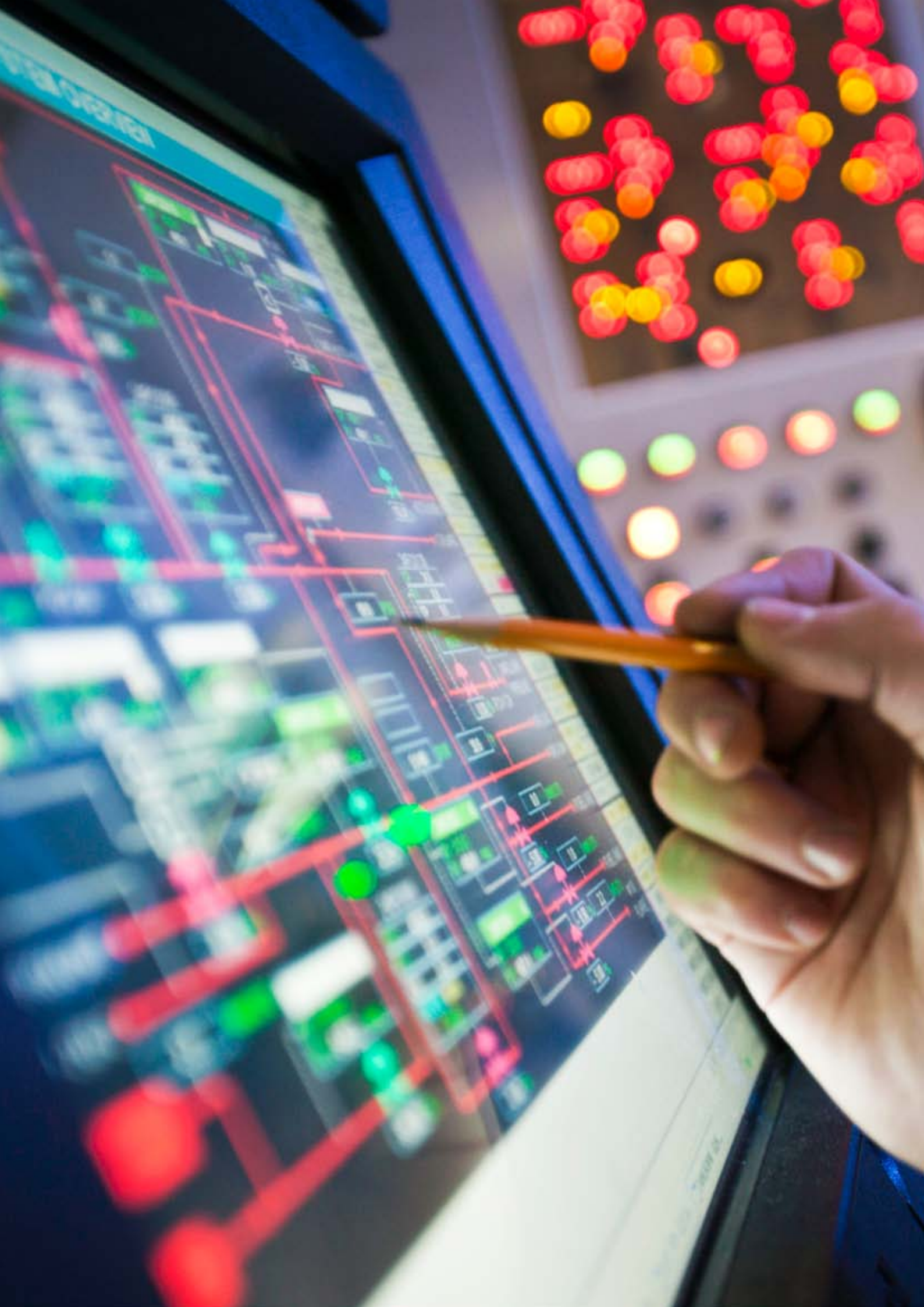
CRO Forum Concept Paper on a proposed categorisation methodology for cyber risk

June 2016



Contents

Introduction

The continuing evolution of cyber risk

The increasing concern around cyber risk continues to dominate discussions in nearly all forums across industries and public sectors. This takes the form of discussions around data protection, network and system security, digital innovation and disruption.

The CRO Forum looked into the issues around cyber resilience in the paper it published in 2014[1]. In this paper, cyber risk was defined as the risk of doing business in the cyber environment. This paper builds on the 2014 paper to focus on how to address the challenges around the collection of data to support improved cyber resilience.

The definition of cyber risk covers:

- Any risks emanating from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks.
- physical damage that can be caused by cyber attacks.
- fraud committed by misuse of data.
- any liability arising from data use, storage and transfer, and
- the availability, integrity and confidentiality of electronic information – be it related to individuals, companies or governments.

The limited and fragmented data on cyber risk presents a significant challenge for all companies as they try to understand, mitigate and quantify cyber risks. A common language is needed that can help the different specialists communicate on cyber risk-related incidents in a way that is understood internally, recognised externally and provides information to help understand the risks and lessons to be learned.

In Europe, a few key events tend to be widely and repeatedly reported and utilised for awareness raising and benchmarking. This is partly due to the high level of sensitivity around cyber-incident reporting and partly due to confidentiality issues that can arise. Any methodology developed to gain more data on cyber incidents and risks needs to acknowledge and address this sensitivity and promote a culture of awareness around which cyber incident can be discussed.

This paper proposes a methodology for a common cyber risk categorisation. The paper's goal is to promote a common basis to help capture data on cyber incidents (incidents both leading to losses as well as near misses) and raise awareness and understanding of cyber exposures, accumulation and resilience.

This methodology has been developed to be compatible with existing cyber incident reporting protocols developed by the IT and Risk Management communities to improve the understanding of cyber risk or to respond to notification demands for threat information from governments. It looks to bring together terminology, reporting practices and expertise from the spheres of IT, Information Security, Risk Management and Underwriting to provide a potential common language for collecting cyber risk data.

It incorporates the standards for operational risk management reporting used with ORX and ORIC[2] and work and schema being developed to help the emergence of cyber insurance as an effective risk mitigation tool (eg RMS[3] and AIR[4]).

[1] CRO Forum 'Cyber Resilience – the cyber risk challenge and the role of insurance' December 2014 http://www.thecroforum.org/cyber-resilience-cyber-risk-challenge-role-insurance/

[2] ORX Association (CHE-109.982.492) and ORIC International are operational risk loss data exchanges helping advance the measurement and management of operational risk through sharing operational risk intelligence

[3] RMS – catastrophe risk modelling company introduced a Cyber Accumulation Management System – http://www.rms.com/cyber

[4] AIRWorldwide – Catastrophe modelling company http://www.air-worldwide.com/Documentation/Cyber-Exposure-Data-Standard/Index.htm

The proposed methodology should provide a common basis for evaluating cyber incidents and enable companies to build up a clear picture of cyber risks, helping them understand their cyber threat environment, from protection to exposure and from mitigation to resilience. It should also be calibrated with a threshold that provides insights on incidents that cause loss and near misses.

On this basis, the use of the standard terms within the methodology should provide information on incidents that can be subsequently analysed from a number of different perspectives. Success will depend on whether this methodology can be made to effectively record and describe cyber incidents in a way that creates a common language through cross-functional cooperation within organisations. As such, it is a proposal for engagement with CRO's, CUO's, COO's, Information Security experts and IT specialists.

The aim of this paper is to stimulate a dialogue on the practicalities of a methodology for common cyber risk categorisation; the possibility of creating a common language around cyber risk; and whether the methodology can support the effective collection of useful data to support enhanced cyber risk management and improved cyber resilience. The methodology is a starting point for discussion and will evolve as we learn from the dialogue and experience.

The CRO Forum plans to trial the methodology among its members to understand the practical difficulties as well as the costs and benefits compared to similar reporting that may exist. There may be significant practical challenges around collecting data using the proposed methodology and some of the terms may need further refinement to be clearly understood.

Separately, the CRO Forum has been working with ORX and ORIC to understand whether data captured using the proposed methodology could be shared at some point to provide wider industry benchmarking.

The CRO Forum welcomes feedback, comments and engagement to explore whether the methodology can be developed to enable easy and cost-effective adoption by companies as part of their frameworks for promoting and enhancing cyber resilience.

Key questions

1. What changes may be necessary to ensure that both the definitions and the information they are intending to capture are understandable across IT Information Security, Risk Management and Underwriting?
2. At what level should thresholds be set to capture incidents that result either in a loss or a near miss?
3. What are the practical challenges and limitations of using this common cyber risk categorisation methodology?

Proposed methodology for common cyber risk categorisation

The categorisation methodology is based around the existing categories, minimum standards and definitions used for sharing of operational risk management incidents through the Operational Risk Databases (ORX/ ORIC).

The methodology illustrated in the diagrams below is as follows:

- Identify a cyber incident using one of 4 categories
- Assess whether the incident meets the thresholds for reporting
- If it does, identify the appropriate event and root cause description
- In collaboration with Information Security / IT Security and Operational Risk Management, identify the actor(s) causing the incident
- Based on the threshold assessment and the dialogue between the different stakeholders, impact categories should be identified for the incident
- Where relevant, any relevant cyber insurance cover should be identified; and
- Similar to existing ORM standards, this process should generate various standard descriptors to describe the characteristics of the incident

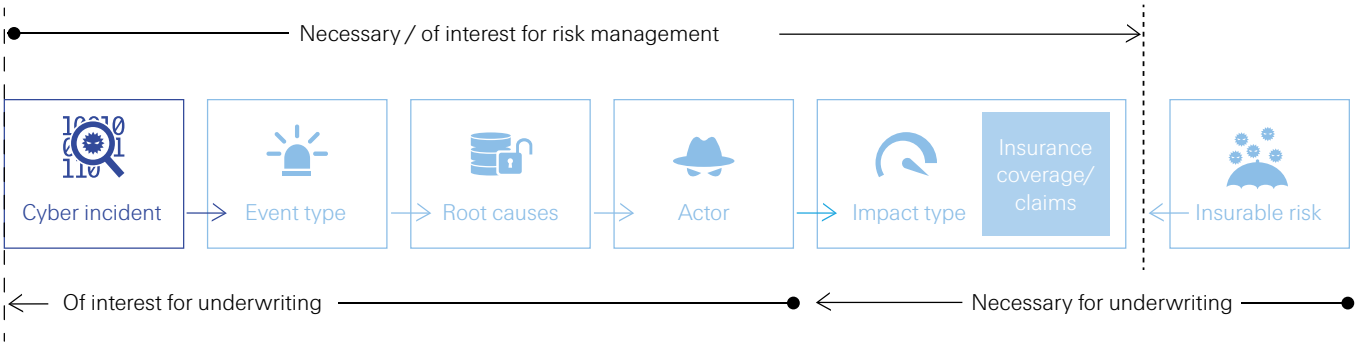
Impact is a key piece of information to identify during the categorisation process, as this is of interest to both operational risk management and underwriting risk management.

It may not be possible to complete all the steps in the categorisation upon identification of a cyber incident. Once a cyber incident has been identified, the focus should be on logging the cyber incident and capturing as many aspects of the categorisation as possible, recognising that these may be updated and adapted as more information becomes available.

The methodology aims to capture the minimum amount of detail needed to provide a high level understanding about an incident. Further attributes can be added by organisations depending on their focus and interest.

As a starting point, it is important to understand: whether companies are able to use the language created by the proposed methodology; whether it enables the collection of more cyber incident information in a common form that can deliver real benefits for the company; and also whether the data itself can prove useful.

In the following chapters, each of the steps in the categorisation methodology will be explained in more detail.



Key Steps

1 Cyber incident occurs

- Cyber incident **identified** and **flagged** [e.g. by IT/Information Security]
- Information about an actor included if possible

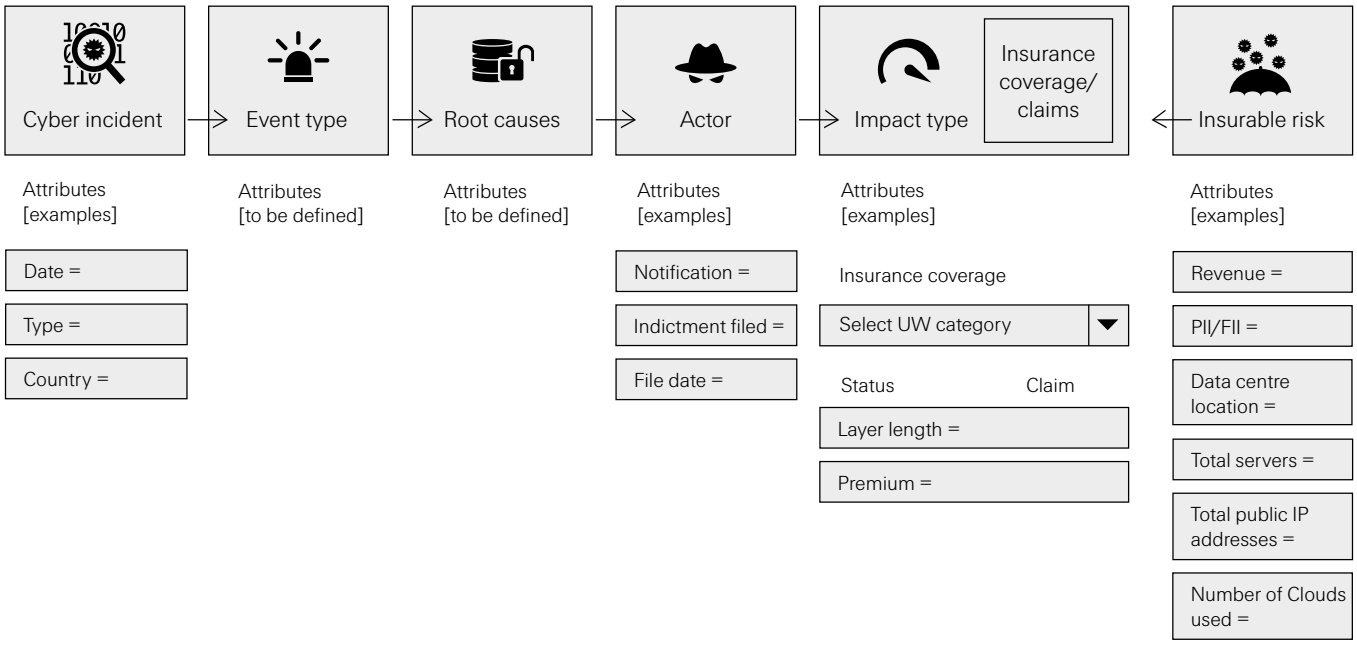
2 Information gathered

- Identification shared with operational risk colleagues to determine the **loss event, root cause** and **impact**

3 Database populated

- Incident cazegorised in the company's operational risk database

Potential attributes can also be added



Potential benefits

A key question that has driven this work is, "how would a common categorisation methodology help the CRO, CIO, CISO and/or COO and eventually the CUO manage organisations' cyber resilience and exposure from the underwriting of cyber risks?"

The primary purpose of the proposed categorisation methodology is to assist CROs, boards and operational risk teams evaluate their company's cyber defence capabilities, resilience and exposure. The cyber categorisation methodology should provide improved data that can support decision making, particularly through the challenge provided by the CROs and CISOs/CIOs/COOs. It should also provide the CUO with coherent and updated information.

The regulation in this area is developing rapidly. The proposed categorisation methodology creates a common language that should enable companies to adapt existing reporting protocols and respond effectively to the changing regulatory demands and notification requirements (e.g. General Data Protection Regulation and other regulatory reporting such as to the ECB[5]).

The immediate benefits for companies using such a common methodology include:

- Recognised definitions of cyber incident, loss event, root cause, actor and impact
- Straightforward process to identify relevant cyber incidents
- Consistent and comprehensive categorisation of cyber incident data
- More comprehensive information on cyber incidents including near-misses
- Methodology to support fact-based evaluation of preparedness and the effectiveness of IT controls
- Internal data to assess and challenge spending on IT/Information Security
- Oversight data for dialogue with IT and outsourcing/third party providers
- Data to manage and limit underwritten cyber exposure; and
- Data to enable in depth scenario and accumulation analysis

Event information can be used to validate information already available from IT/Cyber Security:

- Threat profile
- Core operational risks relating to cyber
- The state of the control environment and associated maturity
- Identification of protection gaps
- Prioritisation and investment decisions (mitigating actions)

As well as benefiting specific companies, a common language could benefit the whole financial services industry. The potential longer term industry benefits are:

- Preparedness for regulatory requirements
- Common awareness of the costs of cyber events (drivers of financial impact)
- Potential for anonymised sharing of cyber incident data across industries to enable benchmarking, awareness and understanding of loss impacts
- Increases industry's maturity and improves chances of preventing cyber related incidents

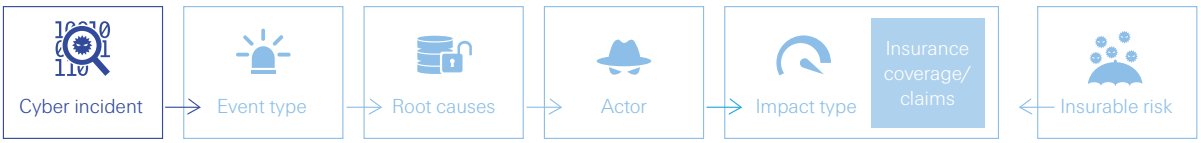
[5] Examples of recent developments, include the IAIS consultation on Issues Paper on Cyber Risks to the Insurance Sector http://www.iaisweb.org/page/news/consultations/closed-consultations/issues-paper-on-cyber-risks-to-the-insurance-sector, the Cyber Incident Data and Analysis Working Group White Papers from the US Department of Homeland Security https://www.dhs.gov/publication/cyber-incident-data-and-analysis-working-group-white-papers; and plans by the European Central Bank to set up cyber attack warning systems for banks http://www.businessinsurance.com/article/20160513/NEWS06/160519880/european-central-bank-to-set-up-cyber-attack-warning-system-for-banks?tags=|83|302|299

Key considerations for discussion

The intention is that the methodology should capture a relatively high volume of data and information compared to the data currently captured through existing ORM processes. The rationale here is that cyber incidents occur with a higher frequency than is currently reported and that there are benefits in building up more rather than less data for analysis.

The adoption of the methodology does represent a need for adaptation and change in focus for existing cyber threat/incident reporting frameworks and processes. Given the need to improve wider understanding and to respond to increasing board/ regulatory interest, there are clear benefits in such changes. Consideration should be given to the potential operational costs of introducing such evolutions and developments around existing systems, especially when these impact several units of the company. Cybersecurity incident handling teams may want to consider whether there is a way of automating the interface between their incident tracking systems and their operational risk systems.

The proposed methodology should be straightforward to adopt and deliver early benefits. Where it is adopted, it should assist CROs and other stakeholders in overseeing the managemen of cyber risks and exposures, both from an operational risk and underwriting perspective.



Cyber Incident

The cyber incident types correspond to the first observation by the impacted company of the cyber incident, malicious or not. The table below gives an overview of what can be observed without requesting any indications of attribution to actors, vector(s) used to commit the event, presumed or proven cause, impact or existence of cyber insurance cover.

Code	Incident Type Group	Description
1	System malfunctions/issue	Own system or network is malfunctioning or creating damage to third-party's systems or supplier's system not functioning, impacting own digital operations.
2	Data confidentiality breach	Data stored in own system (managed on premise or hosted/managed by third party) has been stolen and exposed
3	Data integrity/Availability	Data stored in own system (managed on premise or hosted/managed by third party) have been corrupted or deleted.
4	Malicious activity	Misuse of a digital system to inflict harm (such as cyber bullying over social platforms or phishing attempts to then delete data) or to illicitly gain profit (such as cyber fraud).

Identifying an incident is intended to be a first step. It is expected that once identified, further detail can be added with the use of attributes and the incident descriptors set out in Annex 1.

For the Cyber incident types, relevant attributes may include:

- Date of discovery of the incidents
- Time of discovery
- Place of discovery
- An open field to name the systems, databases or networks impacted or misused
- An open field to name the person/unit who discovered the event and first reported it

Threshold

To balance the costs of collection with the benefits, consideration needs to be taken of the threshold for capturing an incident and including it in a database using the above-mentioned categorisation. The intention is to increase the number of incidents (i.e. losses and near-misses) captured to deliver the maximum number of the benefits discussed above. Therefore, the thresholds should be considered more as guidance to qualify or quantify an event than a constraint not to report it.

It is difficult to assess the full loss impact of a cyber incident using the existing profit and loss level triggers for operational risk reporting as this would likely result in cyber trends and vulnerabilities being overlooked. Consideration is also needed around how to define other thresholds that can address this. One option would be to use one unique monetary threshold (gross loss amount) set for all firms. However, while this might drive completeness, there is a risk that it would only capture low frequency events.

It is proposed that the threshold for capturing cyber related incidents is based on meeting one or more of the following criteria:

- Any monetary loss amount
- Duration of outage/disruption to IT services
- Customers or employee data effected
- A number of users, workstations or servers affected
- A key security control compromise; or
- Legal trigger

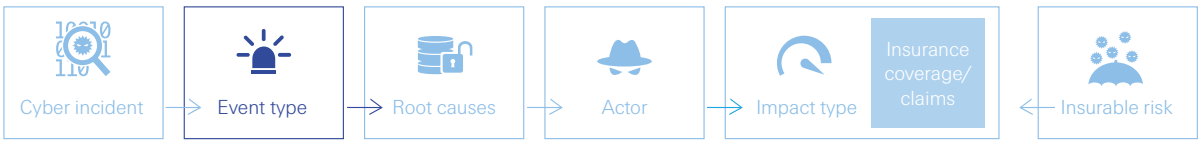
Initial thoughts are that some of the above thresholds could be represented as either a percentage or an absolute number. The level for a threshold needs to be set to capture the maximum number of incidents to best reflect the risk profile while ensuring that relevant incidents are captured. Therefore, the level might be different for different companies.

Given the different sizes of firm, it is not possible to determine a standard set of thresholds at this stage. This is an area where feedback and ideas are sought.

It is proposed that firms use the above list to set their own thresholds. The aim would be to generate a dialogue on how best to establish an industry-wide threshold level that could provide global statistics on an anonymised basis at a later stage.

Once a cyber incident type (and any corresponding attributes) has been captured that meets the threshold for inclusion in the internal reporting database, then the next step is to enter the Event Type Categories and the Root causes of the incident in accordance with the Operational Risk management process.

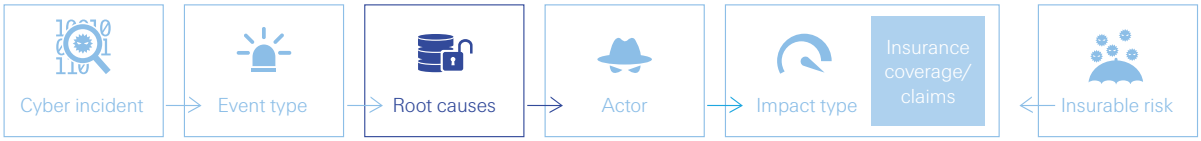

Pers
Name
Home A
Busines
Identity
Passpo
Driving
Income
Car Re
Other
ata
[Identify Person]



Definition of event types

The event categories are those used for Solvency II / ORX /ORIC operational risk management as follows:

Event-Type Category (Level 1)	Definition	Level 2 Categories relevant for cyber
Internal fraud	Internal fraud risk is the risk due to deliberate abuse of procedures, systems, assets, products and/or services of a company involving at least one internal staff member (i.e. on payroll of the company) who intend to deceitfully or unlawfully benefit themselves or others.	Unauthorised activity
		Internal theft & fraud
		System security internal Wilful damage
External fraud	Events arising from acts of fraud and thefts, or intentional circumvention of the law, actuated by third parties, including customers, vendors and outsource companies (including sub-vendors and sub-contractors), with the goal of obtaining a personal benefit, damaging the company or its counterparties (for which the company pays), or damage company's assets. Includes all forms of cyber risk, and frauds by clients and external parties (i.e. parties which do not collaborate usually with the company and have no access to the company's systems, such as non-mechanised brokers).	External theft and Fraud
		System Security External – Wilful Damage
Employment practices and workplace safety	Events arising from acts/omissions, intentional or unintentional, inconsistent with applicable laws on employment relation, health, safety and diversity/discrimination acts the company is responsible for.	Employee Relations
		Safe Workplace Environment
		Employment Diversity & Discrimination
Clients, products & business practices	Unintentional or negligent (careless) failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements) and corporate stakeholders e.g. regulators, or from the nature or design of a product.	Suitability, Disclosure & Fiduciary
		Improper Business or Market Practices
		Product Flaws
		Selection, Sponsorship & Exposure
		Advisory Activities
Damage to physical assets	Losses arising from the loss or damage to physical assets from natural disaster or other events.	Natural disasters
		Accidents & Public Safety
		Wilful Damage and Terrorism
Business disruption and / or system failures	Loss events associated with the interruption of business activity due to internal or external system and/or communication system failures, the inaccessibility of information and/or the unavailability of utilities and other externally driven business disruptions which may harm also personnel.	Systems failure internal
		System failure external
		Network unavailability
Execution, delivery & process management	Losses from failed transaction processing or process management, from relations with trade counterparties and vendors.	Transaction Capture, Execution & Maintenance
		Monitoring and Reporting
		Customer Intake and Documentation
		Customer / Client Account Management
		Vendors & Suppliers



Definition of root cause

The root cause pillar answers the question: "Why did it happen?" in order to improve CRO's knowledge of vulnerabilities and attack trends.

From an operational risk perspective, the root cause(s) identifies the cause of the event or failure to take actions to anticipate and prevent future impacts/losses. The objective is to identify the cause of the event or failure to take actions to anticipate and prevent future impacts/losses.

Analysis has shown that "Root cause" is one of the most important aspects after "Loss event type/Categories" to help better understand exposure to cyber risk and related vulnerabilities.

From an underwriting perspective, it is also useful to record root causes. Once loss data is properly collected, this information will be critical to identify exposure needing improvement in cyber risk assessments of clients' set up and for underwriting quality. The intention is to utilise as much as possible the existing Root cause categories in the current ORM frameworks with some slight refinements to reflect the need for further detail.

1. Codes description

Following a cyber incident, root causes should be identified to provide a more detailed description of what happened using the list mentioned below as a guide:

A. People
Actions arising from individuals within the firm.

- Employee qualification, technical skills, competence: Employee availability (composition of team, overwork, illness)
- Employee conduct (lack of motivation, integrity, honesty)
- Employee human error: oversight error, omission
- Culture/behaviour
- Poor communication
- Employee deliberate harmful act (malicious insider)
- Training & competence
- Key person / knowledge dependency
- Lack of human resources (poor segregation of duties)
- Other (only internal)

B. External causes
Risks arising from natural or man-made events or external harmful or deliberate acts

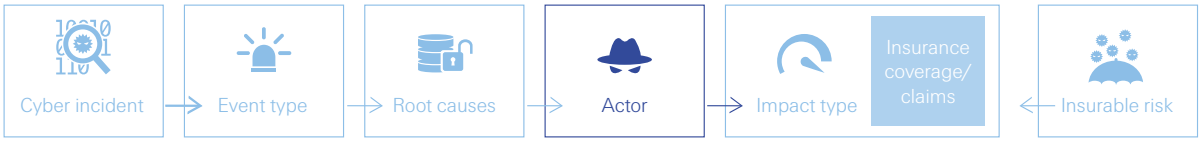
- Natural disaster (major catastrophic event impacting a key centre such as cloud, Internet provider)
- Epidemic/Pandemic
- Default/Misconduct of third party (vendor/service provider/outsourcer)
- External negligent or accidental harmful act
- Inferior quality or unsatisfactory adherence to delivery deadlines of a third party
- Man-made catastrophe
- Infrastructure failure (power / telephony / utilities)
- Changes in political environment
- Changes in legal or regulatory environment or practices
- Client fraud
- Intermediary fraud/misconduct
- Other external deliberate harmful act/theft
- Other

C. Process Risk associated with breakdowns in established processes, failure to follow processes or inadequate processes.	■ Inadequate process/control design and workflows (such as inadequate malware control, vulnerability management or patch management) ■ Inadequate process/control documentation, procedures, policies ■ Inadequate change management / integration into the business (such as inadequate security training or communication) ■ Inadequate monitoring/reporting/control management ■ Inadequate business continuity & crisis management ■ Inadequate vendors/outsourcing agreements & management ■ Lack of automatisation ■ Inadequate data quality ■ Other
D. System: Risk associated with the breakdown, failure or other disruption in technology and data, including inadequate technology to meet business needs	■ Hardware malfunction or failure ■ Software failure (coding/design/testing/legacy systems) ■ Software compromised via 3rd party update (mistake, oversight) ■ System failure ■ Insufficient IT/Infrastructure, hard- and software availability, capacity ■ Insufficient physical security (detection, prevention) ■ Inadequate infrastructure/hardware maintenance ■ Insufficient IT/Infrastructure security ■ Insufficient supply (energy, electricity, telecommunications, etc.) ■ Other

In case the item "other" is selected in the list above, only one root cause can be provided as it would mean that none of the sub categories can accurately describe the loss. The objective is to avoid selecting "other" for all fields.

2. Recording methodology

In cyber incidents, it is often the case that several consecutive failures lead to a harmful event. The existing root cause analysis framework within your organisations should help identify Level 1 and 2 Root cause for the cyber incident. We advise the user to record, at most, three root causes per incident following the above proposed Root causes.



Actors

The attributes present in the root cause schema allow information on the actors and their motivation (if known) to be captured. This provides precise indications useful to various stakeholders about the vectors used to cause the event.

Threat actors
A threat actor is a person or group that targets another person or organisation with some sort of motivation. They can be external or internal to the target, and some can even be involved unknown to themselves. For the purposes of this classification schema five threat actor categories have been defined:

1. Nation states:

Most developed nations and a number of developing nations have in place specific cyber capabilities.

Objectives: Generally, state-sponsored attackers seek high-value information that will give their countries a competitive commercial and/or military advantage such as intellectual property, classified military information, schematics etc.; in this regard they are motivated more by strategic than financial gain. In some reported cases, the objective of a cyber-incursion has been to disrupt another countries' attempts to develop specific technologies or capabilities e.g. nuclear power.

Targets: Nation-state attacks are growing in number, with a wide range of targets in diverse business and commercial sectors as well as in ther nations' government and military apparatus.

Attack vectors: Nation States typically have well-funded and organised cyber capabilities and consequently can utilise very sophisticated tools and techniques to target their 'mission' more precisely and consequently achieve greater success. They also actively fund the proactive research of the latest defence capabilities implemented by businesses in order to identify weaknesses and exploits.

2. Organised criminals:

These are defined as professional, career criminals working together to commit planned and coordinated serious crime on a continuing basis.

Objectives: The primary motivation of criminal groups is to attack systems is for monetary gain. This can be either directly through theft, fraud, extortion etc. or indirectly through identity theft, information brokerage, i.e. buying and selling e-mail address etc.

Targets: Typical organised crime targets include systems that contain personal information, intellectual property, and payment information.

Attack vectors: Characteristically, organised crime groups are highly skilled and sophisticated with access to a range of tools and techniques utilising for example spam, phishing, pharming, spyware, malware, ransomware etc.

3. Hackers:

These are defined as individuals or groups who covertly gain access to a computer system in order to gather information, cause damage etc. Historically, hackers would work alone, but as the hacking community has grown, like-minded hackers have come together to work in alliance and form loosely coupled, globally dispersed hacking groups. Hackers are also related with research and educational activities.

Objectives: Typically, hackers are motivated by the thrill, the challenge or for 'bragging' rights within the hacker community; some, to a lesser extent, can be motivated by monetary gain or notoriety.

Targets: Hackers' targets tend to be wide-ranging in nature from the obvious governments and financial institutions down to the less obvious such as individual celebrities and sports teams.

Attack vectors: While hacking once required good technical skill levels and computer knowledge, there is now a readily available marketplace of easy to use scripts, tools and protocols from the Internet that can be quickly deployed against vulnerable targets.

4. Hacktivists:

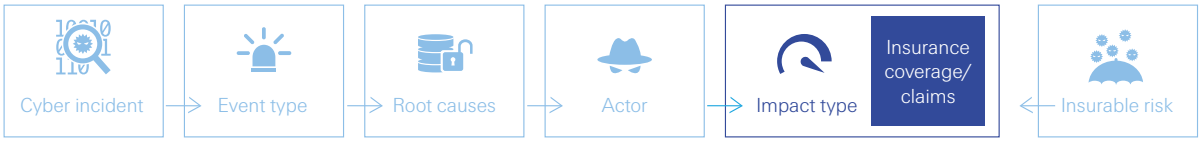
As the name suggests Hacktivists are a subset of Hackers that undertake attacks to promote a specific agenda, often political or religious or related to free speech, human rights, anti-capitalism or freedom of information. This group has similar objectives, targets and attack vectors as hackers.

5. Insiders:

Insiders can be employees or external third-parties such as outsourcing vendors, suppliers or consultants. There are three basic categories of insiders: i) Disgruntled; ii) Criminally motivated; and iii) Unintentional, who unwittingly facilitate outside attacks.

Objectives: The motivation for each category of insider varies; disgruntled employees often look to cause damage to applications or data or inflict embarrassment on an organisation through leaking data or information; criminally motivated insiders may misuse company assets or manipulate the system for personal gain; and unintentional insiders, who may unwittingly facilitate outside attacks, but are not strictly speaking primary attackers

Attack Vectors: Insiders do not need a great deal of knowledge or technical skills in relation to cyber-crime because their inherent knowledge of internal systems, processes and data through their job role often allows them to gain less or even unrestricted access to steal or modify data or to cause damage to systems.



Managing exposures – impact and cover

Any reported cyber incident will have an impact. Understanding the impact of the incident will be key in helping to assess the severity of incidents and identifying proposed areas for IT/Cyber security control and risk management focus.

Additionally, an impact can become an insurance claim if a relevant insurance product has been purchased and covers this type of loss. The decision of whether a loss will be covered should be made by considering additional information (attributes).

These attributes can include the following descriptions:

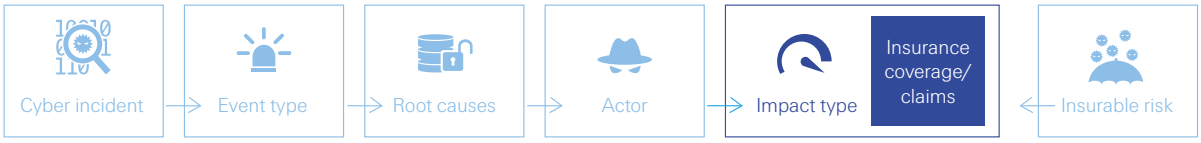
- Exclusions in insurance policy relevant to the Cyber incident
- Other descriptors such as deductibles, (sub)-limitations, etc.
- Premiums for the policy

The categories are compatible with the newly introduced University of Cambridge's framework (RMS/AIR[6]).

The primary purpose of the impact categories is to build a database of all impacts and losses incurred following a cyber incident, whether or not these losses are covered by an insurance policy.

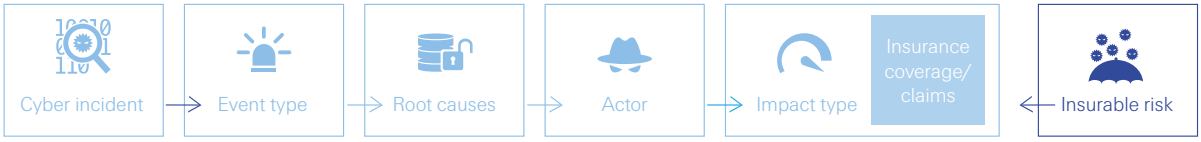
It is thus important to use these codes to register all impacts affecting all cyber incidents, even those not covered by insurance. This will serve the overall objective of gaining a better understanding of cyber risk and its impact.

[6] see footnote 4



Incident type group	Coverage scope
1 Business interruption Interruption of operations	Reimbursement of lost profits caused by a production interruption not originating from physical damage
2 Contingent business interruption (CBI) for non-physical damage	Reimbursement of the lost profits for the observed company caused by related third parties (supplier, partner, provider, customer) production interruption not originating from physical damage
3 Data and software loss	Costs of reconstitution and/or replacement and/or restoration and/or reproduction of data and/or software which have been lost, corrupted, stolen, deleted or encrypted
4 Financial theft and/or fraud	Pure financial losses arising from cyber internal or external malicious activity designed to commit fraud, theft of money or theft of other financial assets (e.g. shares). It covers both pure financial losses suffered by the observed company or by related third-parties as a result of proven wrong-doing by the observed company
5 Cyber ransom and extortion	Costs of expert handling for a ransom and/or extortion incident combined with the amount of the ransom payment (e.g. access to data is locked until ransom is paid)
6 Intellectual property theft	Loss of value of an Intellectual Property asset, resulting in pure financial loss
7 Incident response costs	Compensation for crisis management/remediation actions requiring internal or external expert costs, but excluding regulatory and legal defense costs. Coverage includes: ● IT investigation and forensic analysis, excluding those directly related to regulatory and legal defences costs ● Public relations, Communication costs ● Remediation costs (e.g. costs to delete or cost to activate a "flooding" of the harmful contents published against an insured) ● Notification costs
8 Breach of Privacy	Compensation costs after leakage of private and/or sensitive data, including credit-watch services, but excluding incidents response costs
9 Network Security/Security Failure	Compensation costs for damages caused to third parties (supplier, partner, provider, customer) through the policyholder/observed company's IT network, but excluding incidents response costs. The policyholder/observed company may not have any damage but has been used as a vector or channel to reach the third party
10 Reputational Damage (excluding legal protection)	Compensation for loss of profits due to a reduction of trade/clients because they lost confidence in the impacted company
11 Regulatory & Legal Defense costs (excluding fines and penalties)	A: Regulatory costs: compensation for costs incurred to the observed company or related third-parties when responding to governmental or regulatory inquiries relating to a cyber-attack (covers the legal, technical or IT forensic services directly related to regulatory inquiries but excludes Fines and Penalties). B: Legal Defense costs: coverage for own defense costs incurred to the observed company or related third-parties facing legal action in courts following a cyber-attack.

Incident type group	Coverage scope
12 Fine and penalties	Compensations for fines and penalties imposed on the observed company. Insurance recoveries for these costs are provided only in jurisdictions where it is allowed
13 Communication and media	Compensation costs due to misuse of communication media at the observed company resulting in defamation, libel or slander of third parties including web-page defacement, as well as Patent/Copyright infringement and Trade Secret Misappropriation
14 Legal protection – Lawyer fees	Costs of legal action brought by or against the policyholder, including lawyer fees costs in case of trial. Example: identity theft, lawyer costs to prove the misuse of victim's identity
15 Assistance coverage – psychological support	Assistance and psychological support to the victim after a cyber-event leading to the circulation of prejudicial information on the policyholder without his/her consent
16 Products	Compensation costs in case delivered products or operations by the observed company are defective or harmful resulting from a cyber-event, excluding technical products or operations (Tech E&O) and excluding Professional Services E&O
17 D&O	Compensation costs in case of claims made by a third party against the observed company' directors and officers, including breach of trust or breach of duty resulting from cyber event
18 Tech E&O	Compensation costs related to the failure in providing adequate technical service or technical products resulting from a cyber-event
19 Professional services E&O, Professional indemnity	Compensation costs related to the failure in providing adequate professional services or products resulting from a cyber-event, excluding technical services and products (Tech E&O)
20 Environmental damage	Coverage scope: compensation costs after leakage of toxic and/or polluting products consecutive to a cyber-event
21 Physical asset damage	Losses (including business interruption and contingent business interruption) related to the destruction of physical property of the observed company due to a cyber-event at this company
22 Bodily injury and death	Compensation costs for bodily injury or consecutive death through the wrong-doing or negligence of the observed company or related third parties (e.g. sensible data leakage leading to suicide)



Insurance coverage

The digital world allows almost all (criminal) activities and incidents to happen in the same way as the physical world: things can be stolen, hidden, destroyed, interrupted and abused. This is reflected in the list of categories above showing the types of impacts related to a cyber incident. However, many categories also relate to existing insurance products that will be influenced by changes through cyber development.

A key issue for insurance companies is the availability of incident and claims data in a consistent form that can help underwriters appropriately price the risk. Capturing cyber incident data with the methodology described will support understanding and provide the transparency to allow:

- Any enterprise to assess both 1st and 3rd party cyber insurance coverage fitting their own needs and non-cyber insurance products useful to buy and existing products to possibly change, i.e. increase the sum insured or lower the own retention rate because of a higher occurrence probability.
- The insurance industry to develop appropriate cyber insurance products and learn how their existing portfolios are impacted by cyber incidents. This could lead to changes along the whole risk management process: wordings, guidelines, underwriting and pricing. It will also support the insurance industry in streamlining and standardising cyber policy wordings and modules.
- The insurance industry to manage its cyber exposure and accumulations through the insurance products that it writes.

For an insurance company a cyber-risk assessment is necessary for:

1. Security and business continuity management
In order to achieve suitable protection against cyber incidents, companies need to determine critical data (sensitive data, competitive advantage information) and systems (business processes). Security and BCM also require companies to explore what internal and external threats need to be mitigated. The range of threats is wide-ranging, covering own employees (human error and targeted attacks from disgruntled employees), external attacks and vulnerabilities due to outsourcing and cloud services (check SLAs and contractual penalties). As well as a proper crisis management framework, companies also need to practise and review BCM processes and procedures to help mitigate losses should an incident occur: This must be fed by real incident data such as the ones proposed in this new schema.

2. Underwriting and portfolio management
The underwriting process needs to be adapted to technological developments. Possible emerging cyber risks in existing insurance products (affirmative and silent coverages) need to be monitored and necessary changes identified and implemented, e.g. through adapted pricing calculation, limits (sum insured, retention, reinstatements) or specific exclusions clauses. Crucial for insurance, and more so for the reinsurance industry, is managing newly arising and changing accumulation risks. Ongoing monitoring of new accumulation risk measures must be developed and put in place. This should also cover un-insurable aspects insurance (prerequisites) not met by e.g. pool solutions.

3. Meeting evolving compliance requirements and coping with globalisation

Due to the high impact of technological development, regulators and governments are acutely aware of cyber risk issues. Regulatory focus is mostly on protecting privacy of customers/policyholders. However, new risks could become a threat for social and political peace through, for example, cyber terror, cyber war and attacks on critical infrastructure, which would be a major issue for governments. This has led to diverse regulatory and reporting requirements globally. Requirements vary widely - at times even between states - and can even contradict each other. The introduction of the proposed schema should help all stakeholders meet such requirements and duties.

4. Constantly changing cyber coverage

Finally, all cyber knowledge gathered through own assessments and portfolio analyses can help develop own cyber insurance to protect the company, as well as support cyber product development offered to clients. Since technology is developing at an exponential pace, the parameters influencing cyber risks are constantly changing. Foreseeing upcoming trends is key for effective cyber risk management. Drivers of change are:

- the increasing dependency on internet and technology throughout the business value chain.
- the increasing data volume and types stored, processed and used for analysis (big data) due to the availability of cheap storage and new analytical tools.
- Other trends are less transparent in terms of their likelihood and speed, and imply more disruptive power, for example those arising from the smart world, i.e. smart homes, smart vehicles, smart health, smart manufacturing.

A necessary prerequisite for insurance is the independence of risks. Digitalisation presents a major challenge for the insurance industry as it increases interconnectedness resulting in accumulation risks: the merging of hardware, software, data and infrastructure leads to a very interdependent cyber world. So far, interdependent risks can lead to unforeseen and significant chain reactions. A solid cyber risk framework encompassing this methodology and the sharing of information will support CROs in coping with future cyber risks.

Conclusion

In conclusion, there is an opportunity to develop a common language for the collection of data to support improved cyber resilience. There are clear potential benefits, although the challenges are not to be underestimated.

A dialogue is needed to see whether a common methodology and the merging of existing reporting protocols can deliver standard definitions. This would enable more data on cyber incidents and risks to be collected in a way that addresses sensitivities and promotes the necessary culture of risk awareness necessary to support improved cyber resilience.

This paper sets out a proposed common methodology on cyber risk categorisation. This is a starting point for discussion. It will evolve as we learn from dialogue and experience. Its success will depend on whether the methodology can be made to effectively record and describe cyber incidents in a way that creates a common language through cross-functional cooperation within organisations.

The CRO Forum welcomes feedback, comments and engagement on this important topic.

Annex – Detailed cyber incident type and descriptions

Code	Incident type	Incident type group	Description
A	Own system malfunction	System malfunction/issue	A subject's (can be either a company or a person) own system creates continuous system errors or freezes completely. System rendered inoperable.
B	Own system affected by malware	System malfunction/issue	Internal controls (either human or systems) or users detect malware in own stacks or abnormal behaviour of deployed systems and software. Intrusion must be expected (or suspected).
C	Network communication malfunction	System malfunction/issue	The subject's (company or person) system cannot communicate via the internet or other digital network any longer or the connection is so slow that it becomes unusable.
D	Inadvertent disruption of third-party system	System malfunction/issue	Typically, a hacker will take control of (part of) the company's computer system or network and through this channel conduct illicit activites toward a third-party. This can be for instance under the form of a DoS attacks using many such controlled computers (botnet) or to transmitt subrepticely a malware or wrong informations.
E	Disruption of external digital infrastructure	System malfunction/issue	A subject (company of person) is stopped or impeded in its digital activities or business by a failure of an external digital infrastructure such as a cloud or other data processors/storages.
F	Theft of own data	Data confidentiality	A subject (company or person) detects its own proprietory data (financial data, trade secrets, etc.) outside of its data perimeter, e.g. subject is made aware of the fact that its data is being sold, traded or exposed for instance on the dark web, or that its data is being made available openly.
G	Deletion of own data	Data integrity / Availability	A subject detects that its data has been deleted from its storage solutions or out of its applications.
H	Encryption of own data	Data integrity / Availability	A subject detects that its data is no longer accessible because it has been encrypted by a third party and can only be used again once it is decrypted (often following the payment of a ransom to the third-party).
I	Corruption of own data	Data integrity / Availability	A subject (company of person) detects that its data has been corrupted (changed). This might be very difficult to detect if the changes are small and infrequent and might take a long time to find out. Other corruptions might be more blatant and can be found out easily.
J	Theft of third party data	Data confidentiality	A subject (company or person) detects that third-party's data it stored or processed (typically PII/FII/PHI) is found outside of its data perimeter, e.g. subject is made aware of the fact that this third-party's data is being sold, traded or exposed for instance on the dark web, or that this data is being made available openly.
K	Deletion of third party data	Data integrity / Availability	A subject (company or person) detects that third-party's data it stored/ processed (typically PII/FII/PHI) has been deleted from its storage solutions or out of its applications.
L	Encryption of third party data	Data integrity / Availability	A subject (company or person) detects that third-party's data it stored/processed (typically PII/FII/PHI) has been encrypted by a malintentioned party and can only be used again once it is decrypted (often following the payment of a ransom to the malintentioned party).
M	Corruption of third party data	Data integrity / Availability	A subject (company or person) detects that third-party's data it stored/ processed (typically PII/FII/PHI) has been corrupted (changed). This might be very difficult to detect if the changes are small and infrequent and might take a long time to find out. Other corruptions might be more blatant and can be found out easily.
Q	Misuse of system	Malicious activity	Cyber-bullying, cyber mobbing. A "hacker" or malintentioned actor misuses a digital system such as social media to publish or distribute defamating (libel, slander) or embarassing messages about the victim.
R	Targeted malicious communication	Malicious activity	Typically phishing or CEO scam attempt, or more sophisticated type of request for (confidential) information with a malicious intent.
S	Cyber Fraud, Cyber theft	Malicious activity	A hacker initiate illicit value transfers (such as money transfer) through hacking itself into or misusing credentials and acting in the subject's system.

The CRO Forum is supported by a Secretariat that is run by:

KPMG Advisory N.V.
Laan van Langerhuize 1, 1186 DS Amstelveen, or
PO Box 74500, 1070 DB Amsterdam
The Netherlands
www.thecroforum.org