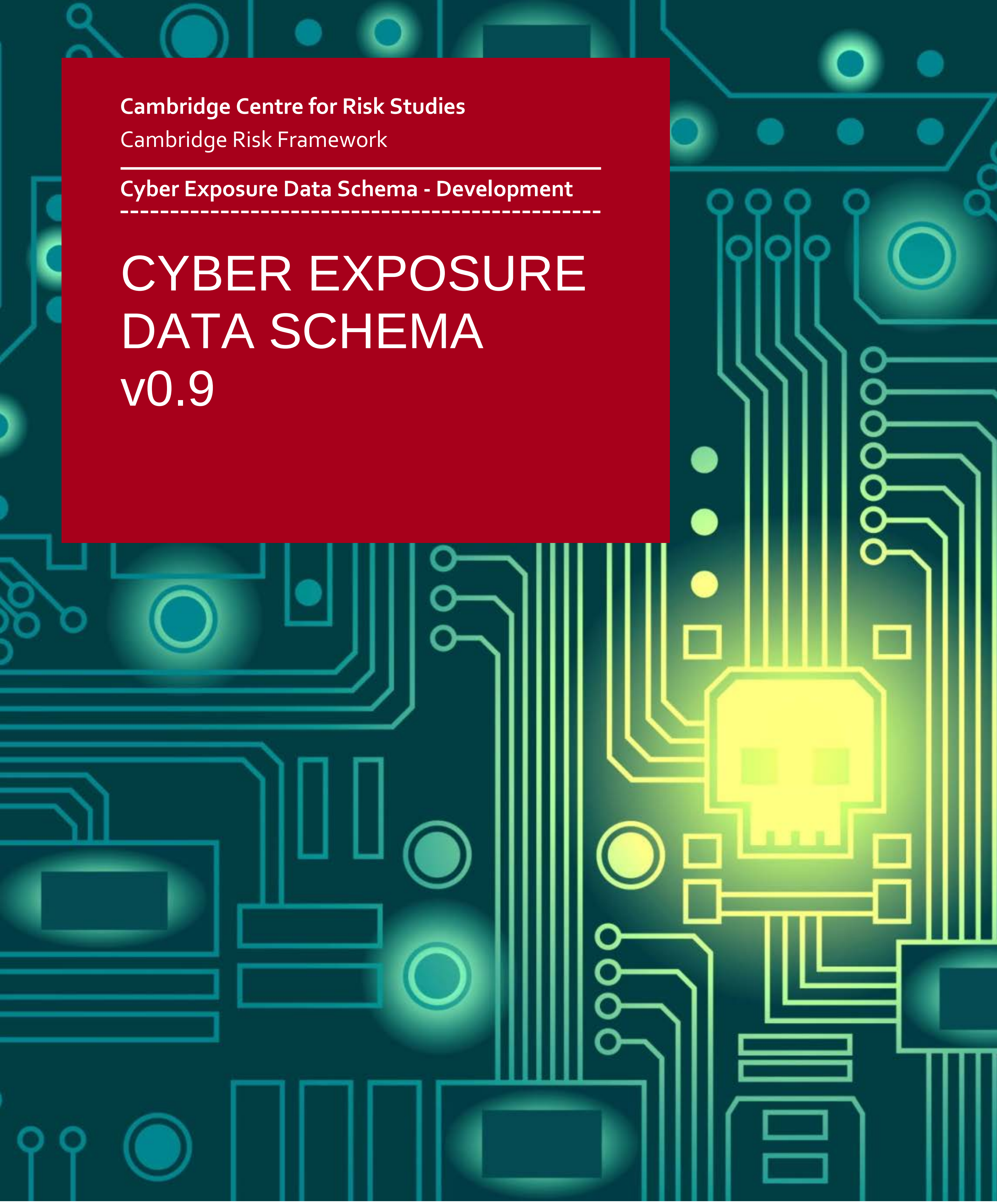

Cambridge Centre for Risk Studies

Cambridge Risk Framework

Cyber Exposure Data Schema - Development

CYBER EXPOSURE DATA SCHEMA v0.9

Centre for
Risk Studies

UNIVERSITY OF CAMBRIDGE
Judge Business School

Proposed Cyber Exposure Data Schema (v0.9)

1 A Data Schema for a Growing Cyber Insurance Market

The market for cyber insurance is growing rapidly and there are several initiatives to develop models of cyber risk and tools for cyber risk management decision support.

The growing cyber insurance market has identified a need for a cyber insurance data schema – 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) enable the development of models for cyber risk that will be applicable to multiple users

c) facilitate risk transfer to reinsurers and other risk partners, and risk sharing between insurers

d) provide a framework for exposure-related dialogues for risk managers, brokers, consultants and analysts.

Over the past year, the Cambridge Centre for Risk Studies at the University of Cambridge has worked with a number of insurance industry organizations and many of the leading practitioners writing cyber insurance to develop a cyber insurance exposure data schema. The cyber risk research at Centre for Risk Studies is supported by a consortium of insurance companies, corporates, industry organizations, and RMS Inc. This is the third round of public consultation on the schema and we are grateful to the many people who have provided inputs into the development of the schema to date.

This document sets out the latest version of the schema incorporating the feedback received. It sets out the consensus principles for the schema, the structure and the proposed tables and definitions of the components. We propose to finalize this process by the end of 2015 and publish the final schema as an open source document in early 2016.

This data schema is intended to be **agnostic to the type of model and account management system being used**, to facilitate analysis broadly, and expand the cyber insurance industry.

A standardized exposure data schema will enable reporting and monitoring of exposure under different categories. Establishing the important categories for exposure segmentation is a key objective of the consultation. In the London market, Lloyd's Managing Agents are now being required to report their aggregate cyber exposures explicitly. This schema is intended to help with this process. Other markets have similar needs to monitor and report on cyber exposure.

A company that reviews its own cyber insurance exposure using the schema will be capable of:

- reporting exposure aggregates by different types of coverage and potential loss characteristics to a level of granularity that can inform risk appetite decisions
- estimating losses from scenarios or other types of risk models to the exposure recorded in the database
- identifying 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
- enabling companies to share or transfer information about exposures in a consistent and standardised 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 of, or a combination of, line of business, geographic region and industry sector, or other attributes in the schema.

Comments and feedback are appreciated. Please provide any comments to Jennifer Copic, Cyber Project Research Associate, Centre for Risk Studies at University of Cambridge. email: j.copic@jbs.cam.ac.uk Tel: +44 (0) 1223 761075

1.1 Feedback acknowledgements

We gratefully acknowledge the inputs to the development of the schema received to date. The final publication will cite the individual contributors of feedback to the schema.

Feedback has been received from

- Insurers and reinsurers who are involved in writing cyber insurance in most of the major and emerging markets for cyber insurance, including US and North America, London market, Bermuda, European markets, Japan, and Southeast Asia
- Reinsurance brokers
- Management consultants and advisors
- Internal insurance modelling teams
- External commercial model vendors

We also gratefully acknowledge the assistance of

- Lloyd's Emerging Risks team for participating in the steering committee
- Reinsurance Association of America, for circulation to membership and providing a platform for schema dissemination at RAA meetings
- CRO Forum for collaboration on cyber data standardization initiatives
- Lloyd's Market Association cyber committee for circulation of consultation documents to members
- Advisen, for inputs into the schema and providing market data and assistance

1.2 Principles of Schema Design

The schema has been developed according to a number of guiding principles.

A. Accumulation Focus

The first iteration (version 1.0) of the data schema will focus on the data required for ***managing exposure accumulations***, rather than other areas of decision support, such as underwriting individual accounts, risk selection, pricing decisions, claims management or operational risk. Some of the key attributes developed for this schema will be of use in these other areas, but maintaining focus on exposure is important.

Rationale: The agreed consensus is that the priority for data standardization is to assist accumulation management and to measure the amount of cyber exposure in an insurer's portfolio.

Underwriting practices and data requested by insurers for risk selection and pricing purposes varies widely and is regarded as competitive-advantage expertise. Proposals to standardize risk selection and pricing data are less likely to be adopted, and the challenge of standardizing the wide range of potential variables being used would be complex. Once an insurance contract has been bound, the information that the insurer captures to manage exposure is a simpler subset, has more commonality, and is less proprietary. We propose to make this the focus of the cyber exposure data management.

B. Early Release of an Initial v1.0 Schema

Many companies have an urgent need for cyber exposure management and are in the process of implementing systems that would benefit from a standardized data schema.

We have limited the complexity and ambition of the schema to enable an initial version of the Cyber Exposure Data Schema 1.0 to be published in early 2016.

Rationale: Having a simple data standard early in 2016 will be better for market participants than waiting to refine a more complex or comprehensive data standard that will take longer to develop and release. Future upgrades to the data standard are likely to be offered fairly rapidly, to expand the scope of the coverage and to increase the complexity. The intention of the version 1.0 schema is to capture 80% of the complexity of the problem, allowing the remaining 20% to be added over time, as the problem becomes better understood.

C. Simple as Possible

An important principle is to make the data schema as simple as possible.

There are practical resource implications of proposing to add new parameters of data to existing information management systems. The more complex and extensive the additions, the more resources and more time will be required to implement the data schema.

The emphasis will be to start simple, and to keep it stable, extensible, and backwardly compatible. It is intended to expand the schema and develop it further over time. It will be possible for individual companies to customize it and extend the schema for their own more sophisticated needs, but the core data standard for exchanging information between parties will constitute the minimum set of requirements possible.

Rationale: Keeping the Cyber Exposure Data Schema version 1.0 simple will maximise adoption, which is an important objective of developing the cyber exposure data schema. We propose to develop the simplest system that will be capable of capturing 80% of the problem, rather than trying to develop a sophisticated system that can apply to every possible situation. We propose to favour breadth over complexity. We expect the data schema to grow in sophistication over time.

D. Extension to Existing Exposure Management Systems

The proposed approach is to provide an extension to ***existing policy and account management database records***, where information is added to existing records of cyber exposure. The exposure data schema is designed to add a number of cyber exposure attributes to existing account or policy-level records.

Organizations that have access only to aggregate levels of exposure data can make assumptions about the distribution of the cyber-specific attributes of the accounts within the aggregated exposure.

Rationale: As the insurance market practice review has demonstrated, current practice varies widely, and accounts may have very different values for each segment of their cyber coverages, so this is best accumulated through individual records, rather than assumed homogeneity in an aggregate value.

An account-level or policy-level data structure has the advantage of being able to apply deductibles, limits and policy-holder information such as exclusion clauses in a more accurate way than using aggregate totals.

E. Exposure Management structured around Cyber Coverage Categories

The proposed approach to tracking exposure is to identify the elements of coverage for cyber-induced loss that are offered in insurance policies. A categorization of loss coverage is proposed that identifies the components of cover that are commonly offered in affirmative cyber products, and that also constitute elements of silent cyber exposure in insurance products that may not have cyber exclusions.

Rationale: The proposed categorization of cyber loss coverage (Table X) has been developed from a detailed review of cyber and traditional insurance products in the market, and refined through consultation rounds with insurance market practitioners. Cyber insurance products being offered on the market vary significantly in which elements of coverage are grouped in a product, and also vary in the way that limits, sublimits and different terms and conditions may be applied to different components of coverage. Tracking the components of coverage is essential to exposure management.

Categories of cover are identified in insurance policies and can be accumulated across multiple accounts. We believe that capturing these fairly granular elements of exposure is the only way to track cyber risk across widely different policy structures, product offerings and lines of business across the market.

2 Consultation Process

The proposed Cyber Exposure Data Schema has been developed through an initial insurance market practice review, where the cyber products and coverages available in the market were collated and compared, and iterations of consultation with market practitioners and industry groups.

The previous consultation documentation rounds were:

Cyber Exposure Data Schema Principles (v0.1): First consultation document on the principles for developing a standard data schema for managing cyber exposures.

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.

2.1 Feedback from v0.5 Consultation Round

Feedback from the v0.5 consultation round has broadly confirmed the structure and approach of the schema and has helped refine it with a number of modifications and extensions incorporated in this latest iteration.

- Overall feedback has been generally very supportive and positive about the initiative, with a broad endorsement of approach and proposed structure
- Each of the sections of the schema has support and recognition of the rationale for why it is there.
- Most respondents are satisfied with the completeness and number of categories in each of the proposed tables – however there were a number of detailed suggestions about refinement that have been incorporated.
- There is continued trade-off tension between the appropriate level of detail that might ultimately be desirable and the need to keep the initial schema as simple as possible to get an early version released.
- There were several suggestions that once the schema was available for accumulation, it could be further extended to other areas, such as operational risk, claims, pricing, and underwriting.
- Common feedback on the proposal of including Cyber Risk Attributes was that this is not currently easily available from all of the insureds or held in exposure management systems, but that these attributes were desirable and necessary to manage accumulations, and that including them in the schema would encourage them to be captured in the future.

2.2 Changes in v0.9

Some suggestions from multiple respondents have resulted in changes to the schema for version 0.9. Changes include:

1 Peril codes have been introduced to identify where cyber is triggering perils that may have coverage under some All Risks policies, specifically cyber-induced fire and explosion for property lines. We have proposed that cyber terrorism is identified as a separate peril code, rather than as a coverage category (in v0.5) – cyber terrorism could trigger any of the coverage categories and it is important that coverage categories are non-overlapping.

2 Coverage categories have been refined, specifically to clarify the Liability coverages. This is to ensure that coverage is complete and non-overlapping. Comments suggested that the Liability - General Commercial category duplicated coverages in several of the other categories. Liability is now split into Products and Operations, Technology Errors and Omissions, Professional Services Errors & Omissions, and Directors and Officers.

3 Wordings of coverage categories have had minor edits to clarify meaning, and each coverage category now specifies whether it includes first party or third party losses.

4 Creation of sub-divisions of the business sectors Information Technology and Financial Services to reflect that these are two of the most important sectors of the cyber insurance market, and contain sub-sectors with significantly different risk characteristics and aggregation potential. Each of these two sectors have been divided into three sub-sectors (Information Technology into Hardware, Software, and Services; Financial Services into Banks, Insurance, and Investment Management).

5 A mapping of NAICS codes to the business sector categories will be published with the schema, in response to requests from a number of respondents.

6 A number of people requested a standard identifier for individual companies, to identify when the same company might be represented by several policies either arising from different divisions within an insurance company or in portfolios of risk transfer or risk sharing with counterparties. Research is currently ongoing to explore the practicality of this and identify which source of data would be the most appropriate for a standardized enterprise identification code.

7 There was a request for a standard definition of a metric of ‘exposure’ from the schema. We have proposed the simplest metric of total limit as the representation of exposure (minus deductible, and proportionate for any co-share).

8 In response to feedback, for cloud service provider, the previous proposal of estimating the importance of providers from their monthly billing has been amended to estimating the business interruption value per day if service is lost from cloud service provider(s).

9 There were several comments on the need for a common measure of cyber security hygiene at a company, and so an additional attribute has been added to accommodate this. This was omitted by choice in the v0.5 proposal as there is no industry consensus around what metric to use for cyber security quality. If an attribute to describe cyber security hygiene is to be a useful and practical addition to exposure management it needs to be standardized to enable companies to exchange information about it meaningfully. We have proposed that if a metric is used, such as a security score or a minimum standard certification, this measure should be convertible into the percentile in the distribution of cyber security quality that presumably exists across the population of insurable enterprises.

2.3 Cyber Exposure in the Insurance Market

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

A. Affirmative Stand-Alone 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

- Stand alone 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 property 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 to cover a privacy breach.

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, apart from certain nominated perils, for example Fire, Lightning, Explosion and Aircraft Impact (FLEXA). These policies have exposure to a cyber attack if one were to trigger one of the nominated perils 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 insurers have identified that may contain silent cyber exposure include property, casualty, energy, marine, aviation, aerospace, specialty, auto, personal lines, terrorism, war and political risk, and others.

2.4 A Framework for Identifying and Managing Cyber Exposure

The proposed Cyber Exposure Data Schema provides a categorization of coverage by types of cyber-induced loss for use across these four areas of exposure, and proposes an approach for companies to be able to flag cyber exposures in the policies they write.

3 Cyber Exposure Data Schema v0.9

An insurance company typically manages its exposure in an existing account management or policy management system that includes information on

a) Policy details, such as detailed information on the policyholder, internal codes for account tracking and reconciliation of premiums paid, claims management system; history of account;
b) Information about the insured asset(s) appropriate to the line of business, for example location, primary characteristics, secondary modifiers, and other parameters for property; information on company activities for general liability, etc.
c) Cover provided, coverage codings, any coverages that are broken down by sub-limits, with their limits, retentions and contractual terms;
d) Exposure values; total insured value; total limit and retention.

Companies typically do not share some of this information (such as premium information) externally, but may share other parts of this information with counterparties for risk transfer, regulatory requirements, or for other purposes.

A key use of the exposure data is to assess accumulation risk – to analyse how a portfolio of policies might suffer high losses through correlated events.

3.1 Total Exposure Value

For each account or policy, a total exposure value should be estimated, based on the total maximum limit, minus the deductible or excess. The total exposure value should be used to identify and rank the accounts and policies that constitute the most exposure.

3.2 Structure of schema

The proposed Cyber Exposure Data Schema provides a standardized minimum set of information to augment the existing exposure information, or structure existing information in a consistent way.

We propose to ensure that the following six classes of exposure attributes are consistently captured with high-level information:

1. Cyber Peril Codes
2. Geographical Jurisdiction
3. Cyber Loss Coverage Categories
4. Business Sector
5. Enterprise Attributes
6. Cyber Risk Attributes

3.3 Cyber Peril Codes

Recognising the cause of loss through a peril code will help with identifying cyber activity that relates to insurance policy wordings and loss types. There could potentially be a number of different types of perils triggered by cyber as a proximate cause. The minimum number of cyber peril codes for the initial schema will be:

- **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[1]').
- **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])
- **Cyber Terrorism** – First and third party claims from a cyber event due to breach of security, that either causes physical asset damage or other losses, where the perpetrator has been identified as a terrorist, terrorist group or nation state and where the event was defined by government as an act of war or a terrorist attack.

Other codes may be added in the future, as required.

3.4 Geographical Jurisdiction

To manage cyber accumulations by geographical market, accounts should be identified by the jurisdiction that will determine pay outs and regulatory attitudes to cyber loss.

- In United States this will be by state.
- In all other territories it will be by country.

3.5 Cyber Loss Coverage Categories

Cyber exposure will be identified by the loss coverage categories that the product and insurance coverage provides. Table 1 provides a high level categorization of cyber loss coverage categories.

For each policy, the coverages contained should be identified, using these categories. A company may offer collections of these coverages in a standardized product or typical offering, and companies may want to define collections of coverages as a product they offer, and relate policies to that product structure. From reviews of cyber insurance market practice, there is little consistency across the market in terms of the combinations of coverages offered in products, so this coverage categorization is offered as a method of understanding what products contain which coverages.

Several of these loss coverage categories are typically sub-limited in stand-alone cyber insurance products and for these, the schema should be used to capture the amount of exposure represented by that sub-limit, with appropriate deductibles or other contractual structure information.

Where the cyber coverage category is included within an insurance policy but not sub-limited or the only coverage category, then it should be identified as one of the categories of cover and subject to the conditions and contractual structure of the policy, including total limits and deductibles where applicable.

3.5.1 Potential for further granularity in coverage categories

The loss coverage categories listed in Table 1 represent primary classes of coverage, and the loss categorization can be treated as hierarchical, with subcomponents of cover identified if required. For example category #6 'Incident response costs' could be broken down into subcomponent costs of external crisis services, forensic investigation, restitution and replacement of compromised equipment, and other elements. In this first version of the schema it is proposed that the initial high level cyber coverage categories are sufficient for the main exposure assessment exercises required by most insurers, but that there is scope for more detailed granularity of analysis in the future if required.

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

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

Table 1: Proposed categorization of cyber loss coverage - primary categories

v0.9 Code	Cyber Loss Coverage – Primary Category	1st party	3rd party	Description
1	**Breach of privacy event**	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**	1st		The cost of reconstituting data or software that have been deleted or corrupted.
3	**Network service failure liabilities**		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**	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**		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**	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**	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**		3rd	Third party liabilities arising in relation to product liability and defective operations.
9	**Liability – Technology Errors & Omissions**		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**		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**	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)**	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**	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**	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**	1st		The cost of expert handling for an extortion incident, combined with the amount of the ransom payment.
16	**Intellectual property (IP) theft**	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**	1st		Cover for costs of clean up, recovery and liabilities associated with a cyber induced environmental spill or release.
18	**Physical asset damage**	1st		First-party loss due to the destruction of physical property resulting from cyber attacks.
19	**Death and bodily injury**		3rd	Third-party liability for death and bodily injuries resulting from cyber attacks.

4.1 Business Sector

Business sector segmentation is important for exposure management, market development, and for the risk characteristics of companies in those sectors.

Table 2 provides a high-level business sector classification that incorporates most of the terminology and classes that have been encountered in the cyber insurance market and that encompass the main activity sectors in the economy and segmentation used in statistical reporting and analysis.

4.1.1 Economic sectors and cyber insurance activity

Classifications of enterprises operating in the economy can be made extremely granular, and there are several standard systems that already exist for coding and classification of companies, most of which are hierarchical and become more granular with different levels of resolution. Of the five leading coding systems (SIC, NAICS, GICS, ISIC, and NACE) used in different regions of the world, our consultation has identified that 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. Table 3 provides a mapping of NAICS codes to the cyber exposure data schema business sector classes v0.9 for the most recent NAICS coding system in use (2012). Concordance tables that map other coding systems and vintages to NAICS, such as SIC, can be found online, for example here.

Table 2: Business Sector classification for cyber exposure

v0.9 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 functions.
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 provides 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 process 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	**Defense / Military Contractor**	Defense 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, theater
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**	

5 Enterprise Size and Economics

5.1.1 Number of Employees

Size of enterprise is one of the leading attributes of accounts collected by cyber insurance writers, both as exposure differentiator, and as a risk factor for breach of privacy incidence. Most writers of cyber insurance differentiate at least large companies from small-and-medium-enterprises (SMEs).

Instead of adopting a classification of companies into pre-determined banded sizes of company (such as 'medium size' being 100 to 499 employees etc.) we propose that the **actual number of employees** is captured as a numeric data field. This will enable companies to do their own banding of company sizes as data provides better understanding of the sensitivity and usefulness of this attribute.

Insurers who want to add this attribute to existing accounts of commercial insureds but who do not currently hold this information can obtain data on the number of employees at an enterprise from third party data providers such as Bloomberg, Reuters, S&P Capital IQ, Google Finance, Yahoo Finance, etc.

5.1.2 Annual Revenue

Revenue information is important both as a cross-reference for company size, and also for exposure estimation where policy coverage includes business interruption or loss of revenue compensation. The annual revenue of a public traded company is public information, and if not provided can be found from annual reports and publicly accessible datasets.

5.1.3 Cyber economy attributes

Subdivisions of the annual revenue to reflect the company's exposure within the cyber economy are proposed as cyber risk attributes, below. These include

- The amount of the annual revenue of the company that is internet-based (i.e. the hourly rate of loss that would occur if the company loses internet connectivity)
- The amount of the annual revenue of the company that is cloud service provider based (i.e. the hourly rate of loss that would occur if the company lost service from its cloud service provider(s)

6 Cyber Risk Attributes

In addition to the categorization of accounts by geographical jurisdiction, loss coverage category, business sector, and size of enterprise, 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.

6.1.1 Breach of Privacy Potential: Number of Confidential Records

Almost all of the coverages provided in affirmative cyber policies include cover for a breach of privacy event. The exposure to this coverage category is from the number of confidential records that could potentially be disclosed from the insured enterprise.

Where possible, we propose that the Cyber Exposure Data Schema captures the total number of confidential records maintained by the company under the following three categories:

1. Total number of records of **Personally Identifiable Information (PII)** maintained by the enterprise, maximum during the year
2. Total number of records of **Payment Card Information (PCI)** processed by the enterprise during the year
3. Total number of records of **Personal Health Information (PHI)** maintained by the enterprise, maximum during the year

Insurers are encouraged to record other and additional categories of confidential data, such as commercially confidential information, trade data, commercial secrets, and intellectual property. However these are more difficult to provide as an objective metric of the amount and importance of these data, and so are less amenable to inclusion in a standardized data schema.

Additional qualifiers may also be important for insurers to record, such as whether the confidential records held by the insured are kept encrypted. However the verification of this and the difficulty of estimating the significance of encryption, means that this is not proposed as part of a standardized data schema.

6.1.2 BI Potential from Internet Failure

A high percentage (69%) of affirmative cyber insurance includes one or more loss coverage categories for business interruption. There is potential for multiple accounts to suffer a business interruption loss resulting from any widespread outage of the internet, even if the internet is generally resilient and the likelihood is very low of any widespread or lengthy disruption of the internet.

Where possible we propose that the Cyber Exposure Data Schema captures the potential for systemic correlated loss arising from dependence on the internet for business activity. This will enable those engaged in risk transfer, such as reinsurers, to assess their accumulations of risks from different cedents' portfolios.

- Estimated business interruption value per day if **internet connectivity is lost**
- Deductibles/retentions and limits on business interruption coverage from internet disruption

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

The potential for multiple accounts to suffer a business interruption loss from the failure of a cloud service provider is an additional systemic risk, with a large number of insureds depending on a small number of industry-leading cloud service providers, even if the likelihood of a cloud provider being disrupted is very low.

Where possible, we propose that the Cyber Exposure Data Schema captures the potential for correlated loss arising from dependence on individual cloud service providers by recording the amount of usage each insured has on each of the major cloud providers. The monthly billing from a cloud service provider is the clearest metric of usage and productivity dependency.

- Estimated business interruption value per day if **service is lost from cloud service provider(s)** (up to three largest providers)

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

Over three quarters of affirmative cyber insurance products included loss coverage for either business interruption or financial loss that could potentially be triggered from the failure of their financial transaction system provider. There is the potential for systemic correlated risk, with a large number of insureds depending on a small number of commonly-used payment transaction systems, even if these transaction systems are highly secure and the likelihood of transaction systems being compromised is very low.

Where possible we propose that the Cyber Exposure Data Schema captures the potential for systemic correlated loss arising from dependence on industry-standard payment and transaction systems.

- Provide the value of the average monthly transactions to the insured’s largest **named financial transaction or payment system** (up to three largest providers)

6.1.5 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 v0.9 schema includes a cyber risk attribute of cyber security assessment.

This can be either a cyber security score – derived from weighting multiple variables that have been assessed, or a certification affirmation that the company meets certain threshold standards.

There are a very large number of cyber security scores in use, some are available commercially and through consulting engagements, others are offered through scorecard checklists. There is no market standard and no consensus around the effectiveness of any particular security score system in predicting the risk of cyber losses in enterprises, although a number of score systems claim to correlate their scores with loss risk.

There are also many IT security certification systems that are in use, ranging from government-backed minimum standards, through to customized penetration testing to affirm certain defined standards of security quality.

The cyber exposure data schema is proposed as a method of standardizing exposure reporting, and in integrating two or more schedules of policies, potentially from different insurance companies, in a reinsurance or market transaction. It will be difficult to compare and benchmark different systems of cyber security assessment in use by each insurer.

Instead we propose that each company uses the cyber security assessment system of its own choice and provides the score assigned to the account, or the fact that the account has a named security certification, but that it defines the scoring system or certification system to any other counterparty provided with its data, exposure report, or risk model that includes their cyber security assessment, as follows:

- The cyber security score should be defined in a supporting document for the counterparty in terms of 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 United States, ranked by quality of cyber security”.

- A cyber certification standard should be defined in a supporting document for the counterparty in terms of the percentile of the total number of enterprises in that jurisdiction that are expected to qualify for that certification, ranked by quality of cyber security. For example "a certification of XXX means that enterprises who pass are in the top 25% of enterprises in United States, ranked by quality of cyber security.

6.1.6 Other Cyber Risk Attributes

There are very many other risk factors that insurers use in selecting their cyber insurance risks and in underwriting and pricing. They range from questionnaires and due diligence on activities, IT personnel and expenditure, security systems, technologies and network configurations, and security awareness and risk governance culture by employees and management.

We encourage companies to record these risk factors and to include them in their exposure management where appropriate. There is little consensus and considerable competitive positioning about the value of different processes of cyber risk assessment and indicators of an insured's IT infrastructure and governance and risk management practices. Where these factors emerge as common practice it may make sense to incorporate them as part of future exposure data schemas, but these are currently too disparate to incorporate as a standard for exposure management.

We believe that the proposed Cyber Exposure Data Schema incorporates the key high-level parameters important for best-practice in exposure management, balanced by practical issues of implementation and provides an important platform to expand and extend the schema in the future.

7 Feedback

Please provide any feedback on this schema design, referencing heading and page numbers, to

Jennifer Copic, Cyber Project Research Associate, Centre for Risk Studies at University of Cambridge.
email: j.copic@jbs.cam.ac.uk Tel: +44 (0) 1223 761075

Please provide your name, job title and organization, and list any colleagues who assisted and who should be credited in providing feedback.

Many thanks for taking part in the version 0.9 consultation for the development of cyber data schema.

Table 3: Mapping of Business Sectors to NAICS (2012)

V0.9 Business Sector Coding	Business Sector	NAICS (Branches Included)	Short Description
1.1	IT - Software	5112	Software Publishers
1.2	IT - Hardware	3341	Computer and Peripheral Equipment Manufacturing
1.3	IT - Services	518	Data Processing, Hosting, and Related Services
1.3	IT - Services	519130	Internet Publishing and Broadcasting and Web Search Portals
1.3	IT - Services	5415	Computer Systems Design and Related Services
2	Retail	42	Wholesale Trade
2	Retail	441	Motor Vehicle and Parts Dealers
2	Retail	442	Furniture and Home Furnishings Stores
2	Retail	443	Electronics and Appliance Stores
2	Retail	444	Building Material and Garden Equipment and Supplies Dealers
2	Retail	445	Food and Beverage Stores
2	Retail	446	Health and Personal Care Stores
2	Retail	447	Gasoline Stations
2	Retail	448	Clothing and Clothing Accessories Stores
2	Retail	451	Sporting Goods, Hobby, Musical Instrument, and Book Stores
2	Retail	452	General Merchandise Stores
2	Retail	453	Miscellaneous Store Retailers
2	Retail	454	Nonstore Retailers
3.1	Finance - Banking	521	Monetary Authorities-Central Bank
3.1	Finance - Banking	522	Credit Intermediation and Related Activities
3.2	Finance - Insurance	524	Insurance Carriers and Related Activities
3.3	Finance - Investment management	523	Securities, Commodity Contracts, and Other Financial Investments and Related Activities
3.3	Finance - Investment management	525	Funds, Trusts, and Other Financial Vehicles
4	Healthcare	62	Health Care and Social Assistance
5	Business & Professional Services	5411	Legal Services
5	Business & Professional Services	5412	Accounting, Tax Preparation, Bookkeeping, and Payroll Services
5	Business & Professional Services	5413	Architectural, Engineering, and Related Services
5	Business & Professional Services	5414	Specialized Design Services
5	Business & Professional Services	5416	Management, Scientific, and Technical Consulting Services
5	Business & Professional Services	5417	Scientific Research and Development Services
5	Business & Professional Services	5418	Advertising, Public Relations, and Related Services
5	Business & Professional Services	5419	Other Professional, Scientific, and Technical Services
5	Business & Professional Services	55	Management of Companies and Enterprises
5	Business & Professional Services	561	Administrative and Support Services
6	Energy	211	Oil and Gas Extraction
6	Energy	213111	Drilling Oil and Gas Wells
6	Energy	213112	Support Activities for Oil and Gas Operations
7	Telecommunications	517	Telecommunications
8	Utilities	22	Utilities
8	Utilities	562	Waste Management and Remediation Services
9	Tourism & Hospitality	72	Accommodation and Food Services
10	Manufacturing	313	Textile Mills
10	Manufacturing	314	Textile Product Mills
10	Manufacturing	315	Apparel Manufacturing
10	Manufacturing	316	Leather and Allied Product Manufacturing
10	Manufacturing	321	Wood Product Manufacturing
10	Manufacturing	322	Paper Manufacturing
10	Manufacturing	323	Printing and Related Support Activities
10	Manufacturing	324	Petroleum and Coal Products Manufacturing
10	Manufacturing	3251	Basic Chemical Manufacturing
10	Manufacturing	3252	Resin, Synthetic Rubber, and Artificial Synthetic Fibers and Filaments Manufacturing
10	Manufacturing	3253	Pesticide, Fertilizer, and Other Agricultural Chemical Manufacturing
10	Manufacturing	3255	Paint, Coating, and Adhesive Manufacturing

10	Manufacturing	3256	Soap, Cleaning Compound, and Toilet Preparation Manufacturing
10	Manufacturing	3259	Other Chemical Product and Preparation Manufacturing
10	Manufacturing	326	Plastics and Rubber Producs Manufacturing
10	Manufacturing	327	Nonmetallic Mineral Product Manufacturing
10	Manufacturing	331	Primary Metal Manufacturing
10	Manufacturing	332	Fabricated Metal Product Manufacturing
10	Manufacturing	333	Machinery Manufacturing
10	Manufacturing	3342	Communications Equipment Manufacturing
10	Manufacturing	3343	Audio and Video Equipment Manufacturing
10	Manufacturing	3344	Semiconductor and Other Electronic Component Manufacturing
10	Manufacturing	334510	Electromedical and Electrotherapeutic Apparatus Manufacturing
10	Manufacturing	334512	Automatic Environmental Control Manufacturing for Residential, Commercial, and Appliance Use
10	Manufacturing	334513	Instruments and Related Products Manufacturing for Measuring, Displaying, and Controlling Industrial Process Variables
10	Manufacturing	334514	Totalizing Fluid Meter and Counting Device Manufacturing
10	Manufacturing	334515	Instrument Manufacturing for Measuring and Testing Electricity and Electrical Signals
10	Manufacturing	334516	Analytical Laboratory Instrument Manufacturing
10	Manufacturing	334517	Irradiation Apparatus Manufacturing
10	Manufacturing	334519	Other Measuring and Controlling Device Manufacturing
10	Manufacturing	3346	Manufacturing and Reproducing Magnetic and Optical Media
10	Manufacturing	335	Electrical Equipment, Appliance, and Component Manufacturing
10	Manufacturing	3361	Motor Vehicle Manufacturing
10	Manufacturing	3362	Motor Vehicle Body and Trailer Manufacturing
10	Manufacturing	3363	Motor Vehicle Parts Manufacturing
10	Manufacturing	336411	Aircraft Manufacturing
10	Manufacturing	336412	Aircraft Engine and Engine Parts Manufacturing
10	Manufacturing	336413	Other Aircraft Parts and Auxiliary Equipment Manufacturing
10	Manufacturing	3365	Railroad Rolling Stock Manufacturing
10	Manufacturing	3366	Ship and Boat Building
10	Manufacturing	336991	Motorcycle, Bicycle, and Parts Manufacturing
10	Manufacturing	336999	All Other Transportation Equipment Manufacturing
10	Manufacturing	337	Furniture and Related Product Manufacturing
10	Manufacturing	339	Miscellaneous Manufacturing
11	Pharmaceuticals	3254	Pharmaceutical and Medicine Manufacturing
12	Defense / Military Contractor	334511	Search, Detection, Navigation, Guidance, Aeronautical, and Nautical System and Instrument Manufacturing
12	Defense / Military Contractor	336414	Guided Missile and Space Vehicle Manufacturing
12	Defense / Military Contractor	336415	Guided Missile and Space Vehicle Propulsion Unit and Propulsion Unit Parts Manufacturing
12	Defense / Military Contractor	336419	Other Guided Missile and Space Vehicle Parts and Auxiliary Equipment Manufacturing
12	Defense / Military Contractor	336992	Military Armored Vehicle, Tank, and Tank Component Manufacturing
12	Defense / Military Contractor	928110	National Security
13	Entertainment & Media	5111	Newspaper, Periodical, Book, and Directory Publishers
13	Entertainment & Media	512	Motion Picture and Sound Recording Industries
13	Entertainment & Media	515	Broadcasting (except Internet)
13	Entertainment & Media	519110	News Syndicates
13	Entertainment & Media	519120	Libraries and Archives
13	Entertainment & Media	519190	All Other Information Services
13	Entertainment & Media	71	Arts, Entertainment, and Recreation
14	Transportation / Aviation / Aerospace	481	Air Transportation
14	Transportation / Aviation / Aerospace	482	Rail Transportation
14	Transportation / Aviation / Aerospace	483	Water Transportation
14	Transportation / Aviation / Aerospace	484	Truck Transportation
14	Transportation / Aviation / Aerospace	485	Transit and Ground Passenger Transportation
14	Transportation / Aviation / Aerospace	486	Pipeline Transportation
14	Transportation / Aviation / Aerospace	487	Scenic and Sightseeing Transportation
14	Transportation / Aviation / Aerospace	488	Support Activities for Transportation
14	Transportation / Aviation / Aerospace	491	Postal Service
14	Transportation / Aviation / Aerospace	492	Couriers and Messengers

14	Transportation / Aviation / Aerospace	493	Warehousing and Storage
15	Public Authority / NGOs / Non-Profit	921	Executive, Legislative, and Other General Government Support
15	Public Authority / NGOs / Non-Profit	922	Justice, Public Order, and Safety Activities
15	Public Authority / NGOs / Non-Profit	923	Administration of Human Resource Programs
15	Public Authority / NGOs / Non-Profit	924	Administration of Environmental Quality Programs
15	Public Authority / NGOs / Non-Profit	925	Administration of Housing Programs, Urban Planning, and Community Development
15	Public Authority / NGOs / Non-Profit	926	Administration of Economic Programs
15	Public Authority / NGOs / Non-Profit	927	Space Research and Technology
15	Public Authority / NGOs / Non-Profit	928120	International Affairs
16	Real Estate / Property / Construction	23	Construction
16	Real Estate / Property / Construction	53	Real Estate and Rental and Leasing
17	Education	61	Educational Services
18	Mining & Primary Industries	212	Mining (except Oil and Gas)
18	Mining & Primary Industries	213113	Support Activities for Coal Mining
18	Mining & Primary Industries	213114	Support Activities for Metal Mining
18	Mining & Primary Industries	213115	Support Activities for Nonmetallic Minerals (except Fuels) Mining
19	Food & Agriculture	11	Agriculture, Forestry, Fishing and Hunting
19	Food & Agriculture	311	Food Manufacturing
19	Food & Agriculture	312	Beverage and Tobacco Product Manufacturing
20	Other	81	Other Services (except Public Administration)

8 Reference Materials: Cyber Insurance Market Practice

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.

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

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.

Lloyd's. 2015; **Lloyd's Risk Codes – Guidance and Mappings**; April 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**;

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