes the rest of the main content of this report. By understanding these processes and analysing how they occur, developing metrics and studying past case studies, we can extrapolate to a plausible extreme scenario of large numbers of individual claims for use in accumulation management.

A cyber catastrophe loss process is one that will generate large numbers of claims from an underlying cause. This may be analogous to 'Proximate Cause' of specific named perils in other classes of insurance. It would be sensible for insurers to consider the cyber loss processes identified here as primary categories of causes of cyber loss and potentially track the incidence of these by cause codes in their risk management operations.

Within a cyber loss process, it is possible to experience a cyber catastrophe where a large number of claims are correlated because they arise from a common underlying cause. Correlation causes include:

- Vulnerabilities in information technology systems which enable widespread exploitation across many insured companies
- Perpetrators that apply resources or techniques that can scale their attacks across large numbers of target companies
- Failures or breakdowns in systems that are key elements in the business operations of many insureds.

5.2 Distributions of Loss Severity

For each of these loss processes we have defined a loss severity scale for an incident of this process to an individual company. Over a period of time a portfolio of insureds is likely to experience a distribution of severities of these events that lead to claims of different amounts. Typically this consists of relatively larger numbers of small payouts and fewer large payouts. This frequency-severity distribution of incidents of each of these loss processes is the main concern for insurers. In some cases insurers may be concerned about a single very severe claim occurring to a large account, but for accumulation management purposes the primary issue is assessing the frequency-severity distribution of incidents that could occur under extreme circumstances. An insurer may be able to assess from their claims experience what their frequency-severity distribution of incidents of these loss processes is for an average year. However, it is difficult to assess what the frequency-severity distribution might be if there were to be a major systemic cyber event during a particular year. We consider 'catastrophe' events for these cyber loss processes and provide a framework for assessing the frequency-severity distribution of claims patterns that could be generated from a correlated underlying cause of increased cyber activity.

5.3 Identifying a Cyber Catastrophe

The 'event' that drives an increased loss severity distribution in an insurer's portfolio is very unlikely to be a sudden occurrence. A cyber catastrophe is unlikely to be instantly identifiable in real time. It is most likely to become apparent over several weeks or months of accumulating claims occurrence. Cyber insurance claims, from data exfiltration occurrences for example, are happening periodically from a variety of separate and unconnected causes at what we might consider a background or baseline rate of occurrence. In these scenarios we consider how a new or increased phenomenon might inflict an unexpectedly high incidence of severe claims – for example, the occurrence of rare software vulnerabilities that might be used by a particularly well-resourced criminal gang to carry out a large number of data exfiltration attacks, or a group managing to use specialist techniques to perpetrate unprecedented levels of theft from financial transaction systems. When these occur, the insurer may not initially be easily able to distinguish them from the background rate of claims, but as they accumulate it will become apparent that something different in scale has occurred.

Unlike natural catastrophes causing property claims, where the event occurs with high visibility, seismometer evidence, or media weather reports, the cyber catastrophe might only become recognized relatively slowly, from forensic investigation and technical diagnosis. 'Attribution' – proving what happened and who did it – is notoriously difficult in cases of cyber attack. It may be difficult to identify all the claims that have been caused by the same piece of malware, or from the same underlying technique of attack or perpetrator. The correlating cause may take time to identify and it is even possible that the complete story is never fully understood, and insurers may find it difficult to differentiate which of the many claims they are dealing with are attributable to the catastrophe cause, rather than from other background or baseline incidents.

For this reason, we consider that a cyber catastrophe event will drive claims from a baseline of the expected average annual occurrence rate of these types of claims (expressed as a frequency-severity distribution) to a new, increased level of frequency-severity distribution. This is expressed as an annual rate. Cyber insurance policies are written as annual contracts, and insurers manage to an annual business cycle.

5.3.1 Duration of Cyber Catastrophes

The duration of the cyber catastrophe events developed for the various accumulation scenarios are all within the one-year period of the modelling output. The duration of these events is determined by the 'campaigns' being waged by the perpetrators, and by the speed of discovery and actions of the collective security community to combat and prevent further loss, which entails how rapidly software vulnerabilities can be patched and how quickly notifications can be communicated and remedial actions coordinated among the insureds and law enforcement agencies. In most cases a campaign of attacks on a whole community of corporates is likely to become apparent within weeks or months. Our examples explore how long these attacks might persist in each type of cyber loss process. All of our scenarios have durations that are limited by the defensive reactions and mitigation activities of the security community to be well within the 12-month window of an annual cyber insurance contract, and it is defensible for insurers to consider this to be a reasonable stress test occurrence window.

It is not impossible, however, that some cyber catastrophe events be sustained for longer than a year. Malware infestations can take a long period to eradicate, there could be latent vulnerabilities in systems that could be exploited across multiple years, and institutionalized cyber attackers could persist with similar or evolving attack techniques for lengthy durations.

If different time window definitions were to become an important component of cyber catastrophe risk management, it may also be problematic to define the moment of occurrence of the loss for a cyber insurance contract. Malware could be inserted into a company's internal networks for a long period before it is activated. Data could be extracted without knowing the exact date on which the extraction occurred. Cyber event attribution difficulties can include defining when something occurred.

Time window definitions have played an important role in natural catastrophe insurance, for example, the terms and conditions of reinsurance contracts tend to have hours clauses, defining a duration within which a peak claims load can be indemnified. Defining a similar time window structure for cyber catastrophe reinsurance would be problematic for all the reasons discussed here. However, an annual cycle of claims, as proposed here, is a reasonable duration of claims-made limitations that should encompass the main cyber catastrophe events that are of most concern to insurers.

5.4 Assessing a Loss Severity Distribution to Use as a PML

Other catastrophe insurance risks, such as natural catastrophes, share a common characteristic in being fat-tailed. Annual claims experience data is a poor predictor of the extremes, and normal volatility in claims observations cannot be extrapolated to estimate the catastrophe tail risk.

With natural hazards, the structure of the fat-tails is governed by the fractal geometry of nature. The size of a windstorm, flood, earthquake, or tsunami can increase in physical dimensions in a manner typically represented by an inverse-power law . With the peril of cyber we still do not know the scaling laws and physical limits that constrain the tail risk. We cannot yet assess with any confidence the probabilities and how loss events will scale for cyber events.

Typical PMLs in other lines of insurance business have return periods of several hundreds of years, i.e., an annual probability of exceedance of less than one in several hundred. If cyber could be assigned probabilities, then we would probably want to have a cyber PML of a similar probability to other lines. This analogy approach has been used by some to propose ranges for potential cyber PMLs.[12]

[12] Marsh and UK Government (2015) proposes that cyber PMLs could be in the range of 0.15% to 20% of total limit

The nature of a cyber catastrophe ‘event’ is that an underlying cause may significantly increase the frequency-severity distribution (more claims and higher proportions of them being severe claims) of insurance payouts. The examples for our stress tests include malicious agents acquiring new exploits that make it easier to exfiltrate data, increased capacities of denial-of-service attacks being developed by determined attackers, unprecedented technical failures in robust cloud services, new technology capabilities being applied by financial fraudsters, and changes to the criminal business model of cyber extortion.

Each of these events has an underlying cause that results in an increased frequency-severity distribution of that type of claim for the year. Each scenario results in a new frequency-severity distribution of claims that is higher than expected for a non-catastrophe year, and sometimes shifted to have a higher proportion of more-severe claims. Estimating the level of the frequency-severity distribution that could occur from the extreme cause is the principle issue in establishing a PML. As with many other types of catastrophe tail risk, there may be no theoretical limit to the severity of an event, just a diminishingly improbable set of circumstances that would need to occur for the loss to reach increasingly severe levels.

For each accumulation scenario we assess and propose a practical level of extreme but plausible circumstances that would generate a significantly increased frequency-severity distribution of claims. This is informed by a number of considerations.

We develop a model for each of the five cyber loss processes, the potential perpetrators and their tools, their targeting and their capabilities, and the security measures that have to be overcome for the loss process to occur. We consider how an extreme event would occur through changes in the loss process to provide an opportunity to scale the loss, for example through increased resources and capabilities of the perpetrators, new technologies becoming available to them, accidental vulnerabilities arising in key systems, systemic errors being discovered in security protection, and other ways that could be proposed to increase the scale of loss. An important element of this is the technical assessment of the constraints to scaling the loss process, and any limits to how far the process can go. Each event causes a loss ‘footprint’ – the number of companies that are affected and a correlating factor for why those companies are affected by the same loss event. For example, if the loss process can be scaled by having three zero-day vulnerabilities occurring in key systems, then the footprint of the event is defined by the companies that have those key systems in common. By estimating the total number of companies that share these types of key systems, we can set upper bounds on the proportion of all companies that might be affected by this type of loss process involving multiple zero-day vulnerabilities in their key systems, and assess practical levels of penetration to assume for stress tests.

The approach that has been adopted for the proposed accumulation scenarios balances technical assessments of severe but plausible occurrence processes, with statistical extrapolation of historical background rates and precedent, benchmarks of PML levels from other perils, and best estimates of acceptable stress levels from insurance specialists.

Ultimately, companies will need to satisfy themselves that they are setting a risk appetite on the basis of well-defined and detailed research into the process, combined with their own loss experiences and judgements about the severity and incidence rates they believe are credible.

5.5 Accumulation Scenarios

The next sections of the report describe accumulation scenarios for five key processes of cyber loss. These are plausible but severe examples of how correlated losses could impact a portfolio of cyber insurance policies and explore how a large number of accounts might suffer losses from a single underlying cause. In each case, we propose a scenario from a technical assessment of feasible ‘vector’ paths that would lead to systemic losses, combined with analysis of limitations as to the extent and severity of the potential impact.

These are not predictions or expectations of how the cyber threat landscape will change. These scenarios are highly unlikely to occur – we propose that they are treated as severe but plausible. They are proposed as stress tests for accumulation management purposes – i.e. how many policies in a cyber insurance portfolio could make a claim and for how much, under these conditions.

6 Cyber Data Exfiltration

Systemic release of confidential customer records from many corporate enterprises

Accumulation Stress Test Scenario: **Leakomania**

Three rare ‘zero-day’ vulnerabilities provide a criminal gang with the capability to scale data exfiltration attacks across thousands of companies. Billions of confidential data records are leaked in a few months, more than the total number of confidential data records leaked in the past ten years.

The highest profile cyber incidents have been data breaches: the loss of confidential data from companies that breach the privacy of their customers, employees, clients, or counterparts. This has been costly to the enterprise, resulting in notification costs, credit monitoring services, and compensation pay outs to all the individuals whose data was compromised, together with regulatory fines, response and forensic costs, and sometimes substantial litigation costs.

The losses faced by individual companies have been instrumental in driving the expansion of the cyber insurance market, as companies seek protection and risk partners in helping with response services. Breach of privacy coverage is the most common element of cyber insurance, with more than 90% of stand alone cyber insurance products offering this, and 80% offering data loss coverage.

The economics of cyber insurance could be severely impacted by a sudden change in the pattern of data breaches, or most critically, in the frequency of occurrence. The accumulation scenario provides a stress test of an extreme but plausible increase in the incident rate of large severity exfiltration events.

6.1 Types of Data

There are many different types of data that might be stolen. These are categorized as:

- Personal Identity Information (PII): credentials such as full name, contact details (address, e-mail telephone), date of birth, social security number, passport number, and driver’s license details. They may also include password credentials to access online accounts for services.
- Payment Card and Credit Card Information (PCI): in addition to personal credentials, financial information such as credit card number, pin, bank account number, and access credentials.
- Protected Health Information (PHI): in addition to personal credentials, medical information such as healthcare records, tests and procedures, insurance plan details, biometric identifiers, medical device identifiers and serial numbers,.
- Commercially Confidential Information (CCI): commercially sensitive information, proprietary business information, trade secrets, and confidential information about counterparties.
- Intellectual Property (IP): copyright, patents, industrial design rights, blueprints, trademarks.

The severity of a data exfiltration event is broadly in proportion to the number of data records lost. Table 6.1 provides a severity scale for a data breach event, defined by the power of ten of the number of personal records, for considering the relative severity of incidents above key thresholds and their frequency.

6.2 Exfiltration Event Catalogue

Records of exfiltration events – incidents of organisations’ confidential data being lost, stolen, or disclosed – have numbered in their thousands over the past decade (see Figure 6.1). Many of these events are go unreported, particularly incidents of small numbers of data records, however modern corporate governance means that the loss of a large data set from any major organisation is publicized and becomes public knowledge. In the United States and increasingly in other jurisdictions there are regulations that now require companies to report data losses of this type. We can have confidence that public records of recent incidents of large data exfiltration events are relatively complete.

Table 6.1: Data Breach Loss Severity Scale

Data Breach Severity	Range (min. to max. number of data records)	Representative Value (Observed average number of Records in that magnitude range)
P3	1,000 to 10,000	4,100
P4	10,000 to 100,000	37,000
P5	100,000 to 1 million	310,000
P6	1 million to 10 million	2,800,000
P7	10 million to 100 million	31,000,000
P8	100 million to 1 billion	115,000,000

Over the past decade there have been many thousands of data exfiltration events in the United States alone, amounting to at least 900 million confidential records lost. Over the past five years, on average there have been at least 60 incidents a year of data breach severity of P4 and above, and at least 18 that were P5 and above. The number of P4 and above events has declined significantly over time as preventative measures have reduced the incidence – the average annual incidence rate was 87 in the five years before 2010 and has fallen below 60 in the five years since.

Data breach is international, with data exfiltration events being reported in at least 61 countries in 2014.[13]

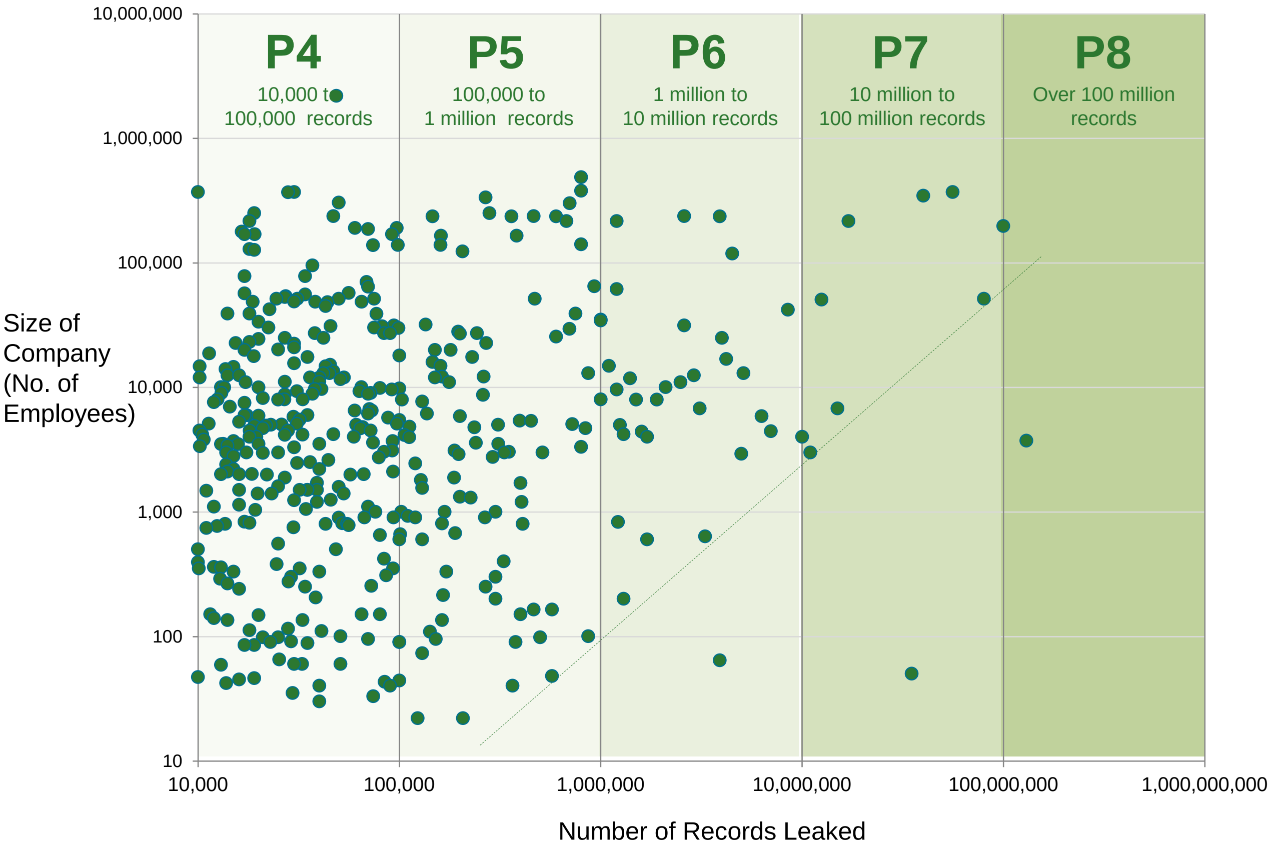


Figure 6.1: Data Breaches Events by Number of Records Leaked and Company Size

[13] Verizon (2015)

6.3 Causes of Data Loss

Figure 6.2 shows the causes of data exfiltration in a representative sample of incidents where the cause is known. Over the past decade the primary cause of lost data has been accidental – typically a portable device containing data files being lost. This has diminished over the past five years as laptop encryption and other preventative measures have reduced accidental loss. There is a trend for an increasing proportion of breaches to be caused by external malicious exfiltration: criminals hacking in to organisations to steal personal data for sale or to use in further criminal exploitation.

Table 6.2: Selected Large Data Loss Events

Breached Company	Number of Records	Year	Data Breach Severity
Heartland Payment Systems	130,000,000	2009	P8
TJ Stores (TJX)	100,000,000	2007	P8
Anthem	80,000,000	2015	P7
U.S. Military Veterans	76,000,000	2009	P7
The Home Depot	56,000,000	2014	P7
Target Corp.	40,000,000	2013	P7
U.S. Department of Veterans Affairs	26,500,000	2006	P7
Office of Personnel Management (OPM)	21,500,000	2015	P7
Bank of New York Mellon	12,500,000	2008	P7
Sony, Playstation Network (PSN)	12,000,000	2011	P7
Fidelity National Information Service	8,500,000	2007	P6
Global Payments Inc.	7,000,000	2012	P6

6.4 Hackonomics

The growing trend of external criminal acts, which is driving the number and severity of data exfiltration cyber attacks, is due to the rewards for the effort of stealing data with a low chance of being caught or suffering retaliation. Conviction rates for cyber criminals are much lower than for many other criminals.

Unlike physical assets, digital assets are not a finite resource – they can be stolen more than once and resold many times. The theft of data is not a zero-sum game. However, the driving reward for the criminals is the monetization of the stolen data. As increasingly large volumes of data have been stolen and offered for sale on the black market, the price that can be obtained for some of the most common types of data has diminished, obeying the economics of supply and demand. Email access credentials for example now command only very low prices as a result of the black market being flooded with these types of data.

6.5 Systemic Causes of Surges in Data Exfiltration Incidents

There is little correlation between one breach event and another in the pattern of observed incidents, other than a general failure of security to prevent it. In some cases the theft of details in one event enables another breach event elsewhere (for example, where people re-use the same password for multiple websites). Some criminal gangs are suspected of being responsible for multiple incidents of data loss. The data breach processes are not inherently systemic.

For insurance accumulation management, cyber writers need to consider how severe their losses could be from data exfiltration events – i.e., how a major surge could occur in cyber data exfiltration events that could be surprisingly higher than expected from previous experience and what systemic correlation could drive it. The accumulation scenario represents a severe but plausible level of high incidence of large severity data breaches and describes the correlation structure for company losses.

Leakomania Scenario Narrative

Phase 1: Preparation

A loose affiliation of hackers located in several U.S. cities forms a gang to reinvest some of the gains from their previous operations to mount a more structured and coordinated campaign of data theft. During their planning they discover that there are three quite different zero-day vulnerabilities for sale on grey markets on the dark web. These have been discovered by unscrupulous hackers who have carried out fuzzing tests on various systems and each is offering to sell the technique they have discovered for around $25,000 in bitcoin.

The gang quickly realise that these three rare vulnerabilities in combination could provide a method to extract confidential data from secure networks across many companies. They realise that they have a finite time window before these vulnerabilities are publicized and fixed by their target victims.

Phase 2: Target Selection

The hackers scan corporations to find configurations of these software systems that match their zero-day assets. They methodically sweep the internet to identify the attack surface of target companies. Companies are pinged to detect the firewall system that they run on external facing servers and the rulesets that have been set in those firewalls. They can detect that around 15% of corporate servers are running '*Fortress Drawbridge*' firewall software v4.3.

The second vulnerability they have obtained is for *Sybil* databases. It is impossible to identify which companies run *Sybil* databases on their internal networks – these are hidden from view. Although they have identified many thousands of companies that run *Fortress Drawbridge*, the hackers' next step is a manual process, so they have to be selective in which companies they invest their time in reconnoitring. They choose large companies with the promise of large dataset rewards. They also prioritise companies with the likelihood of holding confidential healthcare records that are more valuable to sell on the black market.

Phase 3: Data Exfiltration

The hackers code up a Remote Access Trojan (RAT) to insert into each target company to reconnoitre its internal network. It is vital that this software is not detected by corporate anti-malware protection and security systems. An online black market company in China tests their software against all known profiles of malware signatures, to check that the software profile will not be detected by standard anti-malware detectors.

The gang inserts a copy of their RAT though the vulnerability in the firewall at their many target companies. The RAT operates a 'network sniffer' that resides in the company for several weeks, monitoring the network traffic of the organisation, constructing a diagnostic of which types of databases are in use and what data might be stored where, and detecting the brand of corporate webinar system in use. It communicates this diagnostic information back to the criminal gang via a disguised messaging protocol and a complex routing of the message via a number of other countries and to avoid it identifying the recipient.

Only a small proportion of the companies that are penetrated with the RAT keep their data in Sybil databases and also operate *1-to-Many* corporate webinar services. The hackers select these companies to target and ignore all others. Once they have identified a target dataset, they activate their second vulnerability, enabling them to assume administrator rights on the Sybil database, unlock the encryption on the data records, and export the entire dataset in small manageable chunks.

Their third vulnerability enables them to take control of the software that manages the *1-to-Many* corporate webinar services. They use steganography techniques to disguise the data to look like *1-to-Many* video data that is streamed out from the company on the internet so that to the security monitors on the corporate network, this appears to be normal traffic. A 100 GB file containing 100 million records is streamed out of the organisation in chunks at the equivalent file size of two downloaded films.

The hackers then start to sell the data on the black market data exchanges.

Phase 4: Discovery

An incident response team in one of the compromised companies finds the RAT malware on their network. They remove it, profile the software and publish the Indicators of Compromise from the malware as an advisory notice on security websites. Another company's security team also finds the RAT and publishes a second incident. As more are detected, the United States Computer Emergency Readiness Team publishes an Advanced Persistent Threat (APT) notification. Agents of NSA report that unusually large volumes of data are being offered for sale on the black market. The internal investigation teams find the evidence of their Sybil database compromise and realise that they have suffered a serious data breach. They call in an external incident response and diagnostics team, and they report the incident to their Chief Executive Officer.

The company goes public the next day with an announcement that 100 million personal customer data records are suspected to have been stolen, and begins the lengthy process of notification to all of the individuals who may have been affected, providing them with credit-watch services, and offering compensation. The company is notified of a class action being brought on behalf of all their compromised customers.

A second company makes a similar announcement about 60 million confidential healthcare records two days later. The following day a third company announces a 120 million record breach. Security companies quickly identify that these events all involved a Sybil database and other IT components in common. The diagnostics teams put together a profile of the 'Tools, Tactics and Procedures' (TTP) of the attack. They identify all the vulnerabilities that the gang has exploited. The attack methodology is published leading the software vendors of Fortress, Sybil, and 1-to-Many to contact their corporate users and recommend taking these systems out of operation until they can be patched. Many thousands of companies now scan their internal systems rigorously for signs of RAT malware and for compromises on their databases and firewalls.

A large number of companies realise that they too have fallen victim to an attack of the gang. Over a hundred household-name companies publicly declare their data breach in a single week. Many more follow, in the days and weeks afterwards, as more companies confirm that they have had major datasets stolen.

The general public are shocked. Government officials and politicians decry the data crime wave. The NSA, State Department and the Department of Homeland Security mount a highly publicized security operation to catch the perpetrators, involving house raids on suspects and international operations to close down servers suspected of being used in the operations in various Eastern European and Southeast Asian countries.

Phase 5: Aftermath

Billions of data records have been exfiltrated from businesses during this six month crime campaign – a multiple of the total volume of all records lost over the past ten years. The attempts to sell these on the black market have been self-defeating: the price of confidential data records has plummeted.

Companies rush to improve their protection against future data breaches of this type. Many institute security hardening approaches and change internal operating procedures. New laws are passed to require companies to achieve higher security safety standards to protect the public. The US president declares a new approach to law enforcement with a greatly increased budget to create a cyber police force and 'law enforcement for the 21st century.'

In the short term, the incidence of data breaches from other criminals drops significantly: security standards have made it harder to hack a company and the reduced price of data on the black market has reduced the rewards. Cyber criminals switch their efforts away from data theft to focus on different methods of making money from cyber crime.

The police operations to track the gang are moderately successful. Several young men in different cities are arrested. The ringleader is never caught.

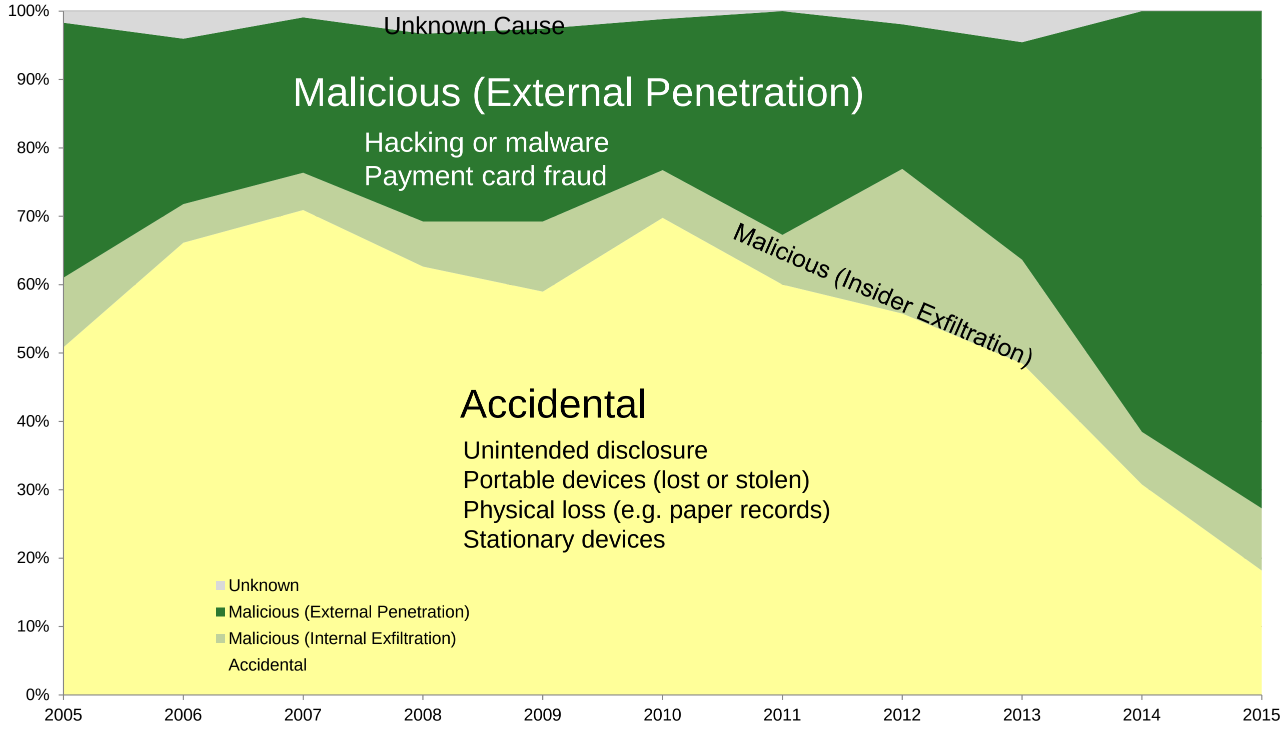


Figure 6.2: Causes of Data Exfiltration – Trends over Time

Table 6.3: Black Market Prices of Stolen Digital Assets (US$)

Digital Asset	2012	2015
Healthcare Record	$5	$15
Bank Account Access Credentials	$3	10
US Credit Card Number	$1	$0.5
Credit History	$0.24	$0.39
PayPal Account Access Credentials	$0.15	$0.25
eBay Account Access Credentials	$0.12	$0.2
Social Security Number	$0.5	$0.1
Email Access Credentials	$0.002	$0.0002
Name, Address, Email Address, Phone No.	$0.001	$0
	Percentage of face value	
CryptoCurrencies (BitCoin etc.)	30%	35%
Loyalty Program Rewards (Airmiles, Supermarket points)	20%	25%
Physical Goods for Sale	10%	12%
Pre-paid Call Minutes	8%	8%

Claims surges from cyber breach events could occur from:

a) Random variation in uncoordinated causes of incidence (sudden increase in accidental losses combined with other unrelated coincidence of attacks and insider exfiltration)

b) A sudden increase in malicious insider exfiltration: a trend where many more people become whistleblowers or data thieves

c) A coordinated campaign of malicious external attacks by criminal gangs

It is clearly insufficient to manage loss limits around the assumption that extrapolation of observed volatility in the short catalogue that exists of cyber breaches is representative of potential extremes. The unreliability of statistical extrapolation of sparse data is the rationale for all catastrophe risk modelling.

It is also less plausible to construct a systemic rationale for a correlate d surge in the actions of a lot of different individuals employed in separate companies to risk prosecution by exfiltrating data.

For the stress test, we propose that the most plausible systemic cause of a surge of increased incidence of large severity data breach events is a coordinated campaign of external malicious attacks. The Leakomania scenario explores the correlation structure and severity limits of a coordinated malicious external attack campaign on corporate targets.

6.6 Vectors for Data Exfiltration

Figure 6.3 illustrates the conceptual process of malicious external exfiltration of data as penetration, access, and exfiltration, showing various options of techniques that can be used to achieve each stage.

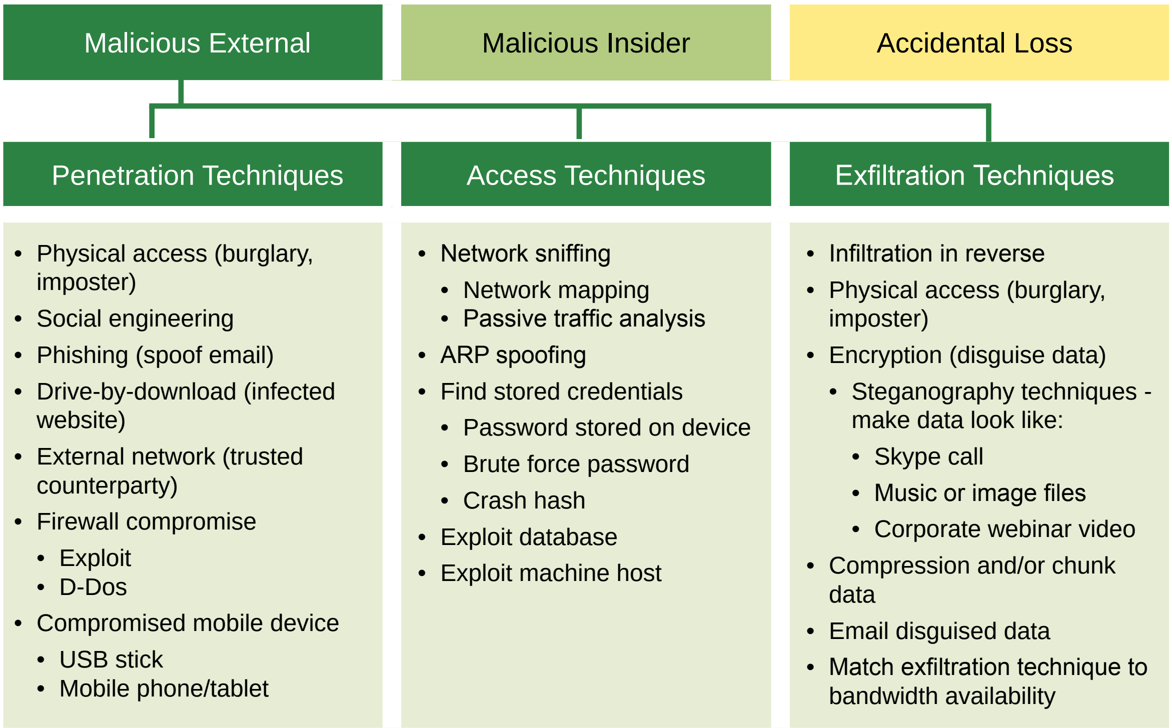

Malicious External
Malicious Insider
Accidental Loss
Penetration Techniques
Access Techniques
Exfiltration Techniques
• Physical access (burglary, imposter)
• Social engineering
• Phishing (spoof email)
• Drive-by-download (infected website)
• External network (trusted counterparty)
• Firewall compromise
• Exploit
• D-Dos
• Compromised mobile device
• USB stick
• Mobile phone/tablet
• Network sniffing
• Network mapping
• Passive traffic analysis
• ARP spoofing
• Find stored credentials
• Password stored on device
• Brute force password
• Crash hash
• Exploit database
• Exploit machine host
• Infiltration in reverse
• Physical access (burglary, imposter)
• Encryption (disguise data)
• Steganography techniques - make data look like:
• Skype call
• Music or image files
• Corporate webinar video
• Compression and/or chunk data
• Email disguised data
• Match exfiltration technique to bandwidth availability

Figure 6.3: Process Vector for Data Exfiltration, Particularly Malicious External Exfiltration

For the scenario to be ‘systemic’ the techniques used have to be easily scalable and replicable from one target victim to the next. If a malicious external actor has to find a customized approach for each different company, this is a significant constraint on scaling the attack.

The most scalable attacks are those that exploit a common vulnerability in systems in use by multiple companies: a Systemically Important Technology Exploit (SITE).[14] For a data exfiltration attack, we consider SITEs that would enable each of the three stages of data exfiltration. In this example we focus on the potential for separate exploits in a firewall system, a key database, and a corporate webinar system. We use fictional systems in the scenario, but theu are representative of real systems in common use. The exploits are imaginary but they are based on real precedents.

[14] This term was first introduced as a way of understanding potential correlated loss in cyber attacks in the example of compromised software algorithms in the Sybil Logic Bomb cyber scenario.

For the stress test scenario we postulate that a criminal gang embarks on a coordinated and well-planned 'campaign' to maximise its gains from data thefts on large corporate businesses. The gang purchases three key zero-day exploits (i.e. technology flaws that are unknown to most of the users and security professionals) from the black market, one for each of the phases of the operation required – penetration, access, and exfiltration. Completely unknown zero-day exploits are rare, so the likelihood of a criminal gang obtaining three unknown zero-day exploits makes this scenario an extreme, but plausible, event.

The criminal gang concentrates its resources on larger companies but, in general, they scan the corporate landscape looking for companies that have these vulnerabilities.

- **Penetration**: The zero-day vulnerability used for penetration is a hidden account and backdoor in version 4.3 of *Fortress Drawbridge* a particular brand of firewall that is one of the industry standard applications in the configuration of corporate servers that interface to the outside world.
- **Access**: The zero-day vulnerability used for gaining access to the stored confidential data on the internal network is a previously unknown flaw in the security protocol of release 7.0 of *Sybil*, a well-known brand of database in common use for customer and human resource management.
- **Exfiltration**: The zero-day vulnerability used for exfiltrating the data is a stenographic technique to disguise the data flows as corporate webinar communications using *1-to-Many*, a popular online meeting software service, so that the internal security software that is monitoring the company's network traffic cannot detect anything unusual.

Only companies that run all three of these systems – use a *Fortress Drawbridge* firewall v4.3, keep their confidential data in a *Sybil* v7.0 database, and commonly run *1-to-Many* webinar software – can be successfully targeted. These examples are fictional but real systems have occasional zero-day vulnerabilities that are unexpected flaws in even the most security-conscious companies.

The gang has finite personnel and a limited time window before their exploit assets become known and their potential targets quickly respond and patch their systems, so they concentrate on finding the maximum number of targets that they can exploit as quickly and as easily as possible. They target large databases in big companies, but are opportunistic and take smaller datasets where they can, from medium sized companies and those with lower levels of security.

The gang operates successfully for about six months until their activities start to be discovered, and their campaign is effectively ended by the FBI publishing their Indicators of Compromise. They compromise a large number of companies before that time, most of which are unaware until the techniques used become known and discoverable once the FBI publication is available.

7 Denial-of-Service Attack

Attacks to disable websites and disrupt online business activity across multiple companies

Accumulation Stress Test Scenario: **Mass DDoS**

Hacktivists build the largest distributed denial-of-service capability yet seen and target it at capitalist corporate websites to disrupt e-commerce. They generate DDoS traffic at many multiples of the most extreme peak rates seen on the internet, which is concentrated on insured businesses.

Two-thirds of all cyber affirmative standalone insurance products in the market provide coverage for business interruption that could occur to corporate insureds from external disruption to web-based services and e-commerce.

Half of all major U.S. companies experienced a denial-of-service attack on their websites in the past year, and one in eight of those attacks overwhelmed their resilience and rendered their internet services unavailable. Denial-of-Service (DoS) attacks are a common method of disrupting website business activities by bombarding them with traffic. These types of attacks coordinated from a network of computers are Distributed Denial-of-Service (DDoS) attacks. There are different types of DDoS attacks (see Section 7.5 below), but the most common is ‘volumetric attacks,’ which flood a website with traffic. These attacks are unsophisticated and relatively easy to carry out by attackers. They do not need to penetrate the company’s defences; they simply have to generate large volumes of traffic to the company’s site. Traffic volumes can be generated by ‘bot-nets’ – a network of remotely controlled zombie computers, which are personal computers infected by malicious software that then sends out messages without the owner even noticing. Traffic can be increased through ‘reflectors’ – other computers that add traffic to a target site – and through ‘amplifiers’ – computers that will respond with more information as a response to a single stimulus.

7.1 Volumetric DDoS Attack Intensity and Website Vulnerability

The intensity of volumetric DDoS traffic is measured in gigabits per second (Gbps). An attack of 10 Gbps (‘Significant Intensity’) is likely to overwhelm the capability of a website with the infrastructure to support around 1 million visitors a month and cause it to become unavailable. A website with more infrastructure and capacity is less vulnerable, and it takes more attack intensity – higher Gbps volumes – to take it down.

An intensity scale for DDoS attacks is defined in Table 7.1, together with the approximate thresholds of website vulnerability as a guide. Websites are ranked by their traffic, so the worldwide ranking of a website is also a rough guide to its capacity and vulnerability threshold for DDoS attacks. The actual ability of a website to withstand a DDoS attack also depends on the response of the operator team, the countermeasure they take, and the redundancy and alternative service capability they might deploy.

Table 7.1: DDoS Intensity Scale and Vulnerability Thresholds

Intensity Scale for DDoS attack:	Significant Intensity DoS	Moderately High Intensity DoS	High Intensity DoS	Very High Intensity DoS
Volume (gigabits per second):	1-10 Gbps	10-50 Gbps	50-100 Gbps	100+ Gbps
Website Vulnerability Threshold (number of visitors per month)	1 million	10 million	100 million	1 Billion
Approximate global website ranking for vulnerability threshold	Top 100,000	Top 10,000	Top 1,000	Top 100
Daily attack rate (worldwide in 2014)	962	101	3.53	0.40

Although attack rates over 600 Gbps have been recorded, it should be noted that maximum attack intensities are constantly being exceeded. There were over 500 DDoS attacks with an intensity of 100 Gbps or more (‘Very High Intensity’) estimated to have occurred somewhere in the world in 2014. Analysis suggests that worldwide there were as many as 1.6 million DoS attacks in 2014, the most recent year for which a full year’s worth of data is available.

7.2 Duration of DDoS Attacks

The duration over which a volumetric DDoS attack can be sustained varies significantly. Most attacks are of short duration: half of recorded attacks last for less than two hours and 70% last less than six hours. But some attacks persist. Sixteen percent of DDoS attacks recorded in 2014 lasted longer than 12 hours, which is significant because the most common deductible period for business interruption being offered by cyber insurance products in the market is 12 hours. We estimate that there may have been over 1,500 DDoS attacks worldwide in 2014 that were either 'High Intensity' or 'Very High Intensity' and also lasted longer than 12 hours.

7.3 Magnitude of DDoS Activity Worldwide

The total volume of DDoS activity can be measured in 'Gbps-hours': the number of attacks combined with their total intensity metric of gigabits per second (Gbps) and the duration of attacks in hours. This provides an estimate of the magnitude of DDoS activity. In 2014 we estimate that DDoS activity averaged over eight million Gbps-hours of attack each month.

The number of annual DDoS attacks fluctuates significantly but analysis of recent trends suggests that the overall number of attacks may not be increasing substantially. However, attacks are getting more intense, with a greater proportion of attacks being of higher intensity, and sustained for longer durations.

7.4 Perpetrators and Motivation

Very few DDoS attacks are successfully attributed or the attackers identified, caught or prosecuted so it is not always possible to identify the motivation of DDoS attacks. A proportion of DDoS attacks are motivated by direct financial gain, with some extortion demands being made to the victim by criminal gangs. However the large majority of attacks are destructive with only indirect or no monetary benefit to the perpetrator. Some DDoS attacks mask other criminal activities, such as a simultaneous breach of a network to steal data. Some may even be accidental or collateral damage from attacks on imprecise targets. There may be commercial competitive dimensions to disabling other organisations' servers. However, most attacks are deliberate attempts to disable the functionality of web systems as acts of sabotage and vandalism.

Major players include state-sponsored actors. DDoS attack capability is seen as a potential weapon for use by nation states in influencing foreign policy, deterring malicious cyber activities from external agents, or as a method of augmenting military actions in a conflict. A number of countries are known to have military or state-sponsored units with powerful DDoS capability such as the Chinese 'Great Cannon' (see case study) and the US National Security Agency QUANTUM internet attack tool. These are predominantly defence and counter-hacking tools but could be used against commercial businesses in extreme circumstances.

A large proportion of DDoS attacks are on government, local or administrative authority sites, or military and operational service sites. A significant number of DDoS attacks are on customer support functions, such as problem reporting, complaints and bug-fixes. Many DDoS attacks appear to be acts of protest. Some are coordinated protests by so-called hacktivists around ideological issues such as human and animal rights, anti-capitalism, climate change, and ecology. An example is the case study presented below on Operation Global Blackout. The financial services industry is a major target for DDoS attacks and a significant proportion of all attacks is directed against targets in the sector.

The most likely perpetrators of systemic DDoS attacks on commercial businesses that carry cyber insurance are well-organized special interest groups that can orchestrate campaigns of DDoS attacks. DDoS attacks are relatively easy to carry out, and the capacity for generating volumetric attacks is already fairly commoditised. There are black market websites offering bot-net capacity for rent. The cost of renting bot-nets to mount a 'High Intensity' DDoS attack of 50-100 Gbps on a commercial website for 24 hours is around $200,000.

7.5 Types of DDoS Attack

The broad types of denial-of-service attacks are:

a) **Volumetric attacks** flood a target network with data packets that completely saturate the available network bandwidth. These attacks cause very high volumes of traffic congestion, overloading the targeted network or server and causing extensive service disruption for legitimate users trying to gain access.

b) **Application-based attacks**, also known as 'layer 7' attacks, target the application layer of the operating system (Open Systems Interconnection model). The attack does not use brute force but is a disguised instruction that forces functions or particular features of a website into overload to disable them. It is sometimes used to distract IT personnel from other potential security breaches. Application-based attacks are reported to constitute around 20% of DDoS attacks.

c) **Protocol-based (TCP Connection) attacks** involve sending numerous requests for data (SYN packets) to the victim server – typically a firewall server – which opens a new session for each SYN packet, overwhelming the control tables of the server. These TCP SYN floods are one of the oldest types of DDoS attack, but are still used for successful attacks.

d) **Fragmentation attacks** use internet protocols for data re-aggregation as an attack vector to overload the processing power of a server. The fragmentation protocol manages the transmission of volumes of data by breaking it down into smaller packets and then reassembling them at their destination. Sending confusing or conflicting protocols floods the server with incomplete data fragments.

Our scenario uses the most common type of DDoS: the volumetric distributed denial-of-service attack.

7.6 Defending Against a DDoS Attack

During a DDoS attack a number of things occur:

- Users experience much slower page load times in their browsers
- Transactions fail
- Services are unavailable

Defending against a determined DDoS attacker is time consuming. Defenders have to analyse the traffic samples to determine the patterns of traffic that they need to disrupt. They then try to block, thwart, or redirect the unwanted traffic. It may be difficult to distinguish DDoS traffic from legitimate user traffic. A clever attacker will confuse the two. It may be possible to react to common attacks within 15 minutes, but some defences can take up to three hours to deploy. The best mitigations have contingency plans in place with upstream providers in readiness, to avoid impacting customers.

7.7 Case Studies of DDoS Attacks

The past 20 years of applied technical research has not produced a complete solution to defending against Denial-of-Service attacks. Attacks continue to occur. Year-on-year variations in the rates can be significant. Recent analysis has seen a number of trends and key statistics:

- Frequency increased 132% in 2014 over the previous year
- Average cost (without extortion) is reported to be
  - $52,000 per incident for small to medium businesses
  - $440,000 per incident for larger businesses
- Average duration of DDoS was 21 hours in Q2 2015, a reduction of three hours from the previous quarter

Case Study: Chinese 'Great Cannon' DDoS Attack on GitHub, 2015

In March 2015, websites that were critical of the Chinese government and being used to circumvent Chinese censorship were targeted by one of the most intense Distributed Denial-of-Service attacks yet recorded. GitHub, a service for the development of IT projects run by GreatFire.org, and the New York Times' Chinese mirror website were rendered inoperable by unprecedented volumes of DDoS traffic, estimated to exceed many hundreds of Gbps at times. The attack persisted in keeping the sites offline for 118 hours (nearly five days). The attack was coordinated from an offensive system, dubbed the 'Great Cannon,' possibly related to the Great Firewall of China operated by the Chinese government, which hijacked and targeted traffic from the servers of the Chinese search engine Baidu, as well as manipulating the traffic of "bystander" systems outside China. The 'Great Cannon' system represented an escalation in DDoS capability and showed the potential to 'weaponise' internet traffic. It has been accused of being a demonstration of capability to target any foreign computer system that offends the Chinese regime.

Case Study: 'Operation Global Blackout'

In 2012 members of the Anonymous hacktivist movement publicized a warning that on March 31st they would launch a distributed denial-of-service attack on the internet's root DNS servers in support of the anti-capitalist protest 'Occupy' movement that at the time was organizing rallies and displays of social disobedience. They threatened to shut down the Internet "where it hurts the most" to punish global e-commerce of multi-national business. Though no attack eventually occured, analysts suggested that the plan details were entirely plausible but would have caused only limited and partial outages of the internet. Anonymous threatened to flood the world's 13 domain name root server IP addresses with traffic generated by a specially designed Reflective Amplification tool (Ramp). Had this occurred it would have broken the address system of parts of the internet – the websites would all still be operational, but typing their usual URL into a browser would fail to find them. The threat prompted engineers and web security specialists to strengthen the domain name system against future attacks of this type.

7.8 Severity Scale for Companies Experiencing DDoS

When a company's website or servers are hit by an overwhelming DDoS attack, their site becomes unavailable. The duration of the unavailability is the primary driver of loss. Table 7.2 provides a categorization of durations of possible unavailability of the website. Severity IO 12+ is typically where insurance companies start to see loss, because most cyber insurance products that cover BI from DDoS attacks have a 12 hour retention or deductible. However the scale includes durations below this to assess the insureds' ground up loss and may be of interest to insurers in assessing the potential for changing retention levels in the design of future insurance products.

7.8.1 Revenue Dependency on Internet Connectivity

The cost of the business interruption caused by a DDoS attack of any particular duration for a company is determined by the internet dependency of the insured company – i.e. the amount of revenue that would be lost per hour of internet failure or connectivity loss.

In the Cyber Exposure Data Schema we propose that insureds being offered BI cover specify their BI potential from Internet failure as an explicit value per hour, which can be factored from annual revenues from e-commerce operations or other contributions to a company's revenue being carried out online. The capture of this information makes it possible to assess accumulation of exposure across the portfolio of all the insured accounts from the potential for internet outage in general, and from systemic incidence of denial-of-service attacks in particular.

Table 7.2: Severity Scale for Internet Outage from DDoS Attacks

Severity Definition: Duration of Internet Outage Experienced by Customer as a Result of Distributed Denial-of-Service Attack

	Internet Outage Severity	Range (in hours)	Representative Value (Average outage hours)
IO 1+	**1-6 hours**	1 to 6	2
IO 6+	**6-12 hours**	6 to 12	8
IO 12+	**12 hours to 1 day**	12 to 24	16
IO 24+	**1-3 days**	24 to 72	36
IO 72+	**3-7 days**	72 to 168	90
IO 168+	**7 days to a month**	168 to 720	240

Table 7.1 presents an approximate relationship between the capacity of a company's website and its vulnerability to the intensity levels of volumetric distributed denial-of-service attacks. Recording the capacity of an insured's website, in terms of the number of visitors per month for example, provides a first-order assessment of the resilience of that website against different intensities of attack. Website traffic statistics are published by a number of third-party providers if the information is not directly provided by the insured.

Mass DDoS Scenario Narrative

Phase 1: Preparation

Grass roots protests by an organisation calling itself the Movement for Economic Justice (MEJ) gathers momentum with organized protest marches and a social media campaign against what it terms the excesses of globalisation and 'turbo-capitalism.' MEJ claims the Internet to be a common humanitarian resource and calls for coordinated action to 'take back the web' from giant corporations that are dominating the web with e-commerce activity. They publish a manifesto calling for hacktivists everywhere to coordinate a summer campaign of distributed denial-of-service attacks on major corporations that they accuse of appropriating the internet. They publish 'DIY DDoS' - online manuals on how to create distributed denial-of-service attacks, and provide links to dark web market sites where DDoS capabilities can be rented or bought.

MEJ has created a large bot-net for use in their campaign by distributing malware hidden in email messages and in web pages that infects domestic personal computers with substandard anti-virus security. They run periodic activation tests across the internet to estimate how effective their malware is at infecting domestic machines. One of the key metrics for the effectiveness of their bot-net is how many of their infected computers are permanently connected to broadband and high capacity lines, capable of generating high volumes of traffic when commanded to do so. They use mailing lists of customers subscribed to online streaming services to boost their numbers of high capacity broadband victims and create a special version of the malware that infects Internet-connected televisions. Their bot-net increases in capability when they add a Chinese version of their malware that achieves good penetration among the 174 million broadband subscribers in China – more than twice the number in the United States.

The objective of MEJ is to create a controllable volume of junk traffic that can be directed to selected targets capable of overwhelming some of the largest commercial e-commerce websites in United States and Europe. To boost the volume of traffic that they can direct they also set up a hierarchy of controllable reflector and amplifier computers – servers that will respond to a data packet that it receives with multiple data packets sent back out. They term the DDoS engine that they have built, their 'Anti-Capitalist Fire Hose'. They program a series of targets into the software that will trigger and aim the attacks.

Phase 2: DDoS Campaign

MEJ publishes a final set of demands denouncing global 'e-mperialism' and warns that unless the Internet is returned to the people, it will take matters into its own hands and bring down websites of trade.

The first DDoS attacks hit the online banking services of some medium-sized banks. Their websites that operate over 10 million transactions a month are overwhelmed with junk traffic bombarding their servers at a rate of more than 50 gigabits per second. Users trying to log into their online bank accounts find that the service is continuously unavailable. The banks' IT teams attempt to block and divert the junk traffic but every response move is countered by the intensity of the attack. The attack continues to keep them offline for several days. News of the attacks hits the headlines and MEJ claims responsibility. Other hackers join in with their own DDoS attacks against other corporate websites.

The MEJ begins to ramp up its attacks and it draws additional capacity from its extended bot-net around the world. They extend their targeting to major retailers, focussing on the e-commerce websites of a range of online stores. These websites are more resilient: several of them have high-volume sites and are in the top 1000 of the world's busiest online stores. They experience attacks of over 100 Gbps and are overwhelmed. Some of the retailers are well prepared and have arrangements with their upstream service providers, switching to a range of alternative IP addresses to dodge the attacks. But the attackers are monitoring their responses and the Fire Hose switches its attack to these new domains. One site after another suffers an attack and becomes unavailable to customers. The attacks spread to many thousands of corporate websites and online services.

The attackers maintain a volume of traffic directed against as many sites as they can manage. They extend the attack to well-known brand names in entertainment and media, telecoms, software companies, professional services companies, and yet others more. The attack capacity fluctuates as computers are switched off and on by their users, unaware that their machines are being used in the attack, and as processing power, connection bandwidth, and internet traffic varies. The volume of traffic generated by the Fire Hose attack and other MEJ supporters is itself a limitation to the capacity of the attack with some parts of the Internet and localized access routes clogging with traffic and limiting the intensity of attacks that can be delivered. The attackers' control software tries to balance these fluctuations and optimise the attacks for the capacity available at any one time. Some attacks are cut short and others started so that companies experience varying attack intensities and intermittent periods of functionality. Although MEJ scales its attacks using amplifier and reflector devices, it has a finite attack capacity. It is trying to attack a large number of targets, and the intensity required to take any major commercial web service offline is considerable. Their attack capacity is spread more thinly as they attempt to widen the scope to more companies. The attack is sporadic, varying against different sites at different times, and continues over several months. Defenders are increasingly able to divert attack traffic and keep their websites operational.

Phase 3: End Game

The public reaction to the continuing MEJ attacks becomes increasingly hostile. Trends in social media show strong protest against disruption to favourite web services. Regional Computer Emergency Response Teams in each country share resources and join with their national intelligence services and many corporate IT response teams to identify the sources and combat the attacks. Attack sources are eventually tracked back through their complex and obscure routing sources and identified as thousands of servers in many different countries, many of them outside international jurisdiction agreements. The defenders begin to fight back, using their own DoS techniques on the attackers, disabling the attack servers that they can find. The attack servers are dynamic and change configuration and routing when countered, but gradually the defenders disable an increasing number of servers and cause attrition on the attack capacity.

The U.S. government also fights back with a coordinated international campaign with many other national governments to deny the attackers their source fire power by asking domestic users to disconnect their computers from the internet and purge any potential malware using an anti-virus program. The attack capacity of the MEJ is gradually eroded, and attacks become weaker and less frequent towards the end of the summer. Politicians appeal to the MEJ to end their campaign and offer conciliatory gestures towards making internet access more egalitarian. The MEJ declares that it has achieved many of its aims and publishes a final bulletin announcing that it is ceasing its attacks.

Phase 4: Aftermath

The summer has seen extreme disruption to a large number of online commercial operations. Many millions of service hours have been lost during the attacks across thousands of websites around the world. Many customers have lost faith in the reliability of internet services and revert to previous practices. The numbers of online customers drop dramatically across many websites and it takes many months before traffic gradually restores to previous levels. E-commerce operations see significant reductions in revenues. Corporate servers are beefed up to make them more resilient to future attacks of this type, with massive redundancy and multiple distributed server operations. The technical media refers to the redesign of corporate online services as "the new arms race". There is an international initiative to form a rapid response force to coordinate responses between countries against future attacks. Proactive law enforcement agencies crack down on the online black market for hacking services, with some high profile arrests and prosecutions.

The blow to e-commerce has been significant but it is not terminal. The faith of the general public is gradually restored, but they demand increased security for their internet activities. In future histories of the internet, the summer that the MEJ tried to 'take back the web' will be seen as a landmark in defining new safety levels for the digital economy.

8 Cloud Service Provider Failure

A large number of companies have business operations disrupted by losing cloud-based functionality when a major cloud service provider company suffers a disruption

Accumulation Stress Test Scenario: **Cloud Compromise**

A technical error leads to an outage at a leading cloud service provider, causing its customers to lose service for many hours until they are gradually reconnected. The outage is on a scale never experienced by a commercial CSP, in terms of proportion of their customers affected and reconnection times.

The digital economy is increasingly dependent on cloud services. A rapidly growing number of companies make use of a Cloud Service Provider (CSP) by outsourcing elements of their data storage, analytics, and information technology functions.

If a CSP were to fail then their customers would suffer business losses. In our survey of standalone cyber insurance products in the market, 69% of our sample included coverage for business interruption that would be triggered by the failure of a cloud provider counterpart. A CSP failure could also be the source of the exfiltration of confidential data records, resulting in the type of claims payouts explored in the Leakomania scenario, or claims for data and software loss if data files were irrevocably deleted. This provides an accumulation issue for cyber insurance where there is potential for a large number of companies to make a claim for business interruption if a major provider of cloud services were to have a lengthy outage or failure, from any cause.

CSPs are themselves purchasers of cyber insurance and, if an insured CSP has a severe outage, could make a sizeable claim under that policy. The systemic dimension of the risk concerns the triggering of large numbers of claims from companies that are CSP customers. The customers and their insurers may attempt to recover their loss payouts from the CSP (and possibly their insurer) but this recovery of loss cannot be assumed. In this scenario, we evaluate losses without recovery from the CSP.

The accumulation stress test scenario explores the issue of a lengthy suspension in the service provided by a cloud service company with a large market share, and how this results in insurance claims from multiple policyholders in a cyber insurance portfolio.

8.1 Cloud Services and Providers

Cloud services can be broadly categorized into four application areas:

- **Software as a Service (SaaS)** is the largest sector of the cloud market, accounting for nearly half of cloud-related business volume. In SaaS, companies such as Salesforce, Cisco Webex, and Intuit run their business as cloud applications.
- **Platform as a Service accounts (PaaS)** account for nearly a quarter of all cloud-related business, and provides companies with development environments for CSP customers to develop, run, and manage their web applications, with the CSP providing networks, servers, storage and other services to host the customer's application.
- **Infrastructure as a Service (IaaS)** constitutes less than 20% of cloud business, and provides virtual computing power and resources, such as virtual computing resources, servers, data partitioning, scaling, security, backup and other services.
- **Enterprise Private Cloud (EPS)**, accounts for around 10% of the cloud market. Enterprise private clouds and virtual private clouds are cloud computing platforms that are implemented within the corporate firewall, under the control of the organization's IT department.

There are over 100 companies that currently provide third-party cloud infrastructure services, with the dominant 'big four' players of Amazon AWS, Microsoft, IBM, and Google collectively accounting for more than half of the market. The largest market share is taken by Amazon Web Services, which in 2016 has around 30% of the market for CSP services.

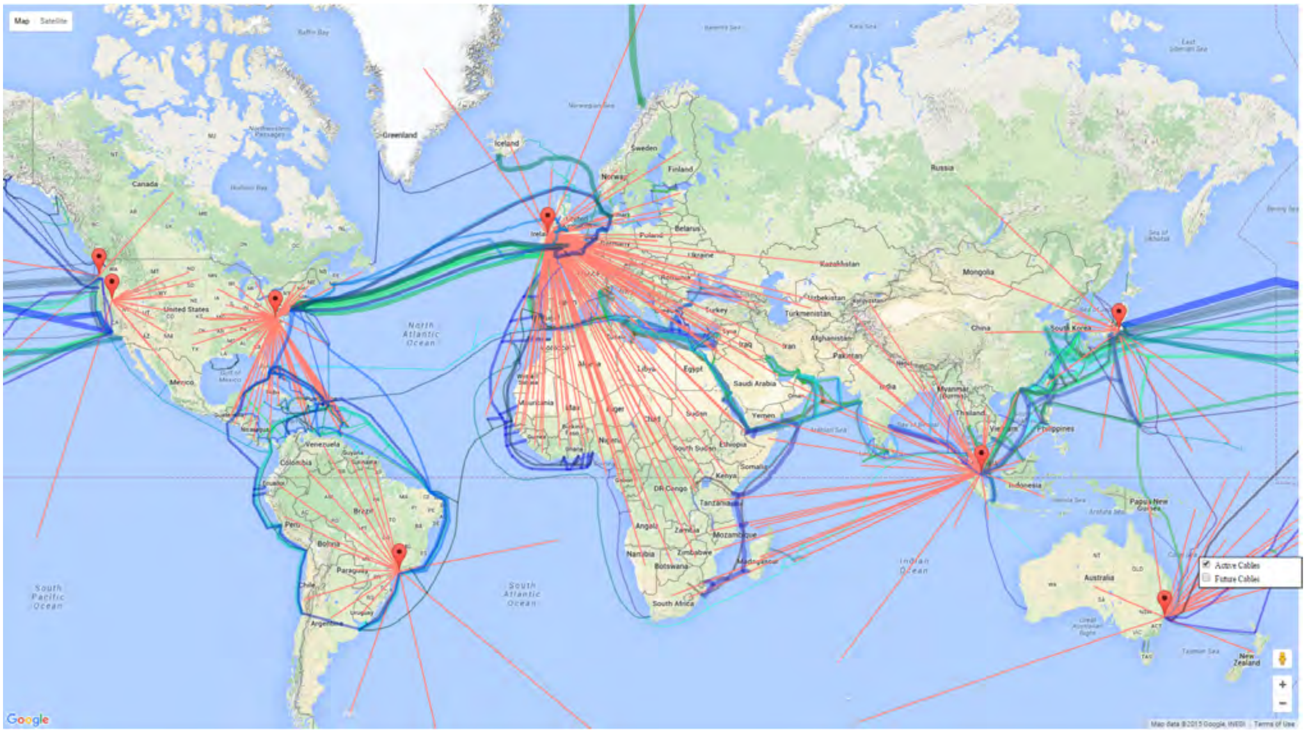


Figure 8.1: Mapping of the Infrastructure of Amazon Web Services

8.2 Diversification across CSPs

Good practice for accumulation management is to know which of your policy-holders is reliant on each of these CSPs, how dependent they are, and to ensure that your portfolio is not too concentrated with any one of the CSPs. The Cyber Exposure Data Schema proposes that insurers explicitly capture the dependency of revenue that an insured policyholder has on their named CSPs. Many of the larger companies use more than one CSP – we recommend that insurers capture the revenue dependency on the insured's top three named CSPs. This enables accumulation monitoring of exposure by CSP and the total limits exposed across all of the insurer's accounts to each of the leading CSPs can be used as an indicator of potential concentration risk, and, if necessary, to manage the diversification of exposure across them.

8.3 The Customers of Amazon

Amazon Web Services – the market leader in cloud service provision – has an estimated 30,000 corporate customers around the world. Other CSPs have different profiles of customers and a different mix of business sectors, but the principles are common to any of the 100 CSPs whose disruption could impact large numbers of customers.

Amazon is configured to provide services to its customers in various regions of the world, It structures its operations around 30 geographical 'Availability Zones', served by 11 regions, with their primary hubs and several hundreds of individual data centres. For example AWS serves the United States with five regions and 13 Availability Zones. The Amazon networks are configured for high reliability and redundant capacity, and each data centre has each redundant power supply, networking and connectivity, housed in separate facilities.

Premium customers can pay to be connected to multiple data centres to give added resilience in case one of the data centres is disrupted. Around 20% of AWS customers have the dual-server service. It is also the case that some companies use more than one CSP, as an added precaution against experiencing disruption from any particular CSP suffering a problem. For insurers, knowing whether insureds rely on a single data centre for their cloud provision is an important differentiation in risk selection.

8.4 Past Outages of CSPs

Because their customers are so dependent on them CSPs pride themselves on their reliability and high level of service continuity. The CSPs are rated by external third parties on their reliability by monitoring their downtime. The big four CSPs, for example, typically achieve over 99.9% reliability of service.

Significant outages however do occur. Examples of past outages include:

- Apr 2011; Amazon Web Services – misrouting sent cluster of elastic block stores into remirroring storm, taking down much of AWS US east region for **eight hours**
- 2009 Microsoft Sidekick suffered a **week-long** service outage, leaving users without MS services (email, calendars, personal data) and losing their cloud-stored backup data
- 2010 Gmail outage; 150,000 Google Cloud Gmail users had empty emails for up to **four days** while Google attempted to restore services, eventually resorting to using physical tape backups
- Microsoft Hotmail suffered a similar outage, also in 2010, when testing scripts deleted 17,000 email accounts, taking **three to six days** to restore from backups
- 2011 Intuit cloud service platform, providing SaaS for TurboTax; Quicken; QuickBooks and other applications went offline for **36 hours**, following power failure that triggered routing problems
- 2015 outages with Amazon and AWS

The large majority of these examples are temporary disruptions of service, typically application failures. In some cases there are permanent losses of data that have resulted from deleted or lost files that backup services were unable to restore, or were only able to restore older vintage versions of the data. The high reliability of CSPs means that although there are a few rare examples of failures of their systems, such as those shown above, there is insufficient observational data to assess the likelihood of a catastrophic failure of these systems through statistical means. Instead, we explore a hypothetical scenario to assess the number of customers of a generic CSP that would be likely to have interruptions and for what periods of time before they are reconnected.

8.5 Footprint of a Cloud Outage Event

Examples of CSP disruption show that each outage has a ‘footprint’ – a subset of the customer base that is affected – and a restoration process, in which service is progressively restored to the affected customers. The typical footprint of an outage is limited by the structure of the network and the number of customers that are reliant on any one component of the system. By distributing the service provision to the customer base across multiple regions and data centres, the amount of the customer base that can be impacted by an accident, failure or cyber attack at any individual site is limited. This scenario explores how a systemic problem could impact a sizeable proportion of the US customer base of a typical leading CSP. The footprint scale that might be possible, in increasing order of severity of impact, and unlikeliness, include:

- Individual application failures for users of a particular product or software service
- General service failure for all customers of a particular localized data centre
- General service failure for all customers of a particular regional hub
- General service failure for all customers of multiple regional hubs
- Complete service failure for all customers of all international hubs

8.6 Severity Scale for Duration of Cloud Outage on Their Customers

Some customers are restored quickly while others must wait longer to be reconnected. The type of technical issue that has caused the outage determines the speed and process of restoration, and there are some examples where all of the affected customers are restored at the same time – all suffer the same duration of disruption – but this is rare.

More typically there is a restoration distribution for customers with a reduction over time of the number of customers in a geographical region. This is typically seen in the restoration of utility services when they suffer a disruption. Utilities are measured by the proportion of their consumers in a given region who are restored to service within a given period of time. The time to restore at least half of the impacted customers ($T_{50\%}$) is a typical metric for response to an outage. Big customers are prioritized in the restoration process but sometimes it is difficult to know which customer can be recovered from which repair. These recovery processes therefore require the repair of the entire interconnected system, and restoring service to everyone as soon as their parts of the service become operational.

Table 8.3: Loss Severity Scale for Coud Outages

Severity definition: Duration of Outage of Cloud Service Provision Experienced by Customer

Cloud Outage Severity		Range (in hours)	Representative value (average outage in hours)
CO 1+	1-6 hours	1 to 6	2
CO 6+	6-12 hours	6 to 12	8
CO 12+	1-2 days	12 to 24	16
CO 24+	2-3 days	24 to 72	36
CO 72+	3-7 days	72 to 168	90
CO 168+	7 days to 1 month	168 to 720	240

Table 8.3 shows a severity scale in terms of the duration of outage that might be suffered by a customer of a CSP. In any major disruption event to a CSP, we can expect a certain proportion of customers to experience an outage of some of these severities. The 'restoration curve' of the event defines the proportion of customers that would experience an outage of different durations.

A typical cyber insurance policy that covers business interruption from cloud service provision has a deductible or insured's retention period before claims recovery, with 12 hours being a typical deductible. The proportion of a CSP's customer base experiencing an outage of CO 12+ is a key metric for the insurance loss of a cloud service outage event.

8.7 Ways That Cloud Service Can Be Disrupted

There are a number of ways that cloud service providers could suffer an outage that affects their customers. These include:

- Mechanical failure of equipment, fires, or physical damage of server sites
- Power failure or other essential utility provision, including failure of the backup generators or cooling systems
- Cyber attack by malicious external actors seeking to disrupt services or steal data
- Internal software system failure by accident or from a malicious insider

CSPs have designed their operations to anticipate these threats to their business, and have strong security, redundancy in their design and protection measures and contingency plans in place in order to minimise their potential for disruption from any of these causes. Nevertheless, system failure is possible. For an accumulation stress test scenario we consider the possibility that accidental software failures cause a market-leading cloud service provider to suffer a multi-regional outage with complex technical issues that hinder the recovery process and results in a significant proportion of its customer base suffering lengthy outages.

Cloud Compromise Narrative

Zambezi is a fictional cloud service provider with a market share equivalent to one of the big four CSPs. Zambezi operates multiple regions and many data centres around the world, with five regional hubs to serve its customers in the United States. It has other hubs in many other parts of the world to serve its international client base.

Phase 1: Accidental Release

Zambezi employs a strong team of technical security specialists who develop tools and detection systems for potential malware and devise contingency plans and response protocols for a wide range of technical issues. One of their leading specialist teams is investigating potential vulnerabilities in their Routing Information Protocols (RIP), the controlling system for connecting customers to the servers in the data centres. They have a testing lab that is disconnected from the main network, but is periodically reconnected to enable live tests of new security systems to be performed. Following one of these routine reconnections, problems start occurring with routers in the regional hub that controls the active data centres. A few initial failures and loss of computing capacity means that the operators open reserve channels to draw capacity from other regional hubs.

The security team suspects that some of the test malware created by the research team has somehow found its way into the operational networks of the data centre. The primary suspect is a binary worm that has been written by a researcher for a conference paper to be presented in a few months' time. The binary worm makes copies of itself if it is not controlled by another software twin. The worm changes the Routing Information Protocols in the routers within the regional hub and its satellite data centres. The address book to the regional hub is effectively being erased, component by component. There are around 2000 routers in the regional hub; some are core routers to direct the primary traffic flows, others are edge routers that connect to customers.

The worm is virulent – it is rapidly self-replicating – and destructive. When it reconfigures the RIP of a router, the router cannot be repaired through remote reprogramming. It requires a manual process of skilled operators to find the router in the racks of the server farms and spend several hours reprogramming the firmware to enable the router to be brought back online and to resume its function. The only saving grace is that the research team have not put effort into disguising the worm – it can be discovered and deleted. But the worm has infected the system extensively and the deletion of instances of the worm leads to reinfection from unfound copies.

Phase 2: General Service Failure

When the worm attacks a router the addresses controlled by that router are lost. The machines, networks and data are unaffected and continue to run, but their users can no longer access them. Each affected customer finds that their connection to their cloud service provided by Zambezi no longer operates. Within an hour, over 5,000 companies find that their cloud service has failed. Around a thousand more of Zambezi's premium rate companies have switched their operations from the affected regional centre to their alternate deployment on one of the other four Zambezi centres.

The crisis response team at Zambezi is managing two operations: the internal response to contain and restore functionality to the regional centre, and the external response to inform and provide information to their customers about the status of the disruption.

Phase 3: Proliferation

The Routing Information Protocol operated by Zambezi allows for a limited load-balancing and software transmission between their different regional hubs. These interactions are routinely security screened to prevent malware transmission between centres. However, the emergency protocols for load balancing and transfer of capacity from one hub to another can allow reduced screening on high volumes of data traffic. It becomes rapidly apparent that the early-stage attempts to compensate for the loss of router capacity in the affected regional centre has allowed the binary worm to spread to two other regional centres.

As capacity begins to be lost from these three infected hubs, Zambezi operational control personnel rapidly isolate all of their other regional hubs and prevent any interaction between them to avoid infection spreading to more centres and potentially affecting their worldwide operations of many regional hubs in other countries.

The three infected hubs suffer a complete general system failure for all of their connected customers within an hour of the onset of the incident. Around 17,500 companies lose cloud service, including 1,500 premium rate customers that were unfortunate to have their alternate deployment centre be one of the other infected sites.

Phase 4: Restoration of Service

Many thousands of routers are infected and inoperable. Each requires over an hour of manual attention to reconfigure and recommission to return to functionality. The crisis management team deploys the initial on-site teams of 20 technical specialists in each centre to reconfigure the affected routers, and sends out a call for additional repair specialists from Zambezi's other regional centres. Crisis management also sends out for external consultants. The technicians repair core routers and edge routers in tandem to enable some of their customers to regain service. It is not easy to know which routers control the routing to specific clients, so it is difficult to prioritize the most important customers. Half of the disconnected customers are reconnected within six hours.

The security team carries out a process in parallel with the router repair to eradicate the infecting worm from the systems. This takes time and has to combat the worm technique of replicating itself when it finds uninfected systems. The restoration process has to combat many instances of repeat infections that cause additional failures in routers that have already been repaired. The process of repairing routers picks up pace when additional technical teams arrive, but the teams continue to have set-backs in partial failures recurring in many different parts of the network.

Many of Zambezi's corporate clients remain without their cloud service after 12 hours. They are still unsure when their service will be resumed. They file claims under their cyber insurance policies for business interruption that lasts longer than their retention of 12 hours. Many call Zambezi's competitors and investigate the possibility of using their cloud service to get a version of their cloud functionality back up and running. Several companies instigate reputation management contingency plans to communicate with their own customers and counterparties who are affected by their operational failure.

Phase 5: Aftermath

The large majority of Zambezi's affected customers have their cloud service restored within 24 hours, but a small proportion is unable to be reconnected for several days and for a few, even longer. Some suffer intermittent failures for quite a while. The process of eradication of the worm and the repair of all of the affected systems takes several weeks.

The whole cloud industry is severely impacted in the aftermath of the event, with all of the major CSPs suffering loss of customers as companies experiment with alternatives to third party cloud service providers. Zambezi particularly is badly impacted, losing customers and facing lengthy legal proceedings and law suits that take several years to settle. However, the economics and utility of cloud service to companies ensures that demand for cloud service provision returns to previous and greater levels after some time. The Zambezi Cloud Failure is taken as an object lesson, and the next generation of cloud service provision is architected to make the system more resilient and reliable than ever, with new levels of security and preventative measures in place.

9 Financial Transaction Cyber Compromise

Theft of large sums in cyber attacks on multiple enterprises that carry out financial transactions

Accumulation Stress Test Scenario: **Financial Transation Interference**

A coordinated cyber heist operation on many financial services companies to syphon funds from transactions, obtain cash from ATMs, and carry out insider trading using stolen information. It is carried out on a scale that is orders of magnitude larger than any known cyber theft to date.

Insurers offer coverage to the financial services sector to cover losses that they might suffer from cyber attacks or computer based fraud, theft or disruption occurring from compromising payment systems or technologies for managing financial transactions. Criminals have always targeted the money held in financial institutions, and physical bank robbery has given way to cyber crime as the preferred technique.

For accumulation risk management, we need to assess the number and severity of claims that could occur from cyber theft activities. Although very large numbers of companies of all different types carry out financial transactions, ranging from retail to e-commerce, the transaction systems that carry the financial flows are the specific liabilities of financial transaction companies. Purchase of goods and services is differentiated from the transfer and reconciliation of payments. The potential for widespread and systemic claims across all the different sectors of the economy from subverting payments after the point of sale are constrained by the legal liabilities being confined to the financial services companies operating the payment transfers. A customer who is defrauded by a cyber criminal after the retailer's transaction is a loss that is borne by the financial service company, not the retailer. This limits the extent of the accumulation risk from financial transaction cyber compromises. Far from being a threat across all possible business sectors that carry out transactions, it is instead a liability that is concentrated in the financial services sector operating the payment and transfer systems. Financial transaction risk is concentrated in banking and payment management companies, investment management, and dealing systems.

Types of financial cyber crime fall into the following categories:

- Penetrating bank networks to get access to accounts and to syphon out money (the 'cyber-heist')
- Stock market manipulation – cyber criminals get access to confidential and privileged information that will affect stock market prices, such as upcoming mergers and acquisitions, and pre-publication company results. This insider trader data is known as material, non-public information (MNPI)
- Deployment of malware to:
    - Gain access to customer accounts
    - Gain access to payment processors
    - Exploit securities and market trading services
    - Bring down a financial institution, business interruption

This cyber cause of loss model assesses the technical possibilities for a successful compromise of one or more commonly used financial transaction systems and, as a result, the extent and duration of financial losses that will flow to the insurer.

9.1 Payment Systems

There are different types of payments within the economy. Payments from end customers are usually referred to as retail payments. Wholesale payments take place between financial institutions and tend to be high-value transactions. Commercial payments are generated by companies and in some cases of particularly large international companies; payments tend to resemble the wholesale payments.

9.1.1 Examples of Payment Systems

There are many organisations and systems that deal with international and domestic payment transfers. Some examples include:

SWIFT (Society for Worldwide Interbank Financial Telecommunication), is operated by its banking and financial institution members and has three major functions:

1) To provide messaging services and interface software;

2) To add to the higher automation of financial transactions;

3) To offer financial institutions to resolve common issues such as standardisation by providing a forum. It operates an average of 23 million messages per day and an average Value Of Trade (VOT) of $400,000 with a median VOT of $5,000 per transaction.

FEDWIRE (Federal Reserve Wire Network) is operated by the Federal Banks in the US. Its major function is to enable financial transfers electronically between different economic agents. Its average value of trade is around £3 million with a median VOT of $30,000.

Target2 (Trans-European Automated Real-time Gross settlement Express Transfer system) is a system owned and regulated by the Eurosystem. It accommodates payments in relation to monetary policy operations, interbank and customer payments and other financial infrastructure administration of euro currency. It is one of the biggest payment systems in the world with an average transaction value of €5.5 million in 2014. The average VOT is estimated to be $1.25 million with a median VOT of $20,000.

Payments systems have evolved rapidly over the years substituting traditional payment methods such as cash and cheques to payments by card. Card payments increased by 17.8 billion from 2009 to 2012 whilst traditional payment methods declined by 3.1 billion in the US. Most credit or debit cards are processed through systems such as Visa, MasterCard, American Express, and Discover. Visa is by far the largest retail system, with more than 1 billion VISA payment cards worldwide, accounting for $2 trillion in transactions a year for 23 million merchants and ATMs and 21,000 financial institutions. In the United States, Visa processes around 5,000 transactions per second (tps), with burst capacity of 24,000 tps.

9.2 Robust Security Measures

Because they are so commonly targeted, financial transaction companies employ some of the highest security and protection measures. Following attacks in 2011, Visa and Mastercard significantly strengthened their security, with MasterCard announcing a $20 million security spend and Visa expanding its Visa Token Service a unifying payment platform with high security standards. Assessments publicise the robust design of Visa's data centre with reports that it 'can withstand earthquakes and hurricane-force winds of up to 170 mph. A 1.5-million-gallon storage tank cools the system. Diesel generators on-site have enough power, in the event of an outage, to keep the centre running for nine days.'[15] Visa has partnered with security company FireEye to launch Visa Threat Intelligence to deliver rapid status update information on emerging cyber threats.

9.3 Precedents of Cyber Thefts and Cyber Frauds

Cyber crime occurs in many different ways, several of them are outlined as different cyber loss processes in this report. Estimates of the annual cost to the global economy of cyber crime range as high as $445 billion. Identifying the costs and incidence of financial transaction crime from cyber are particularly difficult, not least because there is no regulatory requirement for a financial services company to publicly declare a theft from its system, unlike the regulatory requirements for data loss. There are however several examples of large financial transaction thefts that are public. Two of them, Drinkman and Kalinin 2013, and Carbanak

[15] USA Today, "Top secret Visa data center banks on security, even has a moat", 25 March, 2012

APT, are profiled as case studies in this section. Other examples of cyber attacks and thefts from financial services institutions include:

- The 2009 compromise of the US payment processor system responsible for 100 million transactions a month for 250,000 US businesses. Cyber threats have been made to the US Automated Clearing House (ACH) and credit card transaction systems, financial clearing houses, transaction processing systems, private electronic payments network and currency exchanges, point-of-sale systems and ATM systems.
- In 2011 Visa, Mastercard, and Paypal suffered Denial-of-Service attacks on their systems that resulted in service disruptions and reportedly reduced their capacity to 1,000 tps in apparent retaliation for these companies blocking payment to Wikileaks (‘Operation Payback’).
- Cyber attacks have been recorded against a number of other companies namely PostFinance, Heartland Payment Systems (2008), Forcht Bank, and the Swedish prosecutors office.
- In 2014 the Brazilian payment system was attacked by “Bolware” with cyber-criminals infecting about 200,000 computers in Brazil and stealing about $3.75 billion.

9.4 Developing a Financial Transaction Cyber Scenario

Table 9.1 specifies a Financial Transaction Loss Severity Scale, as a banded order of magnitude of losses that an individual bank or financial services institution could suffer as a result of a cyber compromise. This is the value of the amount stolen, not the total cost to the institution, which is likely to be significantly higher with additional costs including incident response, litigation, and business interruption costs.

The accumulation scenario stresses the frequency and severity of claims in an insurance portfolio of insureds in the financial services sector. We propose a scenario where many individual banks and investment management companies are compromised through the cyber criminal campaign of a determined and knowledgeable criminal group.

Table 9.1: Financial Transaction Loss Severity Scale

Financial Transation Loss Severity	Range (min. to max. loss, US$)	Representative Value ($)
FT1	$1 M to $10 M	$5 M
FT2	$10 M to $100 M	$50 M
FT3	$100 M to $1,000 M	$500 M

Case Study: APT and the Great Bank Robbery, 2013-2015

Carbanak, sometimes also known as Anukak, was a sophisticated advanced persistent threat (APT) attack against financial institutions in a number of countries, including Russia, United States, Germany, China, and Ukraine, that may have lasted for at least a year, from around 2013, and may still persist. The attack compromised over 100 financial institutions, with loss estimates as high as $1 billion.

Cyber criminals exploited vulnerabilities in Microsoft Office via spear phishing e-mails (targeted fraudulent emails) to gain access to money processing services, ATMs, financial accounts, and the SWIFT network, giving the cyber criminals a means to move and transfer money. They were also able to get ATMs to dispense money at a specific time for mules to collect.

Initial infections used spear phishing that appeared to be legitimate bank communications, with Microsoft Word 97-2003 (.doc) and Control Panel Applet (.CPL) files attached. When the vulnerability was exploited, the shellcode decrypted and provided the attacker with the Carbanak backdoor, which is designed for espionage, data exfiltration and to provide access to infected computers. When successful, the attackers would carry out a manual reconnaissance of the network, typically installing software called Ammyy Remote Administration Tool or alternatively compromising SSH servers. The attackers then extracted money through ATMs and financial accounts. In some situations, the attackers used the SWIFT (Society for Worldwide Interbank Financial Telecommunication) to transfer the money into their accounts. In other cases, Oracle databases were used to open bank accounts or transfer money.

These attacks caused significant losses to the companies that were compromised: one bank reported a loss of $7.3 million as a result of ATM fraud, while another reported a loss of $10 million because of the exploitation of its online banking platform. Exact details of losses have not been made public by the victims, and estimates of the total loss vary significantly. The majority of victims are based in Russia, US, Germany, China and Ukraine, however attacks involving the Carbanak attack process, possibly being perpetrated by the same gang, have been reported in other regions including the Baltic, Central Europe, the Middle East, Asia and Africa.

Case Study: Drinkman and Kalinin, 2013

One of the largest cyber-crime cases came to light in the United States in 2013. A gang of five were charged with breaking into numerous U.S. financial networks and syphoning off more than 160 million credit card details and more than $300 million from Visa payments of JC Penny, JetBlue Airways, and French retailer Carrefour.

Each of the five gang members specialised in different tasks. Russians Vladimir Drinkman and Alexandr Kalinin hacked into networks, whilst Roman Kotov mined them for data. They allegedly hid their activities using anonymous web-hosting services provided by Ukranian Mikhail Rytikov.

They initially gained entry by using a ‘SQL injection attack.’ Structured Query Language (SQL) is a programming language designed to manage data that is stored in particular databases. The attackers identified vulnerabilities in SQL databases and used those vulnerabilities to get malware into the systems to create a “back door”, allowing them access to the full network.

In addition to stealing private information from companies, they also admitted selling it to so-called ‘dump resellers,’ who then sold it to online forums or individuals. They charged $10 for US cards, $15 for Canadian cards, and $50 for European cards with added chip-and-pin security protection.

Financial Transation Interference Scenario

Phase 1: Preparation

A group of skilful hackers comes together to form the ‘Dangerous Hats’ group. Collectively they have a wide range of sophisticated skills to perform state-of-the-art techniques in the hacking world with contacts worldwide. They decide to target banks and financial trading institutions in the United States, UK, France, Germany, Norway and Italy. Their aim is to steal $10 billion.

Their campaign uses four initial techniques to install the malware they need to gain access to the companies that they are targeting:

1. **Spear Phishing**: campaigns of emails to many individuals in banks and other major financial institutions, disguised as legitimate communications but with malware hidden in the innocuous-looking attachments.
2. **Malvertising**: Widespread presence on the internet allows them to create their own malware and inject it into legitimate online advertising. Individuals that follow the advert to visit the website download the malware.
3. **Phone Phishing**, **or Vishing**: uses a rogue Interactive Voice Response (IVR) system to reproduce a legitimate sounding copy of a bank or other financial institution’s IVR system. The attackers monitor their progress by listening in to the conversations of targeted bank employees and security personnel by compromising their personal cell phones with fitted chips.
4. **WiFi interception**: the gang targets public and free WiFi networks used by bank employees, including the coffee shops in the financial services centres of key cities where they work. The gang compromises the WiFi networks to glean personal information from employees who access encrypted websites. Although the websites are encrypted, the WiFi communications to the websites are not, and key information is harvested.

Phase 2: Robbery

The Dangerous Hats gang targets a large number of banks and financial institutions, concentrating on multi-million dollar thefts from each target. Databases are infiltrated to open bank accounts and transfer money using stolen identities.

The gang also carries out ‘ATM jackpotting.’ For this, the computer software controlling the banks’ ATMs is hacked and instructions are inserted to dispense cash from certain ATMs at certain times. The gang arranges to have their friends in place at each machine at the appointed time to collect the money.

A special group in the gang works on using the confidential information that it accesses to carry out insider trading by making investment profits on information about stock price and pre-publication financial results on companies. By accessing investment management companies, they can see trading orders and, in some cases, as able to pre-empt the order and make margins on the trading transaction.

International transaction arbitrage forms an additional line of theft. Pricing differentials and small-margin transactions for amounts that initially escape investigation are redirected to recipient accounts and then rapidly redirected through a complex network.

Phase 3: Discovery

The banks and financial institutions accumulate large losses as a result of these various cyber security breaches. They compensate their customers and suffer financial losses as a result, but do not publicize the fact that they have had an IT security compromise. The IT security groups from the various financial institutions affected share their information with each other on a confidential basis and the scale of the criminal campaign starts to become apparent.

One of the breaches also involves the data exfiltration of 100,000 consumer credit reports from a bank, which is then forced to reveal the security breach under regulatory rules. The bank is fined and its stock price drops as rumours circulate about other breaches of security in their financial transaction systems.

Share price manipulation is suspected leading to the launch of an official investigation when the acquisition announcement of a major insurance company is preceded by unexpected volatility in its share price. The investigation identifies the breach of information that has enabled external investors to pre-empt the announcement.

The arrest of several people taking carrier bags full of money from ATMs in central Berlin prompts a police investigation that indicates the extent of the computer manipulation of the ATM network and starts to unravel the extent of the international transaction arbitrage. As suspicions of major fraud mount, Interpol begins investigations at many of the banks. As banks realise that they have been affected by the APT, they hire forensic accounting firms. Investigations take about 12 months to unravel a full understanding of the complex and obscure criminal operation that has been perpetrated.

Phase 4: Aftermath

The investigations identify several hundred individuals suspected of being involved in the operation, with a number of eastern European nationals being arrested and charged with running malicious internet fraud campaigns infecting many hundreds of financial institutions in the United States, United Kingdom, France, Germany, Norway, and Italy. Several of the ringleaders are extradited to face justice in the US. In conjunction with the arrests, authorities confiscate computers and rogue DNS servers at the attacked locations to investigate further.

Most of the money is never recovered. Banks and other victims of these attacks face huge losses. Details of the formal investigation are announced on major news channels with citizens being advised to take precautions online.

Officials promise to increase efforts to prevent future events of this type through increased investment in improved security measures and awareness campaigns. Additional security measures are introduced for online banking, transaction reconciliation, and interbank transfers that make financial transactions more complex, more costly, and more time consuming.

The attacks have societal implications, with political demands for improved security and greatly increased investment in security, risk management, and cyber insurance, by financial services companies.

10 Cyber Extortion

Many companies are held to ransom by hackers disabling IT functionality to obtain payoffs

Accumulation Stress Test Scenario: **Extortion Spree**

Hackers graduate from personal computer ransomware to create a sophisticated system of encrypting SME business corporate servers. They attack large numbers of enterprises, and demand high ransom payments, on a scale far beyond anything seen even in the PC environment to date.

Cyber extortion is a rapidly growing area of organized cyber crime using ransomware – malicious software – to lock up data or disrupt business until companies make a payoff. This has been a common method of extorting individuals and small businesses for some years. Cyber criminals are increasingly scaling up their operations and using extortion more commonly against larger companies as they gain confidence and technical expertise. Insurance repayment for extortion is a common coverage in many standalone affirmative cyber liability products in the market, and around three quarters of products offer this. Extortion cover is often sublimited in an insurance policy, and some of the terms and conditions may require the insurer to be notified and approve the extortion payment before it is made.

Although ransomware that encrypts data and locks computers is the most common type of extortion, companies may also be asked to make payoffs to avert the threat of other cyber attack types including denial-of-service attacks, data exfiltration breach, and sabotage to deny a company internet or cloud services. There is a growing infrastructure, extortion economy, and organisation around the criminal industry of cyber extortion. The extortionists have become professional at the process, including setting up call centres to assist the individuals that they are blackmailing with the necessary payment steps and providing technical support for the unlocking of their data, providing decryption codes for the software. Support extends to helping their victims set up bitcoin bank accounts to make untraceable payments. Essential to sustaining the extortion business model is that the criminals honour their side of the bargain by freeing up the locked data when the payment is made. And in more cases than not, the user gets their data unlocked once they pay up.

There are many examples of ransomware that have been developed since the first generation of common products came into circulation around 2005, from early programs in 1989. Some common personal computer ransomware products are listed in Table 10.1 and are illustrated with screenshots in Figure 10.1. 19 of the 20 products listed appeared only recently, showing how rapidly the extortion industry is developing. The most common type is crypto ransomware, which encrypts files, but there is also locker ransomware that disables a computer or other equipment.

Most of these PC software programs tend to operate in a similar way. It usually infects a personal computer through an email that appears to be a legitimate invoice, utility bill, or image, or from the user visiting a website. Once the computer is infected, the hardware and software continue to work while personal files such as documents, pictures, and spreadsheets become encrypted, at which point the user is confronted with a pop-up screen demanding a payment to unlock the data and providing a telephone number or other methods of providing payment. The amounts charged for decryption from personal computer ransomware varies but ransom demands in Table 10.1 range from $25 to $500, averaging around $300. In 2012, 2.9% of victims whose data was encrypted reportedly paid the ransom.

10.1.1 The Role of Cryptocurrencies

Bitcoin, a digital currency, and other cryptocurrencies such as Ethereum, Ripple, and CryptoNote have made it easier to monetise cyber attacks semi-anonymously. According to the Financial Times, ‘using Bitcoin is the online equivalent of leaving a suitcase full of cash in a park, with the added advantage that it is soaring in price.’ Prior to cryptocurrencies, hackers used to ask for payment vouchers such as MoneyPak, PaySafe, or iTunes gift cards, which they could resell. Cryptocurrencies have enabled the rapid growth of the ransomware industry, facilitating the untraceable monetization of the ransom demand.

Table 10.1: Common Personal Computer Ransomware Products and Ransoms Demanded[16]

Name	Ransom (in Bitcoin)	Ransom US$	Discovered
Encryptor RaaS	0.2 BTC	$50	July 2015
Troldesh	1.0 BTC	$250	June 2015
Locker	0.1 BTC	$25	May 2015
Tox	1 BTC	$250	May 2015
Pollcrypto	1 BTC	$250	May 2015
Breaking Bad	AUD $450	$350	May 2015
Alpha Crypt			April 2015
Threat Finder			April 2015
Kriptovor			April 2015
PClock2	0.5 BTC	$118	April 2015
Pacman			March 2015
Vaultcrypt			March 2015
BandChor			March 2015
CryptoFortress	1 BTC	$250	March 2015
TeslaCrypt	2 BTC	$500	February 2015
Coin Locker			February 2015
Cryptolocker2015		$100	January 2015
Ransomweb			January 2015
PClock		$291	January 2015
Keyholder		$450	December 2014

10.1.2 Call Centres

Cyber attackers go to great lengths to obtain money from victims. In some cases they set up call centres, in third-party countries. To avoid being traced, the call centres are quickly disbanded after a certain number of payments are extracted.

10.1.3 Scale of Ransomware Operations

It is difficult to estimate the extent of ransomware success – how many personal and small businesses are infected and pay up – because these events often go unreported. However one operation, CryptoWall, is reported to have earned $18 million from U.S. citizens between April 2014 and June 2015, suggesting it might have extorted as many as 100,000 victims in a single year. Worldwide, CryptoWall is estimated by the Cyber Threat Alliance to have earned almost twenty times that much ($325 million).

10.1.4 Local Government and Utilities

Ransomware attacks have also been reported in local authorities, government departments and public sector organisations. Local administrations in Italy are reported to have paid ransoms of about 400 euros (US$440) to recover corrupted files. Even a police department in Tewsbury, MA, near Boston, notoriously paid $750 in bitcoin to prevent its files from being lost. A number of cyber attacks have been reported on utility companies. Some power companies reported that they experience thousands of attempted cyber attacks every month, with some being associated with ransom demands.

[16] Savage, Coogan, and Lau (2015).

Cyber Extortion Scenario

Phase 1: The Roper

A criminal gang calling itself The CryptKickers has been creating personal computer ransomware for a number of years and decides to reinvest its profits to mount a campaign to target companies instead of individuals. They use a new generation 'polymorphic malware generator' to develop highly effective ransomware binaries: the CryptKicker5. This is a sophisticated suite of ransomware tools, and capable of avoiding detection by some of the common corporate IT security systems used by small and medium-sized enterprises. Their software uses a combination of symmetric and asymmetric encryption techniques to optimise the speed at which the data becomes encrypted when the software runs while also maximizing the encryption complexity and making it difficult for defenders to crack the code.

The main advance in CryptKicker5 is that it maps the corporate network by calculating the size of the organisation, identifying back-up processes and storage systems, and targeting the high-value database and accounting files. The software then posts a screen with demands for a ransom payment and containing a clock counting down to 'Total File Deletion.' The amount of ransom demanded is calculated from an algorithm relating the size of the business network and amount of data encrypted to the demand that the attackers think the senior managers of that business might pay.

The CryptKickers set up a number of virtual call centres in Mexico, India, and Malaysia, with a staff of technical support engineers working from temporary locations, scripted to aid the angry callers through a number of processes, including validation – decrypting one demonstration file using a first-stage decryption key – setting up a new bitcoin account if the caller doesn't have one, making a bitcoin payment transfer into the ransom account, and finally providing the full decryption key and guiding the user through the decryption process to recover access to their files. All telephone communications with the call centres are masked and regularly reconfigured and re-routed to deter call tracing and retaliation.

Phase 2: The Hook

A large number of phishing emails are sent out to the target recipients. The target companies have annual revenues between $2 million and $40 million, selected because their security standards are likely to be vulnerable to the CryptKicker5. The CryptKickers identify junior operatives and middle level managers in these companies from their professional social media profiles, and use email media campaign software to send them customised emails containing official-looking invoice PDFs. When the PDF is opened, it activates the payload: malware which runs invisibly in the background. The large majority of the emails are intercepted by the companies' junk mail filters and never appear in the target's inbox, but a small percentage find their way through. Only some of these are opened by the recipients, as many people are suspicious.

At MediaMark Inc., a company involved in online publishing and advertising, a junior accounts clerk receives an email apparently from one of their suppliers with an invoice. He is suspicious, as it doesn't look quite right, but it might be important. He opens the attachment to verify whether it might be legitimate, but it contains a form letter with many paragraphs of marketing language. He forwards it on to the head of his department, to ask whether he needs to do anything with it.

Phase 3: The Sting

A week later, the Director of IT at MediaMark arrives at work to find the office in chaos and a CryptKicker5 screen on every computer on the company network. The screen demands a $5 million payment in bitcoin within 24 hours and provides a phone number to call. The firm's website is unable to access the key data it needs to publish and, while the site is down, the company cannot generate revenue. The IT director reboots the system and bypasses the CryptKicker5 screen to perform a system check. The computers are functioning but most of the files on the servers are inaccessible. She tries to isolate the infected files and reinstall a recent backup but finds that the backup files are also inaccessible. The most recent accessible backup is more than a week old but their system manages live data streams. She calls their security consulting company and asks them to send an emergency incident response team. Then she calls the Chief Executive. The countdown reads 21 hours.

The company alerts the police and calls their insurer who appoints a claim manager to work with MediaMark. IT report that they are working on the problem but do not know when the system will be restored. The security incident response team attempt to break the decryption code on the CryptKicker5 software but the code is complicated and quick success is unlikely. The CEO holds an emergency board meeting conference call as the clock turns to 18 hours. Customers call, asking why their content is not being displayed – MediaMark stalls by telling them that there is a temporary technical malfunction.

The board reconvenes towards the end of the afternoon with 14 hours remaining to consider the ransom payment. The demand represents around six weeks of revenue to the company. It is likely they could rebuild their web service but it will take at least three weeks, and result in significant reputational damage and loss of customers. They consult with their insurer – they have $4m of limit for cyber extortion in their policy, and a deductible of $250,000. To pay the $5m ransom will cost the insurer $3.75m and the company will have to contribute the remaining $1.25m. They decide to explore the possibility of paying the ransom if they can guarantee that it will restore the business functionality.

Phase 4: The Convincer

With 12 hours to go, the IT director calls the CryptKicker number. She is told to make a transfer of 20,000 bitcoins to an account number. She demands proof that CryptKicker will decrypt the files if the payment is made. CryptKicker provides a decryption code and talks her through the process to decrypt a sample file as a demonstration. Ten hours remain.

The board and the insurance claims manager authorize the payment transfer. It is now late evening and takes several hours to arrange a bank payment into the bitcoin account, but as the clock reaches four hours they call the CryptKicker number again. The payment is made. The CryptKicker support engineer provides a new decryption code and then waits online while the IT director goes through a lengthy decryption process and verifies that the files are recovered. The countdown stops at two hours. When the police investigators attempt to trace the CryptKicker number again they discover it has been disconnected and all evidence of its existence has vanished.

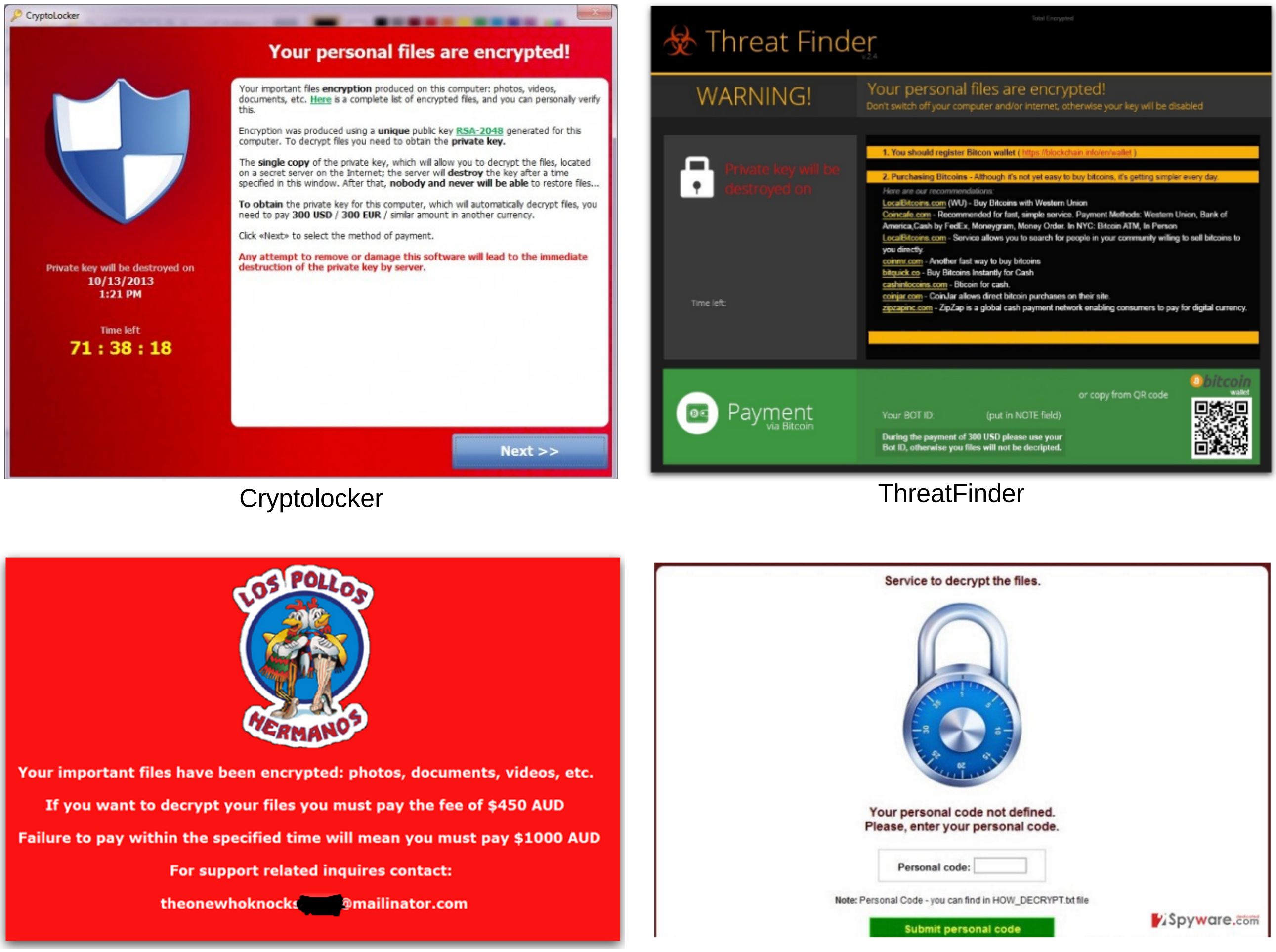
Phase 5: The Squeeze

A similar situation occurs in thousands of similar sized companies. Many of them refuse to pay the ransom and instead rebuild or repair their systems as best they can, while suffering the business disruption and lost income and customers. One or two crack the code to decrypt the locked files. A large number of companies however make the decision that their best outcome is to pay the ransom. Their legal counsel advise that there is nothing illegal in making a ransom payment if they judge it in the best interest of their shareholders, customers, and employees. A large number of these companies are insured and, with the approval of their insurer, find that this makes it easier to restore their business rapidly.

A few larger companies are also affected but, with their heightened security systems, the CryptKicker ransomware produces only localized disruptions to small parts of their networks and these are isolated and ignored.

Each extorted company comes to the same conclusion that it is better to keep news of the incident contained in order to save damage to reputations and customer bases. There is no sharing of information about the extortion between companies – the knowledge about the extent of the incidents is confined to the security companies and the insurers paying out the claims. No government department or regulator is directly involved. There are rumours in the media but not a single headline about the widespread scale of the extortion spree.

The CryptKickers celebrate their new-found wealth and start work on developing CryptKicker6.



CryptoLocker

Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD** / **300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
10/13/2013
1:21 PM

Time left
71 : 38 : 18

Next >>

Cryptolocker

Threat Finder v.2.4

Total Encrypted

WARNING!

Your personal files are encrypted!
Don't switch off your computer and/or internet, otherwise your key will be disabled

Private key will be destroyed on

Time left:

1. You should register Bitcon wallet (https://blockchain.info/en/wallet)

2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:
LocalBitcoins.com (WU) - Buy Bitcoins with Western Union
Coincafe.com - Recommended for fast, simple service. Payment Methods: Western Union, Bank of America,Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, In Person
LocalBitcoins.com - Service allows you to search for people in your community willing to sell bitcoins to you directly.
coinmr.com - Another fast way to buy bitcoins
bitquick.co - Buy Bitcoins Instantly for Cash
cashintocoins.com - Bitcoin for cash.
coinjar.com - CoinJar allows direct bitcoin purchases on their site.
zipzapinc.com - ZipZap is a global cash payment network enabling consumers to pay for digital currency.

Payment
via Bitcoin

Your BOT ID: (put in NOTE field)

During the payment of 300 USD please use your Bot ID, otherwise you files will not be decripted.

or copy from QR code

bitcoin wallet

ThreatFinder

Your important files have been encrypted: photos, documents, videos, etc.

If you want to decrypt your files you must pay the fee of $450 AUD

Failure to pay within the specified time will mean you must pay $1000 AUD

For support related inquires contact:

theonewhoknocks[redacted]@mailinator.com

PowerShell

Service to decrypt the files.

Your personal code not defined.
Please, enter your personal code.

Personal code:

Note: Personal Code - you can find in HOW_DECRYPT.txt file

Submit personal code

Cryptodefense

Figure 10.1: Examples of Ransomware Software Screens[16]

10.1.5 Combating PC Ransomware

Ransomware can be prevented from infecting a computer if it is equipped with good anti-virus software. The most important component of the anti-virus software is keeping it updated. Companies like Symantec, McAfee, Norton, and others track the most common malware and identify its signature to provide their anti-virus software with detection profiles that protect the machines that license it. Extortionists make their money from the initial wave of a new release or from people with lower quality or out-of-date security.

Computer security awareness is increasing in the population in general, and the personal computers in most companies are better protected than they were even a few years ago. This rising standard of security has sparked an arms race between security companies and extortionists, with extortionists developing new techniques and new versions of their ransomware, which security companies detect and devise detection protocols for, and then disseminate across their subscriber base.

10.2 Going Corporate

As the personal computer ransomware industry gains scale, extortionists have become more ambitious and have carried out extortion operations on larger companies and more sizeable organisations.

[16] Savage, Coogan, and Lau (2015).

10.2.1 Severity Scale for Cyber Extortion

Table 10.2 proposes a severity scale for extortion payouts of insured companies, which steps up in orders of magnitude of payout ranges. The large majority of reported ransom payouts from companies that are likely to purchase cyber insurance with extortion coverage are in the lower ranges of E1 and E2, with a few reported payments of E3 to larger companies.

Table 10.2: Severity Scale for Extortion Payouts

Extortion Severity	Range (min. to max. payment US$)	Representative Value (Average Ransom $)
E1	$10,000 to $100,000	$50,000
E2	$100,000 to $1 M	$0.5m
E3	$1 M to $10 M	$5m
E4	$10 M to $100 M	$50m
E5	$100 M to $1,000 M	$500m

The scale includes scope for larger extortion payments to be made, to account for ransom inflation in the future and for use in accumulation stress tests. Very large extortion payments could be made by large or premier businesses in extreme conditions.

Note that the extortion severity scale is defined by the size of the ransom payment. The costs to the company, and the potential insurance payouts, are likely to be significantly greater than this sum as the total costs could include incident response, business interruption, any liability payouts and other costs.

Selected examples of extortion operations reported on businesses are compiled in Table 10.3.

Generally cyber extortion attacks seem to be operating in an environment with low risk and high return. They may be more concentrated in certain industries namely telecommunications, computer system design, and chemical and drug manufacturing sectors, whilst some sectors, such as food and agriculture, have reported a comparably low number of incidents. Financial institutions are prime targets for extortion attacks.

As with many other reports of cyber crime, these accounts are difficult to verify objectively, and there are likely to be many more incidents that are not known publicly.

Small and medium-sized companies have seen numerous cases of customized malware attack their business. Typically, following the cyber attack, the victims contact their insurer. If the insurer does not offer cyber insurance, then they put them in touch with data recovery companies who decrypt the data.

In many cases paid-off extortionists honour their promise and decrypt the data or refrain from the promised attack, but there are counter examples where cyber criminals attack again, for instance, ProtonMail that paid a group called the Armada Collective $6,000 to end DoS attacks on their email service, but were still attacked after paying the demanded ransom.

Table 10.3 shows that the ransoms demanded, and reportedly paid, from large household-name companies can reach millions of dollars. The amounts paid are extremely sensitive, not least because making these amounts public could encourage future attacks. Protecting company reputations ensures that most incidents go unreported. It is likely that cyber extortion payments that are larger than those in the public domain have been made. As with other areas of cyber crime, the recorded maximum observed severity for an event is likely to trend upwards over time.

The moral hazard of paying ransoms is that it encourages the extortionist to repeat their crime on other victims, and the money paid provides them with the resources to sustain and expand their operations.

Table 10.3: Selected examples of cyber extortion attacks on businesses

Financial Institutions Affected	Date	Ransom Amount per Enterprise	US$	Severity
Nokia	2014	"Several millions"	$?,000,000	E3
Three Greek banks	2015	€7m each	$7,507,500	E3
Two Indian conglomerates	2015	"$5 million each"	$5,000,000	E3
UAE Bank	2015	$3m	$3,000,000	E3
Rubber Estate Nigeria Limited	2015	N35 million	$176,000	E2
TalkTalk	2015	£80,000	$117,000	E2
CD Universe	2000	$100,000	$100,000	E2
Domino's Pizza	2014	£24,000	$35,167	E1
VIP Management Services	2003	$30,000	$30,000	E1
Banque Cantonale de Genève	2015	$12,000	$12,000	E1
ProtonMail	2015	$6,000	$6,000	E0
Three Indian banks	2015	'at least 15 machines at 1 Bitcoin each'	$3,500+	E0
Sony	2015	N/A	Unknown	

10.2.2 How Severe Might Ransom Payouts Get?

For the senior managers of a threatened business to agree to payments of ransom, the attacker has to have credible leverage – i.e., they demonstrate that their threat is real and capable of causing the business real harm in considerable excess of the ransom demanded. Also, the managers have to believe that the extortionists will honour their bargain and, in many cases, provide guarantees that the attack will not be repeated.

There may be limits to the amount that a company is willing to pay, or justify to its shareholders. In the future, if ransom payments become common, it is likely to become a political or regulatory issue that may cap the ability of a company to pay large extortion fees. As with other insurance lines that deal with ransoms, such as kidnap and ransom insurance for senior executives and piracy, the insurer providing cyber cover for extortion demands may become closely involved in the resolution of the episode, and so may have some control over the severity of the loss payout.

The extortion severity scale defined in Table 10.2 on page 57 allows for levels of ransom payouts that could conceivably be an order of magnitude larger than those made public so far.

10.2.3 Cyber Extortion Trends

The number of crypto ransomware families on the threat landscape doubled between 2013 and 2015. Extortion claims are trending to become both more frequent and larger in monetary amount, over time.

Two innovations from the past year raise concerns for accumulation risk from cyber extortion coverage:

1. An innovator created a polymorphic malware generator called Tox. This enables large numbers of more sophisticated ransomware to be created to order. While the Tox scheme eventually came to ruin, the business model is being replicated by others. The later business model allows variants of the malware to be created to demand ransom payments as high as $1 million.
2. Extortion demands are supplanting black-market sale of exfiltrated data as the business model for monetizing data breaches by hackers. As the cost of selling data on the black market drops, the value to the hacker is being replaced by demanding ransom payments from the hacked enterprise, threatening to publish all files to the internet if the victim does not pay. Extortion demands could add significantly to the cost of a data breach event, adding compensation for 'cyber extortion' coverage to claims under 'breach of privacy' coverage.

11 Conclusions

11.1 Portfolio Specific Loss Estimation

The accumulation risk scenarios described here are available as loss estimation models in the RMS Cyber Accumulation Management System to model the loss to an insurer's portfolio, structured according to the proposed Cyber Exposure Data Schema.

These scenario models provide a capability for insurers to carry out routine monitoring of their aggregation risk, assessing what their likely claims payout would be to these benchmark extreme events as their portfolio grows. They enable a diagnosis of the key drivers of losses – which enterprise size classes, business sectors, coverages, and attributes of companies in their portfolio are contributing most to their loss potential, and enabling portfolio management to optimize premium income against loss potential.

These events are all extreme but plausible. They are considerable extrapolations from some of the worst incidents and patterns of loss seen to date, but they are constrained by what we know about the technical issues of the cyber loss processes and the threat actors' capabilities.

They provide helpful pointers to use in setting a company's risk appetite. We believe that using these scenarios will help companies improve their knowledge of the cyber peril and help them gain confidence in establishing their risk appetites for insuring cyber.

11.2 Extremes and Scenarios

We have assumed that each of the scenarios occurs separately as a different process. It is not reasonable to expect that these extreme events would all occur in the same year, so we do not propose that a company's worst case is all of these scenarios added up. They are alternative events to stress test a portfolio from several different angles. It is however true that several of these loss processes can occur together in an individual loss incident; a DDoS attack can be part of a data exfiltration attack, a financial transaction theft could occur with an extortion incident, and so on.

11.3 Multiple Scenarios

It is important to consider all the cyber loss processes in monitoring accumulation risk. Data exfiltration is probably the most common current concern for cyber insurers, and the one that causes the most significant day-to-day cost, but it may not pose the greatest catastrophe potential to all cyber insurance portfolios.

Each portfolio will have different losses from each scenario and may rank them differently as their losses will depend on the mix of business sectors, enterprise sizes, and jurisdictions.

The Leakomania scenario for example has different impacts on enterprises of different size, and affects some business sectors much more severely than others. The scenario also projects quite different incidence rates for different country jurisdictions, and different cost structures depending on the country's compensation practices and legislative environments. Companies managing international portfolios of cyber insurance may have different perspectives from those focussed in U.S. Insurers with different blends of portfolio across companies of different size and penetration into different business sectors will benchmark to very different levels of loss.

Companies that are focused on the small and medium-sized enterprise (SME) sectors will want to consider their accumulation exposure from different types of cyber loss processes than those that concentrate on premier enterprises. SME portfolios will have higher impacts from the Extortion Spree scenario than premier portfolios. Portfolios with high concentrations of e-commerce companies will have higher loss exposure to the Cloud Compromise and Mass DDoS scenarios than manufacturing-heavy portfolios. Financial services oriented portfolios will have highest losses from Financial Transaction Interference scenario.

11.4 Accumulation Management Segmentation

These scenarios and loss processes have significantly different impacts on different business sectors, so portfolios with different sectoral mixes will find they have different risk profiles.

The suite of scenarios for the range of cyber loss processes is intended to cover a range of different business sector mixes, enterprise size classes, and countries of the world. The scenarios offered should provide a wide enough range of options to benchmark a broad spectrum of cyber insurance portfolios being managed in the market or targeted for future expansion.

Each of the market segments of enterprise size class, business sector, and jurisdiction can be considered as an accumulation 'zone.' Losses can be managed within these zones and differentiated from each other. In the early stages of natural catastrophe risk management, risk was managed by CRESTA zone – geographical areas that differentiated the risk. These market segments are the equivalent of CRESTA zones in the field of cyber risk. They contain and separate the risk for portfolio management purposes.

11.5 Diversification and Expansion Strategy

The system and its suite of scenarios provide some guidance on accumulation management strategy. The analysis can provide quantification of the diversification benefits that will be obtained from spreading cyber insurance business across the accumulation management market segments. This also enables strategies to be developed for expanding capacity for cyber insurance while minimising the potential for correlated cyber catastrophe loss.

11.6 Expanding Capacity Safely

We have laid out an approach to monitoring and managing cyber accumulation risk. We believe that it provides a framework for companies to assess their own risk appetite for cyber and will prove a useful tool for analysing diversification and exploring loss potential. We hope that it will enable insurers to gauge their loss potential with more information than they had previously and to develop strategies for safely expanding their capacity in the cyber insurance market.

12 References

Advisen and PartnerRe, 2014; **Cyber Liability Insurance Market Trends: Survey**; October 2014.

Advisen, 2014; **The Cyber Liability Insurance Market**; Advisen Presentation; Jim Blinn; 14 March 2014.

Advisen; 2015; **Cyber insurance market update**; Advisen Insight; Advisen Cyber Risk Network; 15 January 2015.

AIRMIC; 2012; **Airmic Review of recent Developments in the Cyber Insurance Market & commentary on the increased availability of cyber insurance products**; Airmic Technical Guide, Association for Risk and Insurance Management Professionals; 7 June 2012.

Allianz; 2015; **A Guide to Cyber Risk: Managing the impact of increasing interconnectivity**. 9 September 2015.

Anderson, Roberta, A.; 2013; **Insurance Coverage for Cyber Attacks**; K&L Gates; The Insurance Coverage Law; Bulletin, Vol. 12, No. 4; May 2013.

Aon Benfield; 2014; 'U.S. Cyber Insurance Market' in **Insurance Risk Study: Growth, Profitability, and Opportunity**; Ninth edition, 2014.

Aon Benfield; 2014; Cyber Risk Update for Insurers; October 2014.

Aschkenasy, Janet; 2013; **"CGL exclusions will fuel cyber purchase trend"**; Advisen Cyber Risk Network; 28 Nov 2013.

BakerHostetler; 2013; '**International Compendium of Data Privacy Laws**'; Bakerlaw.com.

Betterley Report, 2015, **Private Company Management Liability Insurance Market Survey—2015**; August 2015;

Betterley Report, 2015; **Cyber/Privacy Insurance Market Survey— 2015**; June 2015.

Biener, Christian; Eling, Martin; Wirfs, Jan Hendrik; 2015; **Insurability of Cyber Risk: An Empirical Analysis**; Working Papers on Risk Management And Insurance, No. 151 – January 2015.

Cambridge Centre for Risk Studies, 2014, **Stress Test Scenario: Sybil Logic Bomb Cyber Catastrophe**; Cambridge Risk Framework series; Centre for Risk Studies, University of Cambridge.

Cambridge Centre for Risk Studies, 2015, **Cyber Exposure Data Schema Principles (v0.1)**: First consultation document on the principles for developing a standard data schema for managing cyber exposures.

Cambridge Centre for Risk Studies, 2015, **Cyber Exposure Data Schema (v0.5)**: Second consultation document to develop a standard data schema for managing cyber exposures. This document included a section documenting the cyber insurance market practice review.

Cambridge Centre for Risk Studies and Risk Management Solutions, Inc.; 2016; **Cyber Insurance Exposure Data Schema v1.0**; Cyber Accumulation Risk Management working paper.

CRO Forum, 2014; **Cyber resilience – The cyber risk challenge and the role of insurance**; Dec 2014.

Cyber Risk & Insurance Forum (CRIF); 2014; **Cyber Risk Matrix: Connecting Your Threat, Impact, & Insurance**.

Cyber Risk & Insurance Forum (CRIF); 2015; **Cyber Risk Legal Update**; Aug 2015.

ENISA; 2012; **Incentives and barriers of cyber insurance market in Europe**; European Union Agency for Network and Information Security; June 2012.

EY; 2014; **Cyber insurance, security and data integrity; Part 1: Insights into cyber security and risk**; June 2014.

EY; 2014; **Mitigating cyber risk for insurers; Part 2: Insights into cyber security and risk**; June 2014.

Gallen, Christine; 2015; ABI Research on **"Risks to Drive US$10 Billion Cyber Insurance Market by 2020"** Market Watch; 29 July 2015.

Hartwig, Robert P. and Wilkinson, Claire.; 2014; "Cyber Risks: The Growing Threat**.**" Insurance Information Institute; 2014.

HM Government, UK, 2014; **Cyber Essentials Scheme**; June 2014.

HM Government, UK, 2015; **Cyber Essentials Scheme – Assurance Framework**; January 2015.

Lloyd's/ABI, 2015; **A Quick Guide to Cyber Risk**; Lloyd's in Partnership with Association of British Insurers.

Lloyds, 2015, **Lloyd's Business Blackout Report**; Emerging Risk Report - 2015.

Long Finance, 2015; **Promoting UK Cyber Prosperity: Public-Private Cyber-Catastrophe Reinsurance**; July 2015; A Long Finance report prepared by Z/Yen Group and co-sponsored by APM Group.

Marsh & UK Government, 2015, **UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk**; March 2015.

Marsh, 2015, **A Framework for Managing Cyber Risk**; April 2015.

McGuireWoods; 2013; **A Buyer's Guide to Cyber Insurance**; 2 October 2013.

PwC; 2015; **Insurance 2020 & beyond: Reaping the dividends of cyber-resilience**.

Surfass, Stephen A.; 2015; 'Cybersecurity in 2015'; Presentation to Reinsurance Association of America Annual Meeting April 23, 2015; DrinkerBiddle.

Thomas, L. and Finkle, J.; 2014; **"Insurers struggle to get grip on burgeoning cyber risk market"**; 14 Reuters; 14 July 2014.

U.S. Department of Health and Human Services; 2014; '**Data breach results in $4.8 million HIPAA settlements**'; HHS.com; May 7, 2014.

Verisk; 2014; **Cyber Insurance Survey;** Prepared for ISO by Hanover Research, November 2014.

Verisk; 2015; **ISO Cyber Coverage Options for Small and Midsize Businesses**; 3 March 2015.

World Economic Forum; 2015; **Partnering for Cyber Resilience: Towards the Quantification of Cyber Threats**; in collaboration with Deloitte; January 2015.

Zurich; 2014; **Risk Nexus - Beyond data breaches: global interconnections of cyber risk**; Atlantic Council; April 2014.

Zurich; 2015; **Risk Nexus - Global cyber governance: preparing for new business risks**;Report in collaboration with ESADEgeo-Center for Global Economy and Geopolitics.