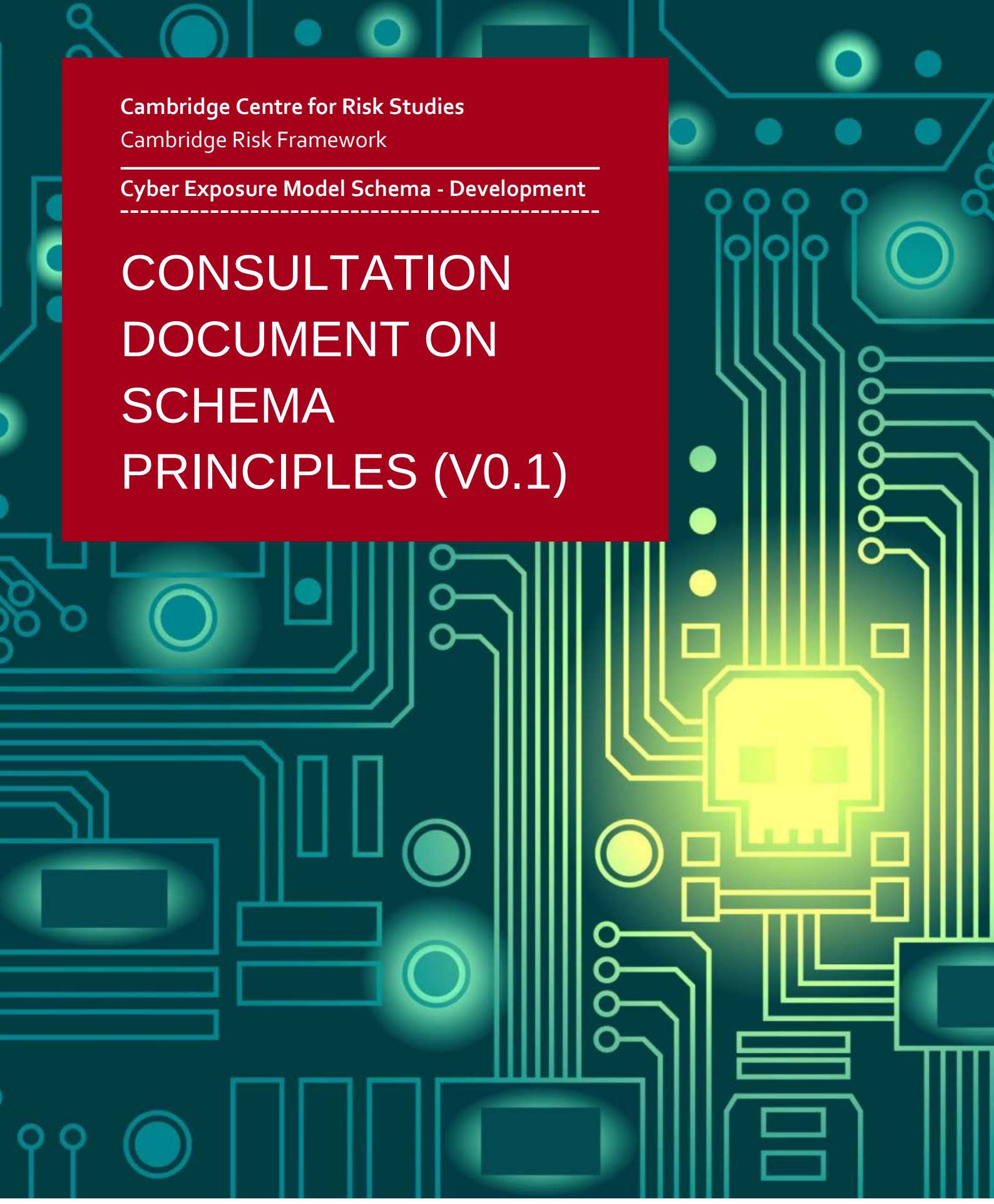

Cambridge Centre for Risk Studies

Cambridge Risk Framework

Cyber Exposure Model Schema - Development

CONSULTATION DOCUMENT ON SCHEMA PRINCIPLES (V0.1)

Centre for **Risk Studies**

UNIVERSITY OF CAMBRIDGE
Judge Business School

Development of a Cyber Exposure Data Schema

Consultation Document on Schema Assumptions (v0.1)

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) enable models to be developed for cyber risk that will be applicable to multiple users,

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

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

The schema is being developed initially through consultation with a small number of development clients and in subsequent stages, where necessary, may be expanded to broader industry review. It 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, and intended to facilitate analysis broadly, to 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.

A database of cyber insurance exposure that conforms to the schema will be capable of estimating losses from event scenarios or other types of risk models to the exposure recorded in the database. Exposure needs 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.

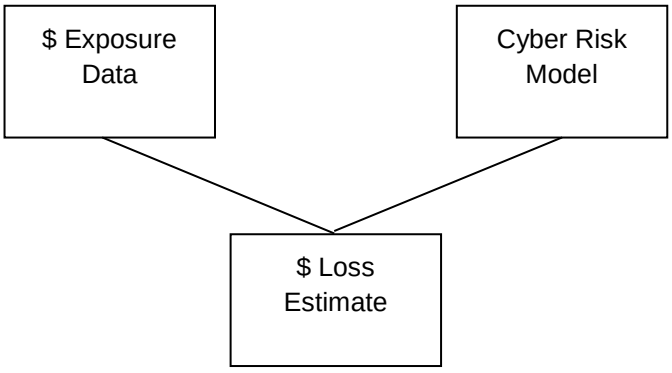

Figure 1 Basic Approach to Insurance Company's Loss Estimation using Exposure Data Structure in Conjunction with Risk Centre Stress Test Scenario

Assumptions

We ask our development clients to each provide their feedback on the following key assumptions, either to endorse the principle, refute it, or to qualify it.

1. 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 and pricing decisions.

Rationale: Our review of the market practice 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 would not be 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 this the appropriate focus for your needs?

1.1 Type your comments here

2. Account Level

We propose that the approach will be to as much as possible use ***existing policy and account management database records***, filtered on the appropriate attributes (fields) to determine which accounts that are impacted by a scenario.

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 (even if, initially, the modelling is equally as coarse as an aggregate loss model). We expect each company to maintain a master database of their accounts that new attributes can be added to, 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?

1.2 Type your comments here

3. Simple as Possible

An important principle is to make the data schema as simple as possible. The emphasis will be on keeping it stable, backwardly compatible, and expanding and developing it further over time. We believe that having a simple version available quickly will be more successful than spending longer to develop a more sophisticated data structure.

Rationale: Keeping the cyber exposure data schema version 1.0 simple will maximise adoption, which is an important objective of developing the EDM. 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 proposed to limit the number of additional cyber risk related attributes that might be required to be added to a company's policy database to five.

Please Comment – is this approach adequate your needs? 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 Type your comments here

4. Adopting a Categorization of Cyber-Induced Losses

We propose to adopt and extend an insurance industry-derived categorization of cyber-induced loss[1] as a framework for primary coverage classification, but extending this further where necessary. This high-level loss structure is described in table 1, below.

Rationale: We propose to build on the existing published expertise from the March 2015 report in categorizing cyber-induced loss, developed by a steering group of 15 insurance companies and several industry organizations and government agencies. Our review of this – see table 1 below - suggests that this is broadly compatible with the coverages and loss types being addressed in the schema, but we may need to extend and improve granularity of the scheme, particularly for cyber liability-related loss coverages, and this will be developed in detail in our iterations of the data schema towards version 0.5 and 1.0. We believe it provides an authoritative framework from which to build.

Please Comment – is the loss categorization approach proposed in Table 1, below, appropriate and adequate? If we used the structure are there missing categories or any additional comments you could provide on the proposed structure? In addition please add to Table 1 your own estimate of how important these individual loss categories are to your business.

1.4 Type your comments here

5. Prioritization of Affirmative Cyber 'Breach' Products

In developing the cyber data schema our long term ambition is to cover both affirmative cyber products and also silent cyber exposure. We recognize that categorizing all of the lines of silent cyber exposure in a comprehensive structure, within our proposed timeline may be a challenge. We propose to prioritize the development of affirmative cyber.

Rationale: It is important to get an agreed cyber data schema out and in use within the target timescale (i.e. early 2016) to maximize industry adoption. We recognize that the lines of insurance business that might potentially represent silent cyber exposure could be extensive and complex to develop exposure data structures for. It may be preferable to focus on affirmative cyber cover to enable the publication date to be met. It may be possible to include some of the principle lines of insurance business that represent significant silent cyber exposure in the initial release but we propose to prioritize the development of the affirmative cyber exposure and add what other lines can be managed with the resources in the time available.

Please Comment – is this prioritization acceptable? How important is silent cyber coverage to you as an accumulation issue? Is it better to develop an early version that can be useable or would you prefer to wait until the EDM can cover all lines?

1.5 Type your comments here

6. Event Based Cover

The data structure will be focused around identifying accumulations that could be impacted by cyber 'events', and paid out as a per-occurrence compensation structure. We are assuming the period of indemnity is limited

[1] Marsh & UK Government (2015) ***UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk*** https://www.gov.uk/government/publications/uk-cyber-security-the-role-of-insurance

to one year in cyber (i.e. that 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).

Rationale: There may be coverages that are aggregate loss covers or risk share agreements that are not concerned with individual events, but pay out on cumulative loss payouts. The exposure data model will need to cover and help identify the burning costs of sectors and groups of insureds that experience higher-than-average claims patterns, but the main principle use of exposure tracking will be for extreme events or claims that could cause correlated accumulations of risk.

Please Comment – is a per-occurrence type of coverage approach appropriate and adequate for your needs? If the schema incorporates an assumption that cyber is a one year coverage what exceptions might it miss? – please comment.

1.6 Type your comments here

	Loss Category	Marsh (2015) code	Marsh (2015) Definition	Typical Cover(s)	Comments from the Cambridge/RMS team on interpretation and potential adaptation for use in the data schema	Please add your prioritization (1= most important) or other comments
1	**Breach of privacy event**	F	The cost to investigate and respond to a privacy breach event, including IT forensics and notifying affected data subjects. Third-party liability claims arising from the same incident. Fines from regulators and industry associations.	-Data Liability/Data Breach -Data Breach Response Services -General liability	Cost to investigate and respond should be covered under K (How is this different?) F should be costs of notification and compensation to record-holders and regulatory fines (Maybe three different sub-types of costs, F1 is notification costs; F2 is compensation costs; F3 is fines?	
2	**Data and software loss**	C	The cost to reconstitute data or software that has been deleted or corrupted.	-Data Asset Restoration -Data Recovery	We may need or choose to subdivide into different categories of data loss, perhaps C1 = Personal Data Records; C2 = Other/Commercial Data; C3 = Software loss; And even subdivide the Personal Data Records into C1.1 = Personally Identifiable Information (PII); C1.2 = Payment Card Information (PCI); C1.3 = Protected Health Information (PHI) etc.	
3	**Incident investigation & response costs**	K	Direct costs incurred to investigate and "close" the incident and minimize post-incident losses. Applies to all the other categories/events. e.g. forensics and notifying affected subjects.	-Incident response costs -Technical Forensics	Would be interested to know how this is handled under coverages, how it is measured and compensated	
4	**Liabilities**	G	Third-party liabilities arising from certain security events occurring within the organization's IT network or passing through it in order to attack a third party. [In Marsh Report this category is titled 'Network failure liabilities'.	-Network security -Errors and Emissions -Professional Indemnity	Propose to make this the main category for all legal liability (i.e. 'Casualty') payouts resulting from cyber. May need different sub-types e.g. G1 = General Liability; G2 = Directors and Officers; G3 = Errors and Omissions coverage; G4 = Professional Liability; G5 = Medical Professional etc.	
5	**Financial Theft**	E	The direct financial loss suffered by an organization arising from the use of computers to commit fraud or theft of money, securities, or other property.			
6	**Business interruption**	B	Lost profits or extra expenses incurred due to the unavailability of IT systems or data as a result of cyber attacks or other non-malicious IT failures.	-Business Interruption -Contingent Business Interruption		
7	**Cyber extortion**	D	The cost of expert handling for an extortion incident, combined with the amount of the ransom payment.	Cyber Extortion	Sub-types? D1 = Cost of hiring experts; D2 = Ransom payment?	
8	**Intellectual property (IP) theft**	A	Loss of value of an IP asset, expressed in terms of loss of revenue as a result of reduced market share.		Is this a common coverage? How is the indemnification compensated?	
9	**Impact on reputation**	H	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.	-Reputation -Crisis Management	Would be interested to know how this is handled under coverages, how it is measured and compensated	
10	**Physical asset damage**	I	First-party loss due to the destruction of physical property resulting from cyber attacks.	-Traditional property cover (silent or with endorsements) -Stand alone cyber property cover General liability	Would be interested to know how this is handled under coverages, how it is measured and compensated	
11	**Death and bodily injury**	J	Third-party liability for death and bodily injuries resulting from cyber attacks.	-General liability	Would be interested to know how this is handled under coverages, how it is measured and compensated	

Table 1: Cyber loss categories, After: Marsh & UK Government, March 2015, UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk https://www.gov.uk/government/publications/uk-cyber-security-the-role-of-insurance

1.7 Add comments and prioritization in the right hand column. Please add any other comments on table 1 here

Section 2: Cyber Insurance Market Practice Review

We are currently compiling a review of cyber insurance market practice – current activities and common products and processes in the offerings of cyber insurance, and the exposures and business priorities of companies that write cyber insurance. This will be used to structure the exposure data schema and prioritize the attributes likely to provide most commonality.

We are not requesting any information that is proprietary or confidential and all information provided will be treated in confidence. No information that is provided for this study will be made available to others and will not be individually identifiable in any report output we produce.

Market Practice Review Request

If you haven't yet provided information for our market practice review, we would appreciate any examples you can provide (from your own business or others in the market) of the following.

- Cyber insurance products that companies are currently offering or participating in, cyber-related endorsements or extensions on policies in other insurance lines of business, and insurance coverages in other lines of business that could be impacted by future cyber-related events, even if these are 'silent' on whether cyber is covered or not. Where possible we would like to relate their coverage categories to those in Table 1.
- Cyber insurance product policy application forms in use, which list questions for underwriting consideration.
- Policy forms, typical coverage structures, retentions and limit examples, sub-limit structures and options, language, terms and conditions, exclusion language and contractual structures.
- Publications, documents or internal reports that summarize the cyber insurance market, current practices, or guidelines.

Are you able to provide any information or examples of these? Please list examples you can provide and send with this report or separately to Rob Savage.

2.1 Please list examples of Cyber Insurance Market Practice Review exhibits you are able to provide:

Insurance Information Management Systems in Use

To design the cyber exposure data schema we need to understand how companies are currently tracking and managing insurance exposure data across a number of classes of business, and how cyber policies are currently being captured.

We would like to get a better understanding of

- The systems that you use for recording exposure from insurance policies written across multiple classes of insurance business, the types of databases used and the vendors and product names and versions of any commercial software systems being used to manage policies that might be impacted by cyber exposure management.
- Is it possible to add attributes (fields) to these systems to identify cyber risk?

Please provide a brief description of the in-house systems you use to track exposure data, and their extensibility for cyber. If different systems are used for different classes of business, please identify each one.

2.2 Please provide a brief description of the in-house systems used to track exposure data, and how practical it would be to add additional fields or code values.

Markets of Most Importance

Please provide a high-level overview of the major geographical markets and lines of business that are of interest. We are not asking for confidential data or detailed $$ premium income or exposure values, but would appreciate some kind of relative ranking or % split of activity in different areas so that we can see what is material to your business.

	For Affirmative Cyber Insurance	For Other Non-Cyber Insurance Lines
North America		
United States		
Canada		
Latin and Central America		
Name specific important countries?		
Europe		
United Kingdom		
Germany		
France		
Spain		
Other (Name specific important countries?)		
SE Asia		
Japan		
China		
S Korea		
Taiwan		
Other (Name specific important countries?)		
Rest of Asia		
Name specific important countries?		
Australasia		
Australia		
New Zealand		
Middle East		
Name specific important countries?		
Rest of World		
Name specific important countries?		

Table 2 Relative ranking of markets where cyber and other lines of business are currently important to you, or you expect them to be in the near future.

2.3 Please provide a relative ranking of the importance of these geographical markets to your business. Please provide any other comments

Business Sectors of Most Importance

Please provide a high-level overview of the major business sectors, economic or commercial activity groups, or 'occupancy' types that are of most importance to you.

We are not asking for confidential data or detailed $$ premium income or exposure values, but would appreciate some kind of relative ranking or % split of activity in different sectors so that we can see which are most material to your business in prioritizing our efforts.

If you use a different categorization of business activity or sectors, please identify this, and if there are categories of importance or sub-categories that are of major significance to your business, please call these out.

	Business Sector	For Affirmative Cyber Insurance	For other non-cyber insurance lines
1	Mining & Primary Industries		
2	Energy		
3	Transportation/Aviation/Aerospace		
4	Manufacturing		
5	Utilities		
6	Technology & Telecoms		
8	Financial Services		
9	Professional Services		
10	Retail		
11	Healthcare		
12	Pharmaceuticals		
13	Property		
14	Education		
15	Entertainment		
16	Tourism & Hospitality		
17	Food & Agriculture		
18	Public Authority; NGOs		
19	Defense / Military Contractor		
20	Other		

Table 3 Relative ranking of business sectors where cyber and other lines of business are currently important to you, or you expect them to be in the near future.

2.3 Please provide a relative ranking of the importance of these business sectors to your business. Please provide any other comments.

2.4 Please identify what method you use for tracking or categorizing business or economic activity sectors in your business (e.g. SIC code, NAICS code, GICS coding or other system)

Lines of Non-Cyber Insurance Business of Most Importance

Please provide a high-level overview of the lines of business other than cyber that your company writes or is most heavily involved in. This is intended to help prioritize the categories of potential silent cyber exposure that the data schema may need to cover.

We are not asking for confidential data or detailed $$ premium income or exposure values, but would appreciate some kind of relative ranking or % split of activity in different lines so that we can see which are most material to your business in prioritizing our efforts.

If you use a different categorization, grouping, or naming of lines and classes of business, please provide your version. If there any classes of business that have been missed or are of major significance to your business, please call these out.

Property	
	Personal Lines/Homeowner
	Personal Contents
	Commercial Property
	Construction & Engineering
	Commercial Facultative
Casualty	
	Workers Compensation
	Directors & Officers
	Financial Lines
	General Liability
	Healthcare Liability
	Professional Liability
	Product Liability
	Product Recall
Auto	
	Personal Lines
	Commercial & Fleet
Marine & Specie	
	Cargo
	Marine Hull
	Marine Liability
	Specie
Aerospace	
	Airline
	Airport
	Aviation Hull & Cargo
	Other Aviation
	Space
Energy	
	Downstream
	Energy Liability
	Onshore Energy & Power
	Upstream

Specialty	
	Accident & Health
	Aquaculture insurance
	Contingency - film & event
	Equine insurance
	Excess & Surplus
	Life Insurance
	Livestock
Life & Health	
	Individual Life Insurance
	Group Life Insurance
	Health Insurance
	Income Protection
	Death & Disability
	Hospital Cover
Pension and Annuities	
	Standard Annuities
	Variable Annuities
	Enhanced Annuities
	Life Settlements
War & Political Risk	
	Kidnap & Ransom
	Political Risk
	Political Violence & Terrorism
	Trade Credit
Agriculture	
	Multi-peril crop
	Crop hail
	Livestock
	Forestry
	Agriculture
Other (Please specify)	

Table 4 Identification of which lines of insurance business your company writes or is most heavily involved in, currently or you expect to be in the near future.

2.5 Please provide a relative indication of the importance of different lines of business to your company (e.g. ‘Major’; ‘Moderate’ ‘Low’ or ‘None’). A breakdown by the primary categories is fine, but the more detailed lines would help provide more granularity if possible. Please identify any missing categories of interest, and any other comments.

Section 3: Cyber Exposure Data Schema v0.1

The purpose of this document is to outline a potential structure for an industry-standard Cyber Exposure Data Schema v0.1, to elicit early-stage comments and feedback from development clients.

Cyber Exposure Data Schema Structure

Our assumption is that each insurance company maintains policy level information (or policies suitably aggregated) in a database table of some type, which can be extended for cyber exposure monitoring.

Our v0.1 concept assumes that existing data architectures can have additional attributes applied to it. These attributes will be used for accumulation monitoring and risk analysis. In most cases we expect that the systems that companies have already in place to monitor, manage and analyse their exposure will be extensible to incorporate additional attributes. We also are proposing that some field attributes that are already used will have additional parameters or codes added for specific relevance to cyber risks.

The required structure is likely to vary according to class of business – for example casualty is likely to have a different data structure to property. We are asking our partners if possible to provide a listing of the data attributes they record for policies in each of the different classes of business they write that are of importance to them.

Please identify the attributes typically stored in your company policy database for different classes of business, for example, in any of these categories below, for the most important classes of business to you that you identified in 2.5, above. This information could be supplied in a separate document or data schema.

1. Cyber insurance
2. Property
3. Casualty/Liability
4. Auto
5. Marie and Specie
6. Aerospace
7. Energy
8. Speciality
9. War and Political Risk

An example of the type of listing requested is given in table 5, using property lines.

Listing of Key Attributes Requested, using Property Class of Business as example

Address Information: attributes such as
- Region Code
- Country Code
- State Code
- Street level address
- Lat/Long

Property Information: attributes such as
- Economic Sector Code (sometimes called activity code or industry code)
- Built Asset Code (sometimes called construction code)

Coverage Information: attributes such as
- Class of Business Code (assumed to be “property”)
- Peril Code (assumed to be “cyber”)
- Sub peril code
- Cover Code
- Exclusion Clause List (NMA2912, NMA2914, CL380 etc.)

Exposure: attributes such as
- Total Insured Value
- Deductible
- Limit

Table 5: Example of Key Attributes Requested, using property insurance as an example.

3.1 Please list the attributes (main fields) captured in your existing policy tracking or exposure management systems, for the primary classes of insurance business of most importance to you.

Cyber Specific Attributes

We are interested in your views on which potential cyber exposure attributes should be added to the required cyber exposure data schema. Attributes will be prioritised to assist with accumulation management – i.e. attributes that help identify when several policies could be affected by a similar or single event, and that assist in aggregation control – clusters of similar policies with potential for correlated loss. Research into cyber-related risk modelling is developing rapidly, with several different models already available. The work that will be supported by this cyber exposure data schema will help to identify scenarios of potential cyber events that could trigger large scale losses for multiple companies.

From principle 3, in the first section, we propose that the schema will be kept simple by standardizing a maximum of five attributes of cyber insurance policies. These five attributes are likely to be proxies – data from which is it possible to infer a wider range of characteristics of how an insured is vulnerable to a cyber attack. Volumes of detailed data such as is found in typical cyber underwriting questionnaires is unlikely to be practical as a data standard, so would be avoided. We would expect insurers to capture their own detailed underwriting information and detailed risk profiling data in their own systems, but propose that the data standard will be limited initially to high level account-level information, oriented around breach coverages. Some possible candidate attributes include.

- Number of Employees / Size of company
- Business Sector of Company
- Number of Records of Sensitive Personal Data that are kept within the Company's IT System
- Sensitive Data Records Categorized by Type; for example: Personally Identifiable Information (PII), Payment Card Information (PCI), Protected Health Information (PHI) etc.

3.1 Please list the cyber-specific attributes that you think will be most important to be included in a data standard for the exchange of cyber insurance policy-level information and accumulation management

Thanks and Accreditation

Many thanks for taking part in the consultation for the development of cyber data schema version 0.1.

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.