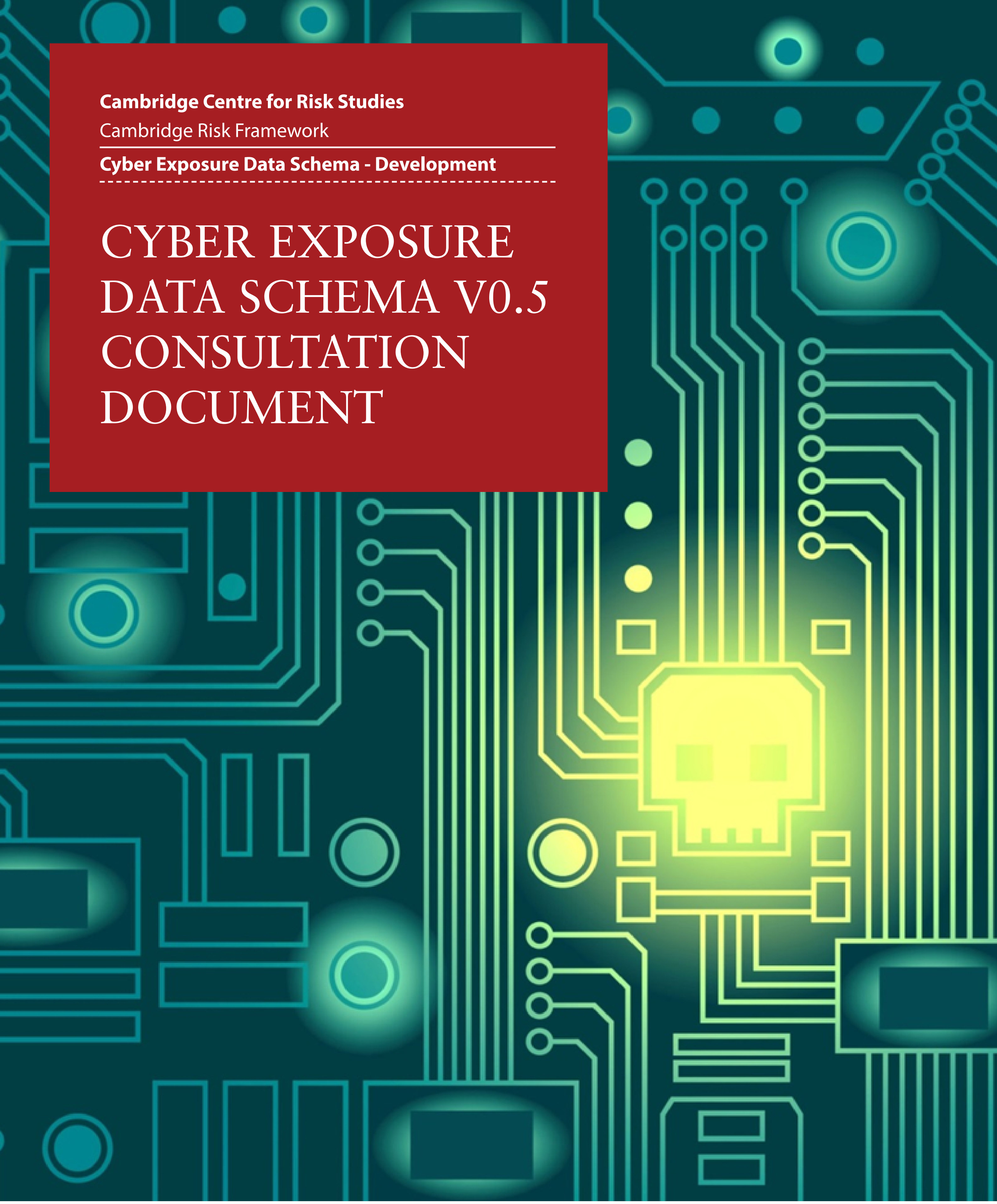

Cambridge Centre for Risk Studies

Cambridge Risk Framework

Cyber Exposure Data Schema - Development

CYBER EXPOSURE DATA SCHEMA V0.5 CONSULTATION DOCUMENT

Centre for
Risk Studies

UNIVERSITY OF
CAMBRIDGE
Judge Business School

Development of a Cyber Exposure Data Schema

Consultation Document on Proposed Exposure Data Schema (v0.5)

Context: the Need for a Standardized Cyber Exposure Data Schema

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.

We propose to develop an exposure 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 and quantifying cyber exposure

b) enable the development of models for cyber risk that will be applicable to multiple users,

c) to 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.

The schema is being developed through consultation with insurers and reinsurers who are involved in writing cyber insurance, internal insurance modelling teams and external commercial model vendors, and also with industry organizations, regulators, and providers of data and services to the insurance industry. The Schema is intended to capture the main lines of business affected, with key attributes that are relevant to accumulation management, and that will map to losses resulting from cyber scenarios.

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 syndicates 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 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 proposed to be captured 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.

We invite your comments and feedback – please add your comments in the fields indicated and return the document by 23 October 2015 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

Section 1: Principles of Schema Design

The proposed schema concept has a number of guiding principles.

Please comment on these guiding principles.

A. Accumulation Focus

This initial development (to 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 consensus from the review of cyber insurance market practice 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. A review of market practice, presented in the next section of this document, suggests that 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.

Please Comment – is exposure management the appropriate priority for a cyber data schema?

1.1 Please type your comments here

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 propose to publish an initial version of the Cyber Exposure Data Schema 1.0 in early 2016 and to do so will limit the complexity and ambition of the schema to meet this deadline.

Rationale: We propose that having a simple data standard early in 2016 will be better than waiting to refine a more complex or comprehensive data standard that will take longer to develop and release. We propose to upgrade the data standard in future as rapidly as possible, to expand the scope of the coverage and to increase the complexity. The intention is to have a schema that can capture 80% of the complexity of the problem, allowing the remaining 20% to be added over time, as the problem becomes better understood.

Please Comment – Is it better to develop an early version that may be limited in scope or would you prefer to wait until the schema can include a broader range of coverage and complexity?

1.2 Please type your comments here

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. For version 1.0 we propose to require only [seven] additional fields of cyber risk related attributes.

Please Comment –Do you agree that having the schema adopted by others is worth accepting initial simplicity in the first version? Are you comfortable with an expectation that new versions of the data schema could be developed fairly rapidly in the future, as wider adoption drives more complexity and sophistication?

1.3 Please type your comments here

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 records.

Where organizations have access only to aggregate levels of exposure data, the schema will incorporate the ability for aggregate data to contain assumptions about the cyber-specific attributes of the accounts within the aggregated exposure.

Rationale: There are two approaches to managing accumulation – aggregation into totals in n-dimensions or filtering through database queries. We propose to use an approach of ensuring that account level information is appropriately filtered, rather than maintaining an aggregate matrix. An account 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.

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.

The schema is designed assuming that each company will maintain a master database of their cyber accounts, or a copy of this database where new cyber exposure attributes can be added, where necessary.

Please Comment – is this an appropriate approach for your needs? Are there issues in your practices that would make approach difficult for you to use?

1.4 Please type your comments here

E. Exposure Management structured around Cyber Coverage Categories

The proposed approach to tracking exposure is to identify the full range of elements of coverage for cyber-induced loss that are offered in insurance policies. A loss coverage categorization 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: We have developed a categorization of cyber loss coverage (Table 4) from published expertise and a detailed review of cyber and traditional insurance products in the market. This identifies around 20 primary categories of cyber loss coverage. These categories of cover can be identified in insurance policies and used to flag up their existence in multiple accounts and quantify the amount of exposure represented by each of these separate categories of coverage. 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.

Please Comment – Does using cyber loss coverage elements make sense as an organizing principle for tracking cyber exposure? Is it practical as a way of tracking coverage across multiple lines of business?

1.5 Please type your comments here

Section 2: Cyber Insurance Market Practice Overview

This section presents an overview 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. This is the result of extensive interviews with representatives from different sectors of the cyber insurance market, including underwriters, exposure managers and analysts, primary insurers in US, 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 on the market, confidential internal documents provided under non-disclosure by a number of market participants, and an extensive review of published reports and literature, examples of which are listed in the reference section at the end.

The information on cyber insurance market practice is reviewed as a key input into the design of a Cyber Insurance Exposure Data Schema. It is important that any proposed exposure data schema fits current practice and is aligned with practical issues of implementation, and reflects the main priorities for the business user.

Likely to be a dynamic market

It is recognized that the cyber insurance market is changing rapidly, and that common practice will evolve quickly as the market develops. The future market is likely to see much more granular and detailed data become available, expansion into new markets, the development of new product coverages, and the evolution of new contractual structures, terms and conditions. A data schema that reflects today's practice will not be able to anticipate all possible future changes. Its design should be extensible and expect to be updated with new versions relatively frequently, but retain 'backward compatibility' – i.e. develop in ways that do not render previous versions obsolete.

Customizable and useful internally

It is also fully acknowledged that each company has its own set of data attributes that it monitors and uses to manage its 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.

This schema is not attempting to standardize all aspects of risk assessment or to collate proprietary information. It is focussed on exposure and accumulation management, rather than risk selection, underwriting, pricing, claims management, or operational risk management. The schema is intended to be extensible and will enable companies to add private attributes for their own internal use.

The proposed data schema is intended to start with a minimal set of practical attributes that reflect current market practice, but that can be extended and made more detailed in future versions.

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.

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 all of these areas of exposure, A to D, and proposes an approach for companies to be able to flag cyber exposures in the policies they write.

Identifying silent cyber exposures entails a review of contractual language, clarification of perils, and coverage areas provided in the policies in an insurance company’s portfolio. Many companies are currently identifying ambiguities in coverage areas and clarifying whether they have cyber exposure on a policy and if so and where possible, to move the insured to affirmative cyber cover.

Affirmative cyber coverage is likely to grow significantly as a result of exposure clarification and with the dynamic of growing demand from customers for cyber insurance. The proposed Cyber Exposure Data Schema provides a framework for identifying and quantifying these exposures at a sufficiently granular level for portfolio risk management.

Coverages provided in Affirmative Cyber Insurance

At least 35 insurers[1] are currently offering products for stand-alone affirmative cyber liability insurance. 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. The products reviewed are listed in Table 1.

The review consisted of the analysis of public materials, and in some cases non-public documentation provided by supporting insurers, and includes application forms, product brochures, coverage diagrams, policy wordings, internal and external publications, typical coverage structures and example terms and conditions, including exclusion clauses and contractual language.

Wide variation in coverage

Coverage provided by products currently on the market varies widely.

Table 2 provides a summary of the coverages offered by the sample of cyber insurance products, and how common different types of coverage are within the sample analyzed. The analysis developed a categorization of coverage by type of cyber-induced loss that the coverage will indemnify. The coverage categorization and definitions are provided in Table 4, as part of the Cyber Exposure Data Schema version 0.5 proposal.

[1] Advisen and PartnerRe (2014)

Company	Cyber Insurance Product
ACE	Dataguard Advantage
Aegis	Cyber Resilience
Aegis	Cyber Resilience+
AIG	CyberEdge
Allianz	Cyber Protect
Ascent Underwriting	CyberPro
Aspen	ARML
Aviva	Cyber Cover
Axis	PRO PrivaSure
Barbican	eRisk
Beazley	Beazley Breach Response
Brit	Global Cyber, Privacy & Technology (GCPT)
Canopius	Cyber Liability
Chubb	Cyber Security
Hartford Munich Re	CyberOne
Hiscox	E-Risks
Liberty Mutual	Liberty Mutual Data Compromise CyberOne™ Endorsements LIU Tech, Data and DataPro Insure™
JLT	Intangibles protection insurance plus (iPI+)
Markel	Privacy, data-breach and electronic risks (PDE) /ComTech
Marsh	Cyber Gap Insurance
QBE	Cyber Response
Swiss Re CRS	Cyber risk protection
Travelers	Cyber First/CyberRisk
Verisk	ISO Businessowners Program
Willis	FINEX Global Cyber Cover
XL Catlin	Cyber and Data Protection
Zurich Insurance UK	Cyber Protect

Table 1: Affirmative cyber insurance products analyzed by coverage provided, for this cyber market practice review as an input to the design of the proposed cyber exposure data schema

The coverage categorization uses and further develops a cyber loss categorization scheme published by a government and insurance industry study earlier this year[2] developed by a steering group of 15 insurance companies and several industry organizations and government agencies. This has been extended and reframed to apply to all of the loss coverage types that have been identified in the insurance products on the market. In this consultation round, you are invited to comment on this categorization structure later in the document.

There are twenty primary categories of coverage identified. Each of them can be further subdivided into component parts if required. It is fairly typical for coverage to be sub-limited 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 captured.

No standardization of product offerings

Variation in the coverage provided by the product offerings on the market is wide. There is no standard yet emerging for a cyber liability insurance 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.

[2] Marsh & UK Government (2015)

Schema v0.5 Coverage Code (Table 4)	Cyber Coverage	Number of Products Offering this Cover	% of Sample Reviewed
1	Breach of privacy event	24	92%
2	Data and software loss	21	81%
6	Incident response costs	21	81%
15	Cyber extortion	19	73%
4	Business interruption	18	69%
12	Multi-media liabilities (disparagement)	17	65%
7	Regulatory/defense coverage	16	62%
14	Reputational damage	12	46%
3	Network service failure liabilities	11	42%
5	Contingent business interruption	8	33%
10	Liability (Errors & Omissions)	7	27%
9	Liability (Professional Indeminity)	6	23%
13	Financial theft & fraud	6	23%
16	Intellectual property (IP) theft	6	23%
19	Physical asset damage	5	19%
20	Death and bodily injury	4	15%
18	Cyber terrorism	3	12%
11	Liability (Directors & Officers)	3	13%
8	Liability (General Liability)	2	8%
17	Environmental damage	1	4%

Table 2: Categories of cyber loss coverage included in the cyber insurance products reviewed, and how common each coverage type is across the market. Coverage definitions are provided in Table 4.

Most common coverage categories

The coverage types that are most common across the market are shown in Table 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. Coverage for physical damage, injury, and environmental consequence are some of the least common offered. Threats from Operational Technology (OT) are less well covered than Information Technology (IT), reflecting cyber losses that have been most prominent recently.

Per Occurrence, Annual Contract

All of the products reviewed offer coverage as a per-occurrence compensation structure, with a period of indemnity limited to one year (i.e. cyber insurance is typically written on an annual contract basis and with the exception of certain legal liability covers, the risk period expires at the end of the contractual term).

Implications for Exposure Schema Design

The young market for cyber insurance is still exploring which types of loss coverage are most in demand from its customers, as well as the costs to insurers of providing different components of risk transfer and loss indemnification. The wide variation in types of loss coverage, and the lack of current product standardization, suggests that a cyber exposure data schema should be built around the categories of coverage, rather than any one product configuration. The schema proposes that cyber loss coverage categories form the structure of cyber exposure management.

Cyber Underwriting and Risk Selection Practices

Underwriting processes appear even more disparate and varied across the industry than coverage offerings.

Our Cyber Insurance Market Practice review included underwriting and risk management practices by reviewing cyber insurance policy application forms, interviewing selected cyber underwriters, and compilation of cyber insurance underwriting market practice reviews by others[1].

A classification of factors that various writers include in their underwriting process for cyber risk includes (but not an exhaustive list):

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 & 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 & 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 & testing
- Sizing of firewalled separate data storage compartment
- Network security system software & 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 & 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

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.[2] The variety of underwriting attributes, the current lack of consensus around which are most important, the fact that these assessments are considered areas of competitive expertise, and the subjectivity of assessing many of these factors means that very few of them are applicable for standardization in an exposure schema.

The focus of the proposed Cyber Exposure Data Schema is on exposure management, and is not intended as a guide to underwriting or risk selection.

[1] For example Verisk (2014); CRO Forum (2014); Airmic (2012);

[2] Verisk (2014).

Key cyber exclusion and endorsement clauses

There a several key exclusion clauses in cyber insurance, such as NMA2914, NMA2915, CL380 and LMA3030.

- Terrorism or Malicious Attacks Exclusions
    - **CL 380** – Institute Cyber Attack Exclusion Clause
    - **LMA 3030** – Terrorism Form
- Property Damage Exclusions
    - **NMA 2912** - Information Technology Hazards Clarification Clause
    - **NMA 2914** – Electronic Data Endorsement A
    - **NMA 2915** – Electronic Data Endorsement B

Please Comment – Are there any other standard or bespoke exclusion clauses we should identify or flag in a Cyber Exposure Data Standard? Are there any standard cyber endorsements for general liability or other policies? Which of these exclusions or endorsements do you commonly use?

2.1 Please type your comments here

Business Sectors of Most Importance

Insurers and cyber market analysts commonly segment the market of cyber insurance purchasers by business sectors, such as retail, financial services, technology etc. Business sector segmentation is important both for market development and for risk characteristics of companies in those sectors. There is little consensus around the structuring of this segmentation: a number of companies have developed their sectorization as an ad-hoc process, although many companies seem to use categories with similar names and sub-divisions. Market analysts broadly report around these sectoral divisions.

The business sectors of the market are important to insurers not only for monitoring business development, through metrics such as premium income, they also represent important profitability sectors, by monitoring claims frequencies and loss ratios. Some companies have also developed specialist domain expertise in writing cyber insurance that is concentrated in certain business sectors. Monitoring exposure accumulations for a standardized set of primary business sectors is an objective of the Cyber Exposure data Schema.

Our review of market practice suggests that few companies adhere strictly to any of the accepted coding systems used in economic or industry sectorization, such as SIC codings, NAICS, GICS, although some elements of these are commonly incorporated. Most companies impose their own higher order groupings that encompass these codings. In property insurance it is common to record occupancy types or usage categories for the commercial customer’s business activities, so fairly complex coding structures have been developed for commercial activities related to building usage. Company practices appear to vary widely in the granularity of their business sectorization, with some maintaining as few as three or four primary categories and others maintaining schedules of many hundreds of activity codings.

Table 6 proposes a high-level business sector classification that incorporates most of the terminology and classes that have been encountered, and that encompasses the main activity sectors in the economy and the categorization used in statistical reporting. In this consultation round, you are invited to comment on this sector classification structure later in the document.

Table 3 shows the estimated ranking of these sectors, in five approximate tiers of interest by importance of that sector for the cyber insurance market, derived from published market analysis reports and inputs from cyber insurance practitioners.

V0.5 Business Sector Coding	Business Sector	Tier by interest
1	Information Technology	Tier 1
2	Retail	Tier 1
3	Financial Services	Tier 1
4	Healthcare	Tier 2
5	Business & Professional Services	Tier 2
6	Energy	Tier 2
7	Telecommunications	Tier 2
8	Utilities	Tier 2
9	Tourism & Hospitality	Tier 3
10	Manufacturing	Tier 3
11	Pharmaceuticals	Tier 3
12	Defense / Military Contractor	Tier 3
13	Entertainment & Media	Tier 3
14	Transportation/Aviation/Aerospace	Tier 4
15	Public Authority; NGOs; Non-Profit	Tier 4
16	Real Estate, Property & Construction	Tier 4
17	Education	Tier 4
18	Mining & Primary Industries	Tier 5
19	Food & Agriculture	Tier 5
20	Other	Tier 5

Table 3: Business sectors of interest to the cyber insurance market, ranked by tiers of interest.

Size of Enterprise

A further segmentation of the market of interest to cyber insurers is the size of company. Much of the early market was developed by providing coverage to large corporations. There is increasing reported interest in mid-size companies, and from a growing small to medium enterprise (SME) sector.

Size of company by number of employees is also a risk factor that has been observed in cyber claims analysis, and insurers are increasingly capturing this data parameter about their insureds. Several companies have adopted the US Census Bureau classification of ‘Large’ being more than 500; ‘Medium’ meaning 100 to 499; ‘Small’ being 20 to 99 employees.[1]

Managing exposure information by size of enterprise may be important for many insurers, so it is proposed to capture number of employees as an exposure management attribute in the schema.

Geographical Markets of Most Importance

The very large majority of insurance premium for cyber coverage today is for the United States market. Insurance market surveys suggest that cyber insurance take-up is growing rapidly in many other countries.[2]Cyber exposure is not geographically constrained in the way that many other insured perils are, and some cyber threats can be expected to cause losses to exposure in multiple geographical markets. Different countries have quite different jurisdictions that determine payouts, in legal liability consequences and regulatory compensation requirements so geography is still significant. In United States, compensation and regulatory implications for cyber exposure still vary significantly by state, so state-level geography of insureds is relevant for exposure assessment, if practical.

The proposed cyber exposure data schema proposes to capture the geography of exposure by country, and in the United States by state. Higher resolution geographical location is not significant for cyber exposure.

Markets thought to be significant for cyber insurance for the next three years include the following:

[1] Caruso (2015)

[2] Thomas and Finkle (2014)

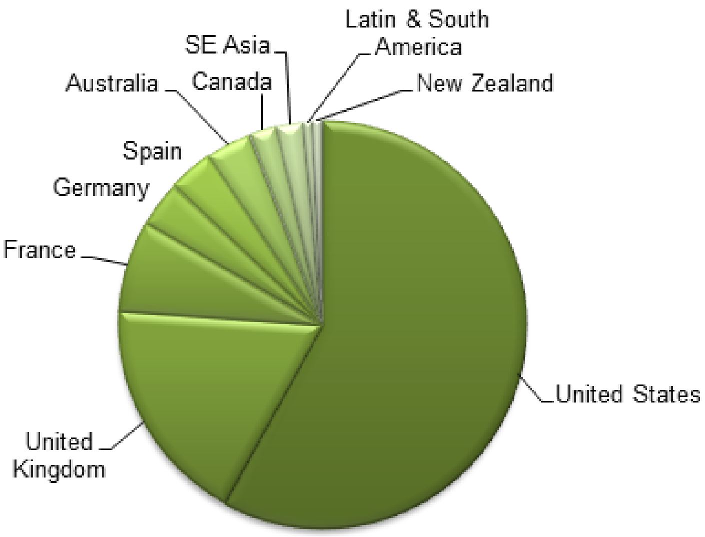

Figure 1: Geographical markets of most interest for cyber exposure management for the next three years.

Other markets mentioned as being potentially growth areas in the next few years include India, Switzerland and Singapore, with the European Union expected to become a significant market across its member countries with the impending EU directive on cyber security.

Insurance Information Management Systems in Use

Insurers manage their exposure data using a wide variety of different information management systems across the industry, including systems provided by a range of third party vendors and those developed in-house. Insurers have typically adapted third party systems or built their own proprietary system to manage their exposure data monitoring and reporting. Different heads of cover and lines of business are sometimes managed using separate systems internally. Property exposure is typically more rigorously managed in detail than casualty and liability exposure.

Coding systems vary widely and there is little commonality between different insurers in the categories and codes used, except where regulators require explicit reports.

Cyber exposure is typically managed today as an extension of one or more of the internal systems, with ad-hoc codings and classifications added, and in some cases the adaptation of non-cyber data structures and coding systems to approximate to the needs of cyber exposure tracking.

Underwriting systems separate from exposure systems

It is common practice for insurers to manage their exposure data separately from their underwriting information. Much of the attribute information that might have been captured at the underwriting stage is not easily accessed in the exposure system.

Insurance companies are currently managing cyber exposure using a variety of different systems and approaches. Some companies have multiple systems for the different areas of their business that could potential contain cyber exposure. The exercise of consolidating cyber exposure management represents a significant challenge for many companies.

Resource considerations in schema design

The Cyber Exposure Data Schema will need to be implemented by exposure management teams initially adding coding attributes to existing data. This is likely to be a painstaking process, possibly involving account by account tracking and analysis. Once the system is established and structured, then the additional data requirements can be captured at the point of entering new accounts into the system. The resource effort required to implement the proposed schema is an important constraint, and each new data item proposed will add significantly to the resource effort required. Keeping the schema as simple as possible is an important principle in limiting the resource effort needed for implementation.

The proposed Cyber Exposure Data Schema needs to be compatible with a wide range of different processes and industry practices. The proposed schema is intended to add the minimum amount of additional attribute information to enable insurers to implement the schema using their various existing systems as practically as possible.

Please Comment – Does this market practice overview align with your own view of the cyber insurance market? Are there important factors in your view of market practice that you feel should be taken into account in the design of a Cyber Exposure Data Schema?

2.2 Please type your comments here

Section 3: Cyber Exposure Data Schema v0.5

We are interested in your feedback to help prioritize which potential cyber exposure attributes should be added to account information in the proposed cyber exposure data schema.

Your feedback will be incorporated into a revision of this proposal, to be published as Cyber Exposure Data Schema version 1.0.

From the insurance cyber market practice review, a minimal set of exposure information that is typically already captured in an insurance company's existing account management systems includes:

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.

The proposed Cyber Exposure Data Schema will provide 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 five classes of exposure attributes are consistently captured with high-level information:

1. Geographical Jurisdiction
2. Cyber Loss Coverage Categories
3. Business Sector
4. Size of Enterprise
5. Cyber Risk Attributes

1. Geographical Jurisdiction

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

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

Please Comment – is this the appropriate level of resolution for a common schema? Are there issues in applying this in practice or appending this information to existing accounts if they don't already have it?

3.1 Please type your comments here

2. Cyber Loss Coverage Categories

To identify cyber exposure it is necessary to identify the loss coverage categories that the product and insurance coverage provides. Table 4 provides a proposed high level categorization of cyber loss coverage categories. In the cyber insurance market practice review, described in Section 1 of this document, these coverage categories were matched to each loss type being indemnified across affirmative provision of cyber insurance and explored for where silent exposure may exist in some parts of traditional insurance lines.

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 if applicable.

Potential for further granularity in coverage categories

The loss coverage categories listed in Table 4 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 version 1.0 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.

Coding IDs to be added

The identifying code numbering of these categories, or their ordering, is a draft placeholder in this version 0.5 document and is not significant for the schema. Unique coding values may be applied to the categories once a final listing has been defined and agreed.

Please provide your comments on the cyber loss coverage categorization, below Table 4.

v0.5 Code	Cyber Loss Coverage – Primary Category	Description
1	Breach of privacy event	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, and other costs from complying with mandatory data breach notification regulations.
2	Data and software loss	The cost of reconstituting data or software that have been deleted or corrupted.
3	Network service failure liabilities	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	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 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	Direct costs incurred to investigate and close the incident to minimise post-incident losses. Applies to all the other categories/events.
7	Regulatory and defense coverage	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, defense 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 (General Commercial)	Coverage from third party law suits arising from both malicious cyber attacks and accidental IT failures. The insurance carrier assumes the defense of the insured and pays legal costs as well as settlement terms. The coverage may include personal liabilities, product liabilities, or other tort claims.
9	Liability (Professional Indemnity)	Cover for the legal costs and expenses of allegations of providing inadequate advice, services, or designs or products as a result of a cyber attack or IT failure. PI cover may also include medical malpractice. This may also include Technology and Contractor Liability Cover.
10	Liability (Errors & Omissions)	Errors and Omissions are a specific type of Professional Liability cover typically designed to cover financial losses rather than liability for personal injury, and covers judgements, settlements and defense costs.
11	Liability (Directors & Officers)	Costs of compensation claims made against the individual officers of the business, 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)	Cost for investigation, defence cost and civil damages arising from defamation, libel, slander, copyright / trademark infringement, privacy violation, negligence in publication of any content in electronic or print media, as well as infringement of the intellectual property of a third party

v0.5 Code	Cyber Loss Coverage – Primary Category	Description
13	Financial theft & fraud	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	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	The cost of expert handling for an extortion incident, combined with the amount of the ransom payment.
16	Intellectual property (IP) theft	Loss of value of an IP asset, expressed in terms of loss of venue as a result of reduced market share.
17	Environmental damage	Cover for costs of clean up, recovery and liabilities associated with a cyber induced environmental spill or release.
18	Cyber terrorism	Cyber attack attributed to cyber terrorists or where government agencies have deemed the attack an act of terrorism.
19	Physical asset damage	First-party loss due to the destruction of physical property resulting from cyber attacks.
20	Death and bodily injury	Third-party liability for death and bodily injuries resulting from cyber attacks.

Table 4: Proposed categorization of cyber loss coverage - primary categories

Please comment on this proposed structuring of cyber loss coverage. Are there any issues in structuring the Cyber Exposure Data Schema by these primary coverage categories? Are there any important categories that are missing? Are 20 categories too many (or too few)? Should some of these categories be collapsed into higher order groupings? Should any of these categories be expanded into sub-categories? Would you propose any changes to the definitions or descriptions of these categories?

3.2 Please type your comments here

3. Business Sector

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

Table 6 proposes a high-level business sector classification that incorporates most of the terminology and classes that have been encountered in the insurance market practice review and that also encompasses all the main activity sectors in the economy and segmentation used in statistical reporting and analysis.

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. Examples of the five leading coding systems (SIC, NAICS, GICS, ISIC, and NACE) used in different regions of the world are shown in Table 5. In addition to variation between coding systems, there is also significant variation in versions and vintages of different editions of each coding system. These economic classification systems have been mainly developed for economic census and analysis, rather than for insurance applications. There is no consensus in which system and version is most widely adopted and there are many different sectoral coding systems currently in use across the insurance industry.

Translation between coding systems

Instead of attempting to standardize a single economic coding system across the insurance industry we propose to define the categories that best align with insurance usage, common terminology and practice, and then develop a concordance – i.e. a translation table that companies can use to align their preferred sector coding practice with these high level business sector categories. Table 5 illustrates how concordance coding can translate categories between different coding systems.

Data Schema		Example coding	Notes
Cyber Exposure Data Schema v0.5		Health Care	
Global Industry Classification Standard	GICS	Health Care	High level: 10 sectors, 24 industry groups, 67 industries, 156 sub-industries (S&P categorized for each major public company)
Standard Industrial Classification	SIC	8000 Services - Health Services	Four digit hierarchical system - 450 categories
North American Industry Classification System	NAICS	62 - Health Care and Social Assistance	Two to six-digit coding o increasing resolution. Latest revision 2012
International Standard Industrial Classification	ISIC	Q - Human Health and Social Work Activities	United Nations system for classifying economic data. Latest revision (4) 2008
Statistical Classification of Economic Activities in the European Community	NACE	Q - Human Health and Social Work Activities	Four level hierarchy; level 1 has 21 sections, level 4 has 615 classes (4-digit code)

Table 5: Different systems available for use in classifying business and industrial sectors in the economy, and an example of a concordance for how to translate the coding of one system into another.

The classification of business sectors for version 0.5 proposes 20 categories for use in cyber insurance exposure monitoring and accumulation management. We are interested in feedback on the number of categories that can provide a practical level of segmentation without being too onerous and on which sectors should be represented in more detail or aggregated into fewer categories.

Please provide your comments on the categorization of cyber insurance business sectors, below Table 6.

v0.5 Code	Business Sector	Description	Example NAICS codes (not exhaustive)	Tier of interest
1	**Information Technology**	Technology sector, including IT hardware providers, computer software vendors, internet service providers, social network companies, and security services	51 Information Industries; 541 Computer systems design services	Tier 1
2	**Retail**	Retailers to general public, sellers of goods and services both in retail stores and online,	52-59 Retail Trade; 50-51 Wholesale Trade	Tier 1
3	**Financial Services**	Financial services including insurance, payment processing and investment management	60-67 Finance, Insurance	Tier 1
4	**Healthcare**	Companies providing provides goods and services to treat patients with curative, preventive, rehabilitative, and palliative care.	62 Health Care and Social Assistance	Tier 2
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.	70-89 Services	Tier 2
6	**Energy**	Companies involved in the exploration, extraction and development of oil or gas reserves, oil and gas drilling, or integrated power firms.	211 Petroleum & Natural Gas extraction;	Tier 2
7	**Telecommunications**	Companies facilitating exchange of information over significant distances by electronic means.	517 Wired telecommunications Carriers; 5172; Wireless Telecomms Carriers	Tier 2
8	**Utilities**	The utilities sector contains companies such as electric, gas and water firms and integrated providers	926 Provision of Electric, Gas and Other Utilities	Tier 2
9	**Tourism & Hospitality**	Companies providing services for tourism, travel, accommodation, catering and hospitality	721 Hotels and motels; 722 Restaurants	Tier 3
10	**Manufacturing**	Companies making or process goods, especially in large quantities and by means of industrial machines	20-39 Manufacturing	Tier 3
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.	424 Pharmaceuticals Drugs merchants	Tier 3
12	**Defense / Military Contractor**	Defense industry comprises government and commercial industry involved in research, development, production, and service of military materiel, equipment and facilities	928 National Security	Tier 3

v0.5 Code	Business Sector	Description	Example NAICS codes (not exhaustive)	Tier of interest
13	**Entertainment & Media**	Enterprises involved in providing news, information, and entertainment: radio, television, films, theater	71 Arts, Entertainment and Recreation	Tier 3
14	**Transportation/Aviation/ Aerospace**	Companies facilitating the transportation of goods or customers. The transportation sector is made up of airlines, railroads and trucking companies.	40-49 Transportation	Tier 4
15	**Public Authority; NGOs; Non-Profit**	National or local government agencies, non-governmental and non-profit organizations	91-99 Public Administration	Tier 4
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	60-67 Real Estate; 15-17 Construction;	Tier 4
17	**Education**	Colleges and universities, independent and unified school districts, student loans and tuition companies	6113 Colleges, Universities and Professional Schools; 611 Educational Support Services	Tier 4
18	**Mining & Primary Industries**	Companies involved in the mining, quarrying, and processing of extracting minerals, coal, ores, main commodities, and natural resources.	10-14 Mining	Tier 5
19	**Food & Agriculture**	Those involved in the food industry, including production, processing, distribution, and wholesale supply	311 Food Manufacture & Processing; 01-09 Agriculture	Tier 5
20	**Other**			Tier 5

Table 6: Proposed classification of business sectors for use in Cyber Exposure Data Schema

Please comment on this proposed classification of business sectors for use in the Cyber Exposure Data Schema.

Are 20 categories too many (or too few)? Should some of these categories be expanded into more granular sub-categories? Should some be collapsed into higher order groupings? Which industry categorization scheme (SIC, NAICS, GICS etc.) and version is used most by your company and which do you think is most appropriate for use in this context?

3.3 Please type your comments here

4. Size of Enterprise

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.

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 datasets.

Please Comment – Are there issues in appending this information to existing accounts if you don’t already track this? Is number of employees preferred to other metrics of company size, such as revenue?

3.5 Please type your comments here

5. 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 will capture a manageable number of cyber risk attributes to explore potential loss from a number of the key cyber coverage categories.

5.1 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.

Please Comment – How important is it to capture the cyber risk attribute of number of confidential records held by an insured? How practical is it to expect that this will be commonly recorded in exposure systems?

3.5 Please type your comments here

5.2 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

Please Comment – How important is it to monitor potential for correlated loss of this type in cyber exposure management? How practical is it for this information to be collected and monitored in exposure systems?

3.6 Please type your comments here

5.3 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.

- Provide the value of the average monthly fee paid to the enterprise's top **named cloud service provider(s)** (up to three largest providers)

Please Comment – How important is it to monitor potential for correlated loss of this type in cyber exposure management? How practical is it for this information to be collected and monitored in exposure systems?

Please make your suggestions here

5.4 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)

Please Comment – How important is it to monitor potential for correlated loss of this type in cyber exposure management? How practical is it to expect that this information could be commonly collected and monitored in exposure systems?

3.8 Please type your comments here

5.5 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 cyber security practices, IT personnel and expenditure, security systems, technologies and network configurations, and security awareness and risk governance culture by employees and management.

As agreed in the initial consultation round, the focus of the Exposure Data Schema is on accumulation management, rather than underwriting, risk selection, or pricing.

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.

Please Comment – Do you have general comments on the schema? Are there other elements or cyber risk attributes that are essential to include in a Cyber Exposure Data Schema v1.0?

3.9 Please type your comments here

Thanks and Accreditation

Many thanks for taking part in the version 0.5 consultation for the development of cyber data schema.

We will credit the individuals and organizations who have assisted in the development of the schema in the final publication. If you are comfortable with being credited, please provide your name, job title and organization, and list any colleagues who assisted and who should be credited.

Please list the names, job titles, and organization of people who helped with responses to this consultation.

Reading Recommendations

The following features the project's reference materials. **Please Comment** – Do you have any suggestions of additional supplementary reading relating to the cyber insurance market practice, particularly with regard to underwriting practices, exposure managment and casualty/liability insurance issues.

Please make your suggestions here

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.
- 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.