Supporting on-going capture and sharing of digital event data

Achieving a common language to enable understanding of and communicate digital risk/events – Findings from the CRO Forum trial data of a common categorisation methodology for cyber events

February, 2018

CRO FORUM

Contents

Executive summary

Supporting on-going capture and sharing of digital event data

With rising cyber-crime highlighting vulnerabilities in digital dependency and the efforts by policymakers to establish frameworks to protect the rights of individuals and business, digital security awareness and resilience is one of the highest priority items on all agendas.

Board and executive management are looking to risk management and/or information security experts (CROs and CISOs) to provide a clear understanding of an organisation's digital resilience and how the organisation can effectively protect itself from cyber threats. However, there are significant inherent difficulties in being able to provide a credible view.

Primarily there is a lack of common data understood by different disciplines within and across organisations. Taxonomies have been developed to describe cyber threat information in a way that can be shared, stored, and analysed in a consistent manner. These include the STIX, VERIS, TAXII, CybOX, RMS, AIR as well as methodologies from US Department of Homeland Security and other government bodies. These taxonomies typically capture data for a very specific purpose and the standards are often very technical in nature. This reduces the ability of such taxonomies to inform wider audiences on the business context of the implications and benefits of using them.

A solution needs to be found that supports a more holistic understanding of digital resilience and security across the business. A common language is needed that enables different specialists to communicate in a way that can be understood across specialisms, within organisations and across industries/institutions. This is key not only to help internal understanding, but also to enable better awareness of what risks can ultimately be transferred to third parties.

The CRO Forum published a concept paper in June 2016 that set out a potential basis for a common language that could be used to describe digital events in a way that leveraged the work of different taxonomies and could fulfil different purposes.

The aim is to help enable an empiric description of digital events that can be accumulated internally to provide insight on the effects of digital events and shared externally to enable benchmarking and greater understanding of relative digital resilience.

3 Stages

The CRO Forum performed a trial within its membership supported by ORX and ORIC International to assess whether such a taxonomy could achieve this aim. The trial was divided into three stages:

- Stage one: testing understanding of the taxonomy within organisations – this led to refinements to the terms used in the taxonomy;
- Stage two: looking at the threshold for capture and sharing of digital event data – this set a basis for thresholds to be used to determine which events to capture;
- Stage three: with the support of ORX and ORIC International, collection and sharing of digital events occurring in a 10 month period, described using the updated taxonomy. These events were captured internally by members and shared anonymously with ORX and ORIC International. ORX and ORIC International then compiled and shared the aggregated data with their members

Nearly 700 medium or high impact digital events were captured and shared by participants over the trial period. This represents a significant first step in confirming that the taxonomy can be used successfully to:

- Consistently capture digital event data,
- Provide useful and actionable insight, and
- Be shared externally to build up a wider picture of digital events and their impact.

The findings from the trial are explored in more detail in this paper. The paper sets out how the taxonomy evolved during the trial, and can be evolved further, to incorporate other taxonomies (particularly STIX and VERIS) as a way of improving recognition of terms across specialisms, fit with existing processes to capture events and increase the value of data captured for different stakeholders. It also explores some of the challenges around setting thresholds and evaluation of events that may be Near Misses.

Consistency and normalisation are key challenges going forward. The paper provides a set of standards and definitions that can be used to support the use of the taxonomy within organisations and promote its consistent application across organisations. This is based on the standards used for the trial and in place with ORX and ORIC International to currently capture operational event information.

Normalisation of the digital event data collected will be an important factor that needs to be considered further should the taxonomy be adopted across different industries to ensure capability to undertake valid benchmarking based on the captured event data.

The value of the exercise that led to this paper can be shown not only by the data collected during the trial, and the potential analysis that is possible from this limited data pool, but also by considering that a number of participants have felt confident to continue collecting and sharing data given the added value such data provides to their understanding of their digital resilience. Propositions are being developed to support the sharing of data.

Exposing the CRO Forum taxonomy to a wider audience is a further step in trying to promote ways to improve digital resilience. The CRO Forum supports the on-going dialogue to support a common language and standard that encourages sharing of digital event data and their effects to enable better understanding of the impact of increased digital dependency.

Section 1 – Introduction

Introduction

In 2014, the CRO-Forum cyber working group published a paper "cyber resilience" which outlined key factors for cyber risk management in insurance companies. One of the success factors identified was the availability of cyber (loss) data. However as cyber insurance products are a relatively new business line for most insurance companies only a little loss history is available as yet. This challenge remains as digitalisation with its fast changing, technological nature makes historical loss information less relevant in assessing and underwriting cyber risks.

According to some studies on insurance market (Accenture's High Performance Security Report 2016 or IAIS' Issues Paper On Cyber Risk To The Insurance Sector) Insurance and Financial sectors are a preferred target for cyber threats, due to the large amount of personal health information, credit card, bank account data, and trade secrets information managed. Nevertheless, the existing Cyber Security data analysis, like the well-known Ponemon Cost of Data Breach study, are considering a high variety of industries and organisations, and are not sector-specific.

The ability to share the limited amount of cyber loss/digital event data available across and within different sector stakeholders to build up a loss database would be a ground-breaking step forward. The CRO-Forum cyber working group decided to support the aspiration of digital event data sharing by developing a methodology on how to categorise and exchange cyber loss data.

The focus of the working group differed from the present language standards oriented to describe cyber threat information in a technical perspective, like STIX and TAXII, as they are missing important attributes for understanding the risk posed by such events. For example:

- insurance policy and loss details,
- the option to enrich the database with existing data loss information available (Verizon, Advisen,...), and
- the possibility to combine with the existing operational risk data

By analysing accepted and popular existing language standards, matching them with the additional requirements, the group came up with a taxonomy that combines three standards: the slightly adjusted STIX/VERIS structure, fields linking with the operational risk data base and insurance related attributes such as those published by the Cambridge University (http://cambridgeriskframework.com/getdocument/38).

Ultimately, twenty global insurance companies tested the methodology over almost a year, collecting over 700 data points. The analysis of the results showed the difficulties around interpreting "Near Misses", that the shared data sets needed additional identifiers (e.g. company size) for meaningful evaluation, and that a financial loss calculation definition was needed (e.g. to include internal employee's extra working time). The taxonomy has been updated with this information.

Cyber insurance business

This paper sets out in Appendix 1 and 2 the reviewed and adjusted framework following completion of the trial, to serve as a basis for further cooperation in sharing digital event data and knowledge. It also outlines how to implement the methodology as well as how findings can be used by the different disciplines in a company around risk management, the IT department and Underwriting.
Two main drivers are considered:

A company's cyber/digital resilience

- Data gathered using the taxonomy can support risk assessment drivers for different jurisdictions and regions, as well as investment decisions
- Basis to support risk modelling for cyber exposure reducing and/or optimising capital allocation
- Operational risk management insights to inform individual cyber scenarios of a company, especially with the ongoing (local and global applicable) changes around compliance and data security
- Security and business continuity management around different (IT) disciplines, from firewalls and network management to shaping service providers, SLA's, or contractual penalties
- Risk education and awareness training, for both internal employees and staff of service providers involved

Cyber insurance business

- Strategy decisions including risk appetite for different markets and industry sectors as well as risk transfer decisions for the different coverages.
- Impact on pricing and various wordings used
- Loss monitoring and trend analysis for diverse geographical conditions
- Underwriting requirements and guidelines
- Insights into concentration of claims and accumulation risk given the high interdependencies across geography's and industry segments
- Lobbying activities representing industry or company

Benchmarking

Applying the digital event data categorisation, various analyses on the overall data collection allow for general benchmarking. Some examples include upcoming trends, recent peaks and troughs or anomalies. By comparing the own digital event data against the anonymised collective, individual benchmarking is possible and delivers insights on strengths and weaknesses of the company.

Areas of benchmarking include efficiency of controls that can indicate obvious room for improvement. The results deliver a highly valuable basis for discussions of risk management within internal departments and external service providers in order to derive project / investment / budget proposals for management within each company. Conclusions also provide overall direction for national governmental and regulatory requirements for different industries. Moreover, it supports streamlining the market variety of data structures, wordings or coverages offered.

Benefits

Since digitalisation is interconnecting the world, transparency on (inter)dependencies is crucial for proper digital risk management within a company. When analysing both a company's and the wider industry's digital event data sets, (un)known reliance between various factors can be discovered.

Many digital events can combine multiple perspectives or vectors that need to be tackled from several angles. It is increasingly important to improve coordination across different disciplines that are often spread out in various departments of a company. The ability to use a standardised basis for sharing information across a company is key.

- For example, an increase of successful phishing incidents should immediately lead to awareness trainings for employees and service providers used as well as improving firewall and network security. In addition, an update of operational risk scenarios might be required.
- Another example is the implementation of the EU regulation "General Data Protection Regulation (GDPR)" with increased data protection regulations: the vulnerability analysis is performed by the data security officer while respective countermeasures and tools necessary will be implemented by security & business continuity as well as IT. Communication department will possibly prepare press releases needed in case of a successful attack. The widely used term "not if but when an incident happens" has proven as an unfortunate truth.
- For underwriters who need to design new cyber security policies, the framework could provide insight and benchmarks in the maturity of the data infrastructure of companies.
- Risk management can benefit from the common database using the data available as an input when performing needed risk scenario evaluations for the Solvency capital requirement.
- In order to make different departments and units act in an efficient and reliable way, and to receive essential results and data in a form they can readily digest, a uniform framework and approach are crucial.

Consistency

By applying the schema consistently and benchmarking findings it will reveal if and how the company's digital resilience is developing: if software and hardware controls are appropriate, if newly implemented services, tools or incident management strategies are efficient, if employees are educated in incident awareness requirements to be able to respond appropriately. Such an approach allows for the building up of a cyber-strategy with a coherent framework for all contributing disciplines that can be implemented and further developed in a consistent way to effectively mitigate cyber risks.

Supporting quality control

Proper monitoring through an internal control system (ICS) delivers a solid basis for discussions within risk management, with IT and services providers on how to shape the future digital defence strategy:

- Which/what are crucial risk control points and how can possible vulnerabilities be discovered and reduced or removed?
- How can the integrity, availability and continuity of key data, the crown jewels of a company, as well as critical systems be guaranteed along the company value chain?
- Are safety and compliance topics addressed appropriately?
- Are outsourcing services and their interface management adopted suitably?

The common database can help in assessing the current status of ICS, answering those questions, and preventing and understanding the threats that are upcoming or increasing in the insurance and financial sector.

Improved budget allocation

Finally, greater transparency supports decision making processes allowing for more appropriately targeted and balanced allocation of both resources and the finite security budgets:

- What are crucial projects to get started immediately?
- Which investments can be postponed for a while?
- What are the skills necessary to remain resilient in the future and how can we attract or develop those talents?
- Which exposure can the company accept within its own appetite and which should be transferred?
- Which are the upcoming challenges and main trends the market is facing concerning cyber threats?

Defining thresholds

Given the frequency with which digital events can occur, for example the number of attempts to penetrate defences as on a firewall log or malware making it through the defence layers, it is necessary to determine thresholds to help select which events will be reported using this common language. A severity matrix is a selection of thresholds across different categories that are used in order to determine their categorisation and prioritisation based on their impact on a firm.

Different factors can be considered such as Financial Loss, Regulatory Impact, Customer Detriment and other similar categories. A value is then assigned for each of these categories in turn, broken down by severity of impact. These values in turn determine the classification of the event. The main classifications are High, Medium and Low but any other similar definitions can be used. The matrix can thus be used to classify risks according to their impact over a broad set of categories and assist with prioritisation, visibility and awareness.

These factors and illustrations of the findings that can come from applying a common language are explored further in the findings from the trial run by the CRO Forum.

Section 2 – Findings from the trial

2.1 Introduction to the taxonomy

A key factor in the success of any initiative to collect and share data is the scope and performance of the taxonomy used to describe submissions and enable valid statistical analyses.

This section outlines considerations relevant to the design of the taxonomy, describes the taxonomy used for the trial, compares the taxonomy with other similar schemes and provides an assessment of how the taxonomy performed during the trial.

Taxonomy design considerations

First and foremost the taxonomy needs to consider the purpose for which the data is to be used. The CRO Forum's objective was to collect data that would enable analyses to inform decisions on digital/cyber resilience and underwriting Cyber insurance business. Furthermore the CRO Forum identified that, for most insurance companies, there is only a little loss experience available in this area and therefore wanted to enable a broader sharing of cyber event data available across insurance and financial sector stakeholders to build up an event database.

To satisfy these objectives the taxonomy needs to enable the capture of events with their actual or potential loss values, to identify the different types of events and to capture relevant supporting context to ensure these events' categorisation is understood. The CRO Forum recognised that several existing taxonomies were available which, separately, described cyber incidents, operational risk and insurance impacts.

It also recognised that using existing elements of well-known taxonomies would provide a good platform for easier adoption amongst participating firms. The taxonomy used for the trial therefore drew upon the relevant portions of the VERIS, ORX/ORIC International and Cambridge taxonomies respectively.

Three further aspects were recognised as important for effectiveness of the CRO Forum taxonomy

- That it is sufficiently easy to use by different specialists across a company.
- That it allows greater opportunity for increasing the number of events collected by participating firms, enabling the faster build-up of a larger database of event information.
- That it supports the collection of sufficiently accurate and consistent data to enable meaningful statistical analyses.

Consideration of these factors led to the CRO Forum taxonomy being defined with a relatively small number of fields with defined categories.

Taxonomy used for the trial
The following table introduces the taxonomy used for the trial.
This is described in more detail in Appendix 2.

Field	Multiple choice
Incident type	
Action	
Asset impacted	Yes
Affected kind of data	Yes
Actor	
Event type	
Root Cause	
Business impact	Yes
Financial impact	
Currency	
Malicious vs. non-malicious	
Status (open, close)	
Impact location	
Threshold rating	
Dominant threshold triggered	
Near miss	
Date of discovery	
Event description	

2.2 Compatibility with other cyber taxonomies

While we consider the developed taxonomy to be optimised for the purpose of collecting data to inform decisions on digital resilience and to offer a solid base for further amendments with a view to support underwriting cyber insurance business, it is recognised that the CRO Forum taxonomy will operate alongside other similar taxonomies that serve specific adjacent needs. The CRO Forum taxonomy actively considered such taxonomies in the design process.

This section provides a comparison between the CRO Forum taxonomy and three other industry standard taxonomies for recording cyber events that have informed and been incorporated into the design of the CRO Forum taxonomy. It considers the type of event that qualifies for capture, the relative scope of coverage and the potential for translation between records in different taxonomies.

2.2.1 Taxonomies considered

The three taxonomies considered are introduced in the following paragraphs:

VERIS
VERIS a community project started in 2010 to define a Vocabulary for Event Recording and Incident Sharing. It is intended to help organisations collect useful incident-related information in order to enable anonymous and responsible sharing of that information. It is an after-the-fact characterisation of cyber incidents intended for post-incident strategic trend analysis and risk management.

STIX
STIX a structured language for describing cyber threat information so it can be shared, stored, and analysed in a consistent manner. It is developed by the OASIS Cyber Threat Intelligence Technical Committee. STIX provides the capability to capture information about security incidents and their effects but does so in the context of a broader threat intelligence framework.

ENISA Threat Taxonomy
Provides for a classification of threat types and threats at various levels of detail. It has been developed over the past years as an internal tool for ENISA used in the collection and consolidation of threat information. Most of threat information included was from existing threat catalogues in the area of information security and in particular risk management.

2.2.2 Taxonomy comparison

This section sets out the key differences between the CRO Forum taxonomy and the other standard taxonomies as described above.

Qualifying records – Risk Events vs security incidents
One key difference is in the types of event which are intended to be captured.

IT security events and minor incidents may occur on a daily basis within an organisation but for the most part these would generally not be considered to represent Risk Events or to be of a materiality that would breach an organisation's Risk tolerance and/or be reportable to the regulator. The CRO Forum taxonomy is intended to be used for material digital events whereas STIX and VERIS intend to capture a much broader number of incidents and security events.

Conversely records in STIX and VERIS are unlikely to be used to capture certain types of incident such as environmental or social. These types of event should be included in data sets using CRO Forum taxonomy.

In addition, it is recognised that there can be value in capturing data on Near Miss events where good fortune prevented any material impact from realising. In looking to implement any Digital Event taxonomy, organisations will also need to consider how a Near Miss is defined and treated, recognising that it is entirely possible that a Near Miss may not always be managed through the Incident Management process.

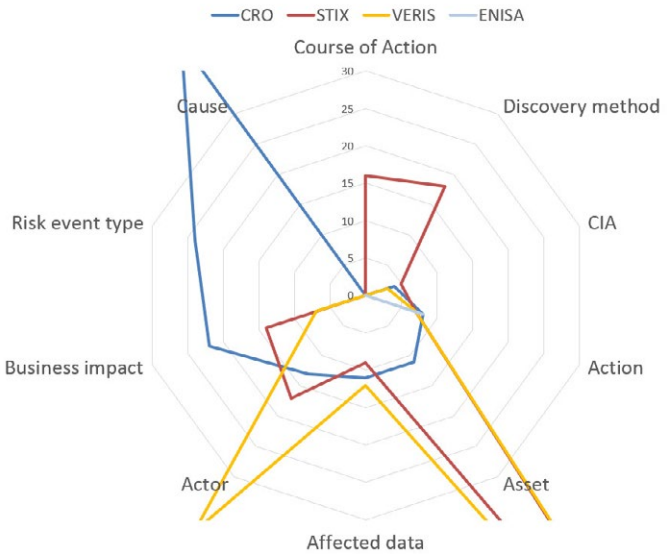
Comparison of scope – Breadth vs Depth
An effective method to visualise the difference between the taxonomies is to plot the number of categories defined for each field of the taxonomy.

To perform this analysis, we have to map loosely equivalent fields between the taxonomies. This is shown for ten key fields in the following table:

CRO field	VERIS field	STIX field
Incident type	Incident type	Nature Of Security Effect
Action	Actions	Categories
Asset	Asset	Affected Assets (Type)
Affected kind of data	Affected kind of data	Victim Targeting
Actor	Actor	Actor (Type)
Business impact	Loss categorisation	Impact Assessment (effects)
Event type	N/A	N/A
Root Cause	Root causes	N/A
N/A	Corrective actions	Course of Action
N/A	Discovery method	Discovery method

For example, the CRO Forum taxonomy defined eight categories within the Action field. Based on these mappings, we can visualise the differences by plotting the number of categories against each field on a spider diagram. The ENISA taxonomy is also included although this only has categories for the Action field.

Taxonomy comparison - number of categories per axis



This highlights some clear areas of difference which are aligned with the purpose of each taxonomy:

- The CRO Forum taxonomy focusses on the cause and risk event type. This is relevant to understand what leads to the risk becoming realised and therefore helpful to understand the likelihood of future events when similar conditions occur.
- The STIX taxonomy has more definitions on the course of action and method of discovery. This is consistent with its purpose as supporting proactive defence because these details will help an organisation detect and deal with incidents early in their lifecycle.
- The VERIS taxonomy is focused on actor and asset. This indicates that VERIS is intended to capture what happened but less about the why and the consequences.

Ultimately, the CRO Forum taxonomy is compatible with other taxonomies and can help provide a more detailed picture of the incidents that affect an organisation in a language that is recognisable to a number of specialisms.

2.2.3 Translation of records

Recognising that some potential users of this proposed taxonomy may already capture incident data in another form, this section provides some guidance on how to translate from STIX records to the CRO Forum taxonomy.

STIX fields to populate

To ensure that a STIX record can be converted to a record in our taxonomy the following optional elements of the STIX record should be populated:

Security_Compromise
Status
Affected_Assets->Nature_Of_Security_Effect
Categories
Affected_Assets->Type
Leveraged_TTPs->TTP->Victim_Targeting
Attributed_Threat_Actors->Threat_Actor->Type
Impact_Assessment->Effects
Impact_Assessment->Total_Loss_Estimation

When converting a STIX record to the CRO Forum taxonomy, the above fields can be translated according to the mapping provided in the previous section.

Additional data to capture

A STIX record is not able to hold all the details necessary to populate a record in the CRO Forum taxonomy. In particular, it will be necessary to separately capture and record the root cause of the event when creating a record in our taxonomy from a STIX record.

However, by migrating findings from STIX or other taxonomies used into the CRO Forum taxonomy, it should be possible to get a more detailed picture on digital events for analysis.

2.3 Data analysis

The results analysed below are based on the selected taxonomy and pilot conducted amongst the participating member firms. Please note that twenty companies provided data during the ten months trial period.

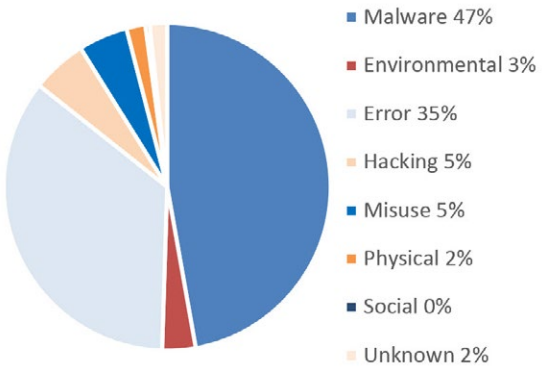
In the following paragraphs, we show several examples of possible data analysis that can be undertaken on the data that has been collected. The examples shown are indicative ideas based on the data pool of events shared by participating firms during the short term trial. They demonstrate the potential to improve the understanding of the types and severity of the various IT-failure events, e.g. IT-security, IT-human or IT-system failures.

In our opinion, such analysis can be useful at different levels: For one single company if the data captured is kept within the company or – if data are exchanged (as was the case in the pilot) – for benchmarking and "market" analysis. Please note that no company benchmarking is presented here as the results of the trial data used for this analysis were fully anonymised. As the trial data was not calibrated with any "size" parameters, no further underwriting analysis has been undertaken.

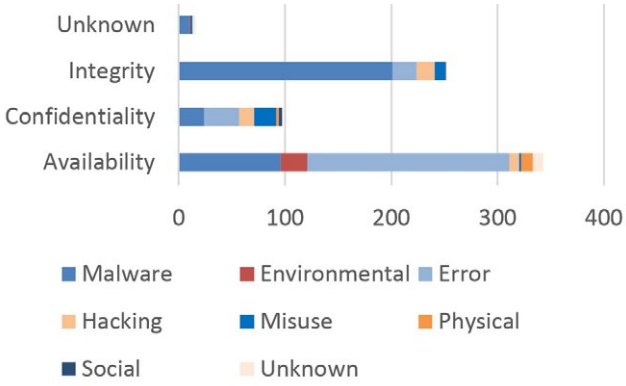
Analysis of Actions and Incident Type

The distribution of the actions shows a very strong emphasis on events caused by Malware (47%), followed by Errors (35%). A more detailed view differentiating the Incident Type of the events (Confidentiality (93 cases), Integrity (249 cases), Availability (339 cases), Unknown (16 cases)) demonstrates that Integrity cases are almost exclusively caused by Malware, whereas Availability cases are mainly caused by Errors. The large proportion of "malware" might indicate that more effort are needed in the malware filtering and defence.

Action (in %)



Action by Incident Type (CIA)

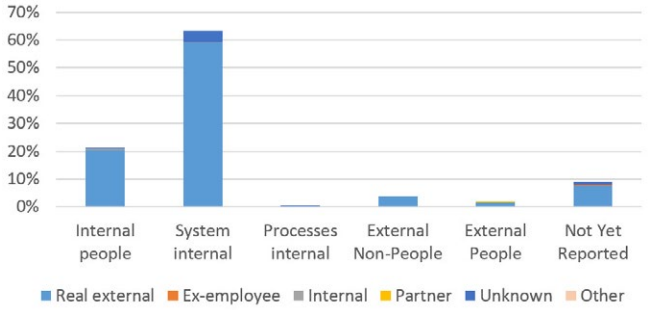


Analysis of Root Cause and Actors

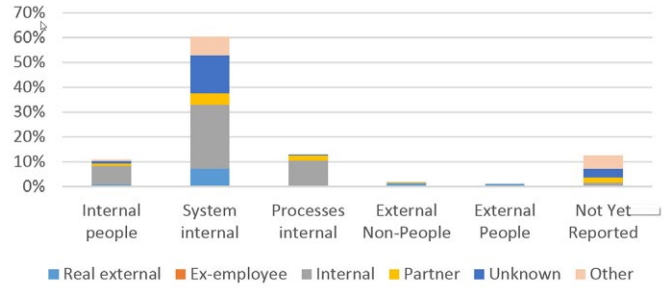
We observe here the distribution of Root Causes split by Actors, in separate views depending on whether the incidents were malicious (attacks, IT-security failure) or non-malicious (errors, IT-system or IT-human failure).

For the malicious attacks, the actors are almost always "Real External" with few being "Unknown" and even fewer being "Internal" and "Ex-employee". For non-malicious events (errors), a clear majority is caused by "Internals", the rest being split over all actors except for "Ex-employee". Should in a future analysis the proportion of "ex-employee" or of "partner" strongly increase, then this would be a clear indication for the need of further actions in these areas.

Malicious: Root Cause split by Actors

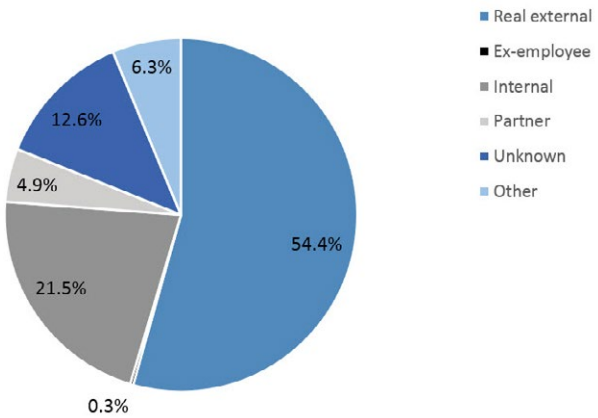


Non-malicious: Root Cause split by Actors



Furthermore an overview of the Actors (malicious and non-malicious together) shows in the pie chart below a clear preponderance for "Real external" (54%) followed by "Internal" (22%) and "Unknown" (13%).

Distribution of Actors



Analysis of Business Impacts, Root Causes and Assets impacted
There are 22 possible Business Impacts covering both first-party and third-party cyber events, including Ransomware and Reputational damages. In the first table below, we show the reported Business Impacts and their split over the five possible Root Causes. Furthermore, in the second table below we show the break-down of the specific Root Cause "System Internal" by Assets impacted. The data captured in this test phase show a strong majority of cases in the "Incident Response" as Business Impact, followed by "Business Interruption (BI)". This is a clear indication for the need of strong Business Continuity as well as carefully prepared Incident Response processes.

Assets impacted (second table) are mainly Servers/Network/Workstation/Terminal, followed by People/Users and Process/ Software.

Root Causes						
People (internal)	18	4	4	12	3	
Systems (internal)	166	27	1	5	0	
Processes (internal)	25	2	1	0	0	
External People	3	0	0	6	0	
External Non-People	1	1	1	2	0	
Not Yet Reported	33	3	5	12	0	
Total	246	37	12	37	3	
Business Impact	BI	Data / SW loss	Financial	Cyber ransom	IP theft	

Root Causes by Asset							
Systems (internal)	Server / Network / Workstation / Terminal	80	29	0	4	0	
Systems (internal)	People / Users	10	0	0	0	0	
Systems (internal)	Media	0	0	0	0	0	
Systems (internal)	Process/ Software	78	2	1	0	0	
Systems (internal)	Data	9	7	0	1	0	
Systems (internal)	External provider	10	0	0	0	0	
	Total	187	38	1	5	0	
Business Impact		BI	Data / SW loss	Financial	Cyber ransom	IP theft	

	64	9	1	2	1	1	0	1	0	2
	241	4	4	5	0	0	2	2	3	2
	1	2	1	1	1	0	0	11	0	0
	9	2	0	1	1	0	0	0	0	0
	3	0	0	2	3	0	0	0	0	0
	17	3	3	6	1	3	3	2	0	0
	335	20	9	17	7	4	5	16	3	4
	Incident response	Privacy breach	Network security	Reputational	Legal - defence	Fines & penalties	Media	Legal - lawyer	D&O	Tech E&O

	220	3	3	0	0	0	0	2	0	1
	209	1	0	0	0	0	1	0	3	0
	0	0	0	0	0	0	0	0	0	0
	14	2	1	5	0	0	1	2	3	1
	3	0	0	0	0	0	0	0	0	0
	1	0	0	0	0	0	0	0	0	0
	447	6	4	5	0	0	2	4	6	2
	Incident response	Privacy breach	Network security	Reputational	Legal - defence	Fines & penalties	Media	Legal - lawyer	D&O	Tech E&O

The total number of incidents in the tables above is amplified, as the tables show all reported impacts, which can be multiple (max three) for the Business Impact field and the Assets field. If we perform a similar analysis on a subset of incidents which ranked the Business Impacts and therefore allows to specifically consider the first reported attribute, we observe that the pattern of Root Causes vs. Business Impacts remains very much the same (first table), whereas the assets impacted (second table) for the Internal Systems are still mainly Servers/Network/Workstation/Terminal but now followed by Process/Software. The abundance in the first analysis above of People/Users affected is mainly due to these entries being made as the second effect in the "Incident response" Business Impact.

Root Causes						
People (internal)	14	1	3	12	3	
Systems (internal)	126	17	0	4	0	
Processes (internal)	25	2	0	0	0	
External People	3	0	0	6	0	
External Non-People	0	0	1	2	0	
Not Yet Reported	0	0	0	0	0	
Total	168	20	4	24	3	
Business Impact	BI	Data / SW loss	Financial	Cyber ransom	IP theft	

Root Causes by Asset							
Systems (internal)	Server / Network / Workstation / Terminal	67	12	0	4	0	
Systems (internal)	People / Users	0	0	0	0	0	
Systems (internal)	Media	0	0	0	0	0	
Systems (internal)	Process/ Software	49	0	0	0	0	
Systems (internal)	Data	1	5	0	0	0	
Systems (internal)	External provider	9	0	0	0	0	
	Total	126	17	0	4	0	
Business Impact		BI	Data / SW loss	Financial	Cyber ransom	IP theft	

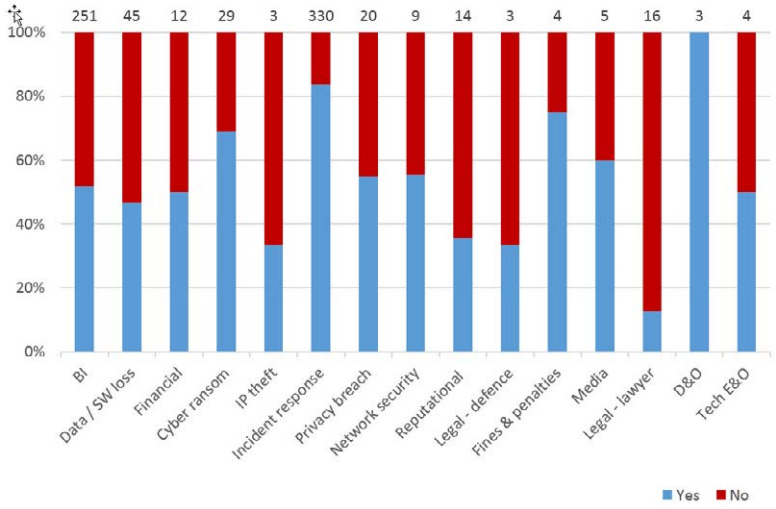
	62	9	1	1	0	0	0	0	0	2
	226	2	3	3	0	0	2	2	0	2
	1	2	1	0	0	0	0	11	0	0
	9	1	0	0	0	0	0	0	0	0
	2	0	0	2	1	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0
	300	14	5	6	1	0	2	13	0	4
	Incident response	Privacy breach	Network security	Reputational	Legal - defence	Fines & penalties	Media	Legal - lawyer	D&O	Tech E&O

	204	1	2	0	0	0	0	2	0	1
	15	0	0	0	0	0	1	0	0	0
	0	0	0	0	0	0	0	0	0	0
	4	1	1	3	0	0	1	0	0	1
	3	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0
	226	2	3	3	0	0	2	2	0	2
	Incident response	Privacy breach	Network security	Reputational	Legal - defence	Fines & penalties	Media	Legal - lawyer	D&O	Tech E&O

Analysis of Business Impacts by Near-Misses criteria

The relative proportion of Near Misses varies greatly by business impact. It is striking to see that especially in the category "Incident Response Costs" the proportion of Near Misses is more than 80%. This might indicate that the entries in this category were done mainly when no other impacts were noticed and not as accompanying impacts beside a more tangible one.

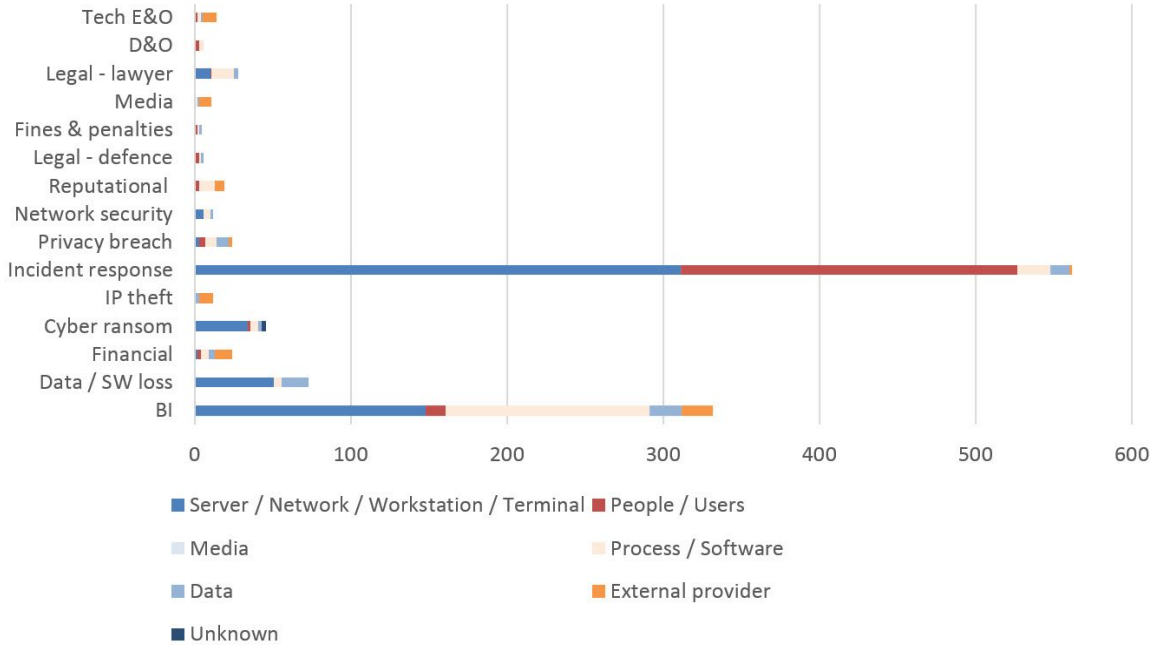
Near miss



Analysis of Business Impact split by Assets impacted

The graph below shows clearly that Server/Network/Workstation/Terminal is the most commonly impacted Asset, independently of the type of Business Impact. For Business Interruption, there is also a fair amount of Process/Application Software impacted. It is surprising to note that for Cyber Ransomware only a marginal number of data assets were impacted.

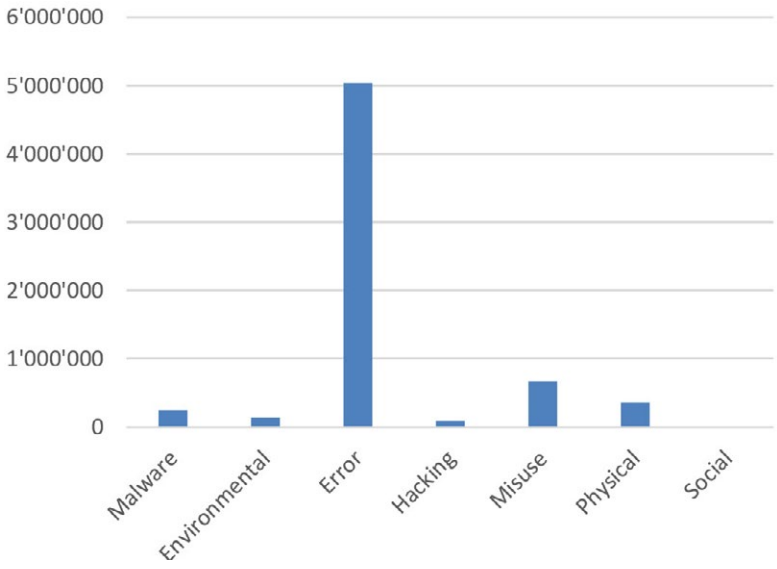
Assets & Business Impact



Analysis of the Financial impact

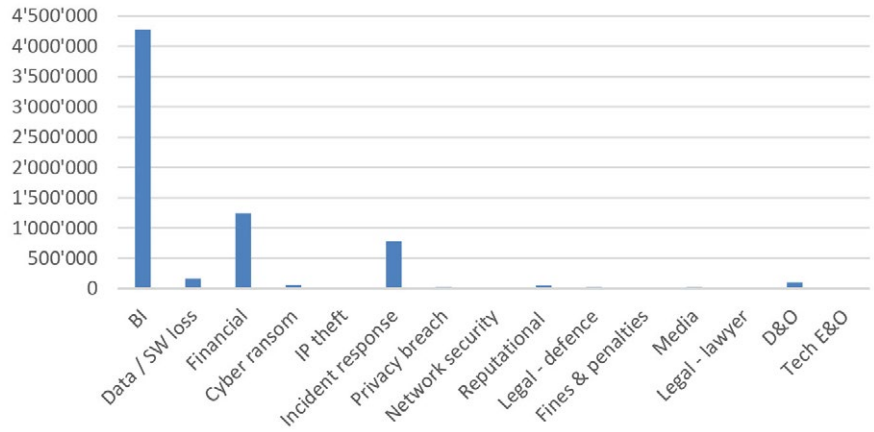
We show here two graphs related to the entries Financial Impact. The first one can be of use for the IT-security function to emphasise which type of Action (by the hacker) created the largest accumulated financial losses. In our data base the Action "Error" is clearly the most impactful in financial terms.

Financial Impact (in EUR) by Action



The second view below will be of more interest to the underwriters, as it can be used – subject to having at disposition a complete (enough) database – for underwriting considerations split by type of policies offered. Here "Business Interruption" has the largest accumulated financial damage.

Financial Impact (in EUR) by Business Impact



Potential challenges uncovered
The analysis of the captured data uncovered some challenges summarised here:

Are some categories being over or under used? Could some overused categories be split to provide greater fidelity?

- The malware category is used in a large number of cases. The provision of only one single malware category means it's not possible to differentiate between incidents involving targeted malware and generic ransomware.

Is there evidence that some fields or categories are being interpreted differently by some contributors such that the aggregate dataset is not consistent?

- There is indication that the interpretation of the definitions of each of the taxonomy fields and the respective categories may not be consistent yet. This enforces the idea that a comprehensive standard and some training on use of the taxonomy with examples is necessary.

Are some contributors reporting difficulty in measuring or determining particular fields?

- CRO Forum members reported difficulty with the root cause field. This is partly because the root cause is not always known and partly because it's not always clear as to one specific root cause as the primary reason.
- Because there are differences in what kind of losses are refunded by the various insurance policies and companies, this is reflected in the financial impact calculation used by the CRO Forum members. Continuing the cyber incident data exchange, a mutual cost calculation and cost description should be defined.

Some contributors may have sourced the data in their submissions from different systems and therefore there may be some translation challenges when submitting events in the CRO Forum taxonomy

- Some members reported sourcing their data from systems which use STIX taxonomy.

To address these challenges and make use of proposed CRO Forum taxonomy, we recommend that organisations need to undertake some preparatory steps including training and understanding the proposed standard behind the taxonomy (as touched on in Section 3) before starting data capturing and reporting to increase accuracy, sharing and ability to undertake consistent underlying analysis.

2.5 CRO Forum taxonomy severity matrix

2.5.1 Evolution of CRO Forum severity matrix

The members of the CRO Forum used an initial matrix for the trial based around the suggestions listed in section 2.5.2.

Consideration was given to whether a common severity matrix could be implemented across all participating companies to aid with the reporting and analysis. However, the conclusion was that even though the severity drivers across the organisations are broadly similar, the severity ratings varied significantly across organisations as nature and size of the each company drives the definition of a significant event. This variation extends both in the type of the rating (days, percentage etc.) and also the appetite for defining what is a high, medium and low risk digital event.

As a result, it is proposed that:
i. Common severity drivers should be utilised; and
ii. Before analysis is undertaken, normalisation of the data pool is necessary.

Initial Severity Matrix

	Definition	High	Medium	Low
Customer Detriment	Best estimate / exact number of clients impacted			
Direct Financial Impact	Unplanned (non-budgeted) adverse impact of P&L	Over XXX M€	Between XX-XXX M€	Under XX M€
Privacy Legislation	Assessment of potential impact on company's internal controls and processes designed to ensure compliance with current and emerging privacy legislation compliance (e.g. GDPR)	Incidents involving external data	Other incidents	
Legal / Regulatory	Litigation expense (annually) and/or Potential for fines or sanctions	> XX M€ annually Most significant fines or sanctions (e.g. loss of licence; closure of business operations)	Between X-XX M€ annually Major fines or sanctions (e.g. suspension of licence)	< X M€ Immaterial fines or sanctions (e.g. increased supervision by / reporting to regulator)
Reputational Impact	Media attention	National to international media coverage, with significant or complete loss of trust and reputation fully impaired or irrecoverable.	Local to national media coverage, with some loss of trust and reputation impacted but recoverable within weeks or months	Local complaint or minimal local media or trade magazine coverage, with minimal or no loss of trust or reputation
Business Interruption / Employee Detriment	Business interruption: additional backlog above tolerance level (monthly)	Above XXX%	Between XX% and XXX%	No backlog / up to XX%
	Employee detriment (or "Productivity impact"): loss of staff (annually)	More than XXX% of staff (annually)	XX to XXX% of staff (annually)	X to XX% of staff (annually)
	"Sales or Distribution impact": delay in strategic plan for a business line	X year	Between X-XX month	No delay / up to X month

2.5.2 CRO Forum suggested severity drivers

The following severity drivers are proposed for the capturing of digital events using the taxonomy.

A. Business Interruption / Employee Detriment

This category includes the impact to the business operations and the employees. The main type of impact utilised is number of days for the first part and percentage of employees affected for the second.

B. Direct Financial Impact

This category shows the direct Income Statement / Profit and Loss impact to the organisation. Methods of quantifying include amounts in specific currency or % of annual Gross Written Premium, Profit, Net Written Premium

C. Legal & Regulatory

This category assesses the cost with respect to legal processes and expenses and also the regulatory implications. The category also includes impact with respect to privacy legislation. Examples of how the impact is assessed include litigation expenses for Legal, fines or specific enforcement under Regulatory and reporting requirements under the Privacy category.

D. Reputational Impact

This category includes the media coverage and reporting obligations following the event. It is mostly assessed as type of media (local, national international) and length of coverage. It also includes reporting obligations such as market updates and press releases to authorities or rating agencies.

E. Customer Detriment

This category includes the impact to the organisation's customers. The rating includes the amount or percentage of customers affected.

2.5.3 Conclusions from CRO Forum trial

In addition to the conclusion documented above, the trial provided useful insight regarding the events identified and their impact. Contrary to expectations, a majority of the events identified had a 'nil' financial impact. This was often due to organisations using existing resources to update preventative controls and remediate incidents.

This supported focus and guidance on how to identify and capture other non-financial impacts. A potential solution being to include non-financial values as the thresholds for digital event reporting.

2.6 Suggestions for improvements

The CRO Forum trial provided evidence on how a common taxonomy can facilitate and enable a collection of digital events that can be utilised to improve risk management and underwriting processes.

The following areas were identified as potential ways of improving the process going forward

A. General Data Protection Regulation (GDPR)

The CRO forum trial acknowledged the recent developments with respect to data protection legislation. It was agreed that once the compliance with the standard advances, there should be additional analysis to ensure the taxonomy is consistent and supports the GDPR requirements. Further refinement may be beneficial to potentially split the category 'breaches of Data Confidentiality' to be explicit on whether the data has been effectively exposed or if it has "just" been illegally accessed .

B. Expansion to additional industries

The members participating in the trial belong to the insurance industry. It was accepted that in order for the taxonomy to realise maximum benefits, it should be expanded to other industries such as banking, manufacturing etc. The CRO forum trial has initiated such an initiative with discussions with the OECD and manufacturing companies such as Airbus. However, it is an area that will require further focus and development.

C. Unity of data

Data collected using the CRO Forum taxonomy should be able to be combined irrespective of the repository used to aggregate and store the anonymised digital event data to allow for a more comprehensive analysis.

D. Normalisation/Calibration of data

As already mentioned earlier, it will be necessary to introduce calibration parameters (such as the corporate's number of employees or turnover) to enable a quantitative underwriting analysis.

Section 3 – Guidance on communication, training and data quality standard

3.1 Background

Effective implementation of a Digital risk event taxonomy requires a number of functions and processes to work in harmony. Breaking down organisational boundaries and establishing a better "connection" between Risk and 1st Line IT is imperative to ensure the timely identification of Digital risk events and this must be supported by frictionless supporting processes.

To fully embed the Digital risk event taxonomy across functions, breaking down organisation boundaries and harmonising disparate processes, will require:

- Data Quality: An agreed and consistently implemented set of Data Quality standards (see Appendix 2). The Data Quality standard should clearly describe what a Digital risk event is, possible root cause(s), their impact(s) and an approach to determining whether these are considered to be material.
- Training: It will be important to ensure that all impacted functions (inc. CISO, IT Operations, Risk and Underwriting) receive suitable training. This training should not just cover the specifics of the Digital risk event taxonomy and Data Quality standard but should also consider this in the context of each functions respective processes and related implications.

This section should be used to help inform the development of a robust communication plan and help organisations shape the activities required to align the key contributing processes necessary to implement and populate the Taxonomy with Digital risk event data.

3.2 Risk events & incident management definition

Risk Events are considered to be the occurrence of an Incident (internal or external) where one or more operational risks materialise due to inadequate or failed processes, people, or systems. Organisations may choose to define Incidents in different ways but four possible types are:

- Assistance: A request from an IT user for support or advice, potentially ranging from things such as gaining or restoring access to a specific system to asking for help to purchase new IT equipment.
- Service Failure (or Compromise): Notification that a given IT service or services are unavailable or not operating as expected. An IT service in this context could relate to a specific system, 3rd party service, data or voice network service etc.
- Data Breach: Identification that there has been a compromise of corporate data. This could relate to a breach in Confidentiality or loss of data (e.g. lost laptop, mobile device, data file), Integrity or corruption of data and Availability or data that cannot be accessed.
- Change Request: Small operational changes can often be accommodated using the Incident Management process. These are those that can generally be completed on first contact and so are limited in scope.

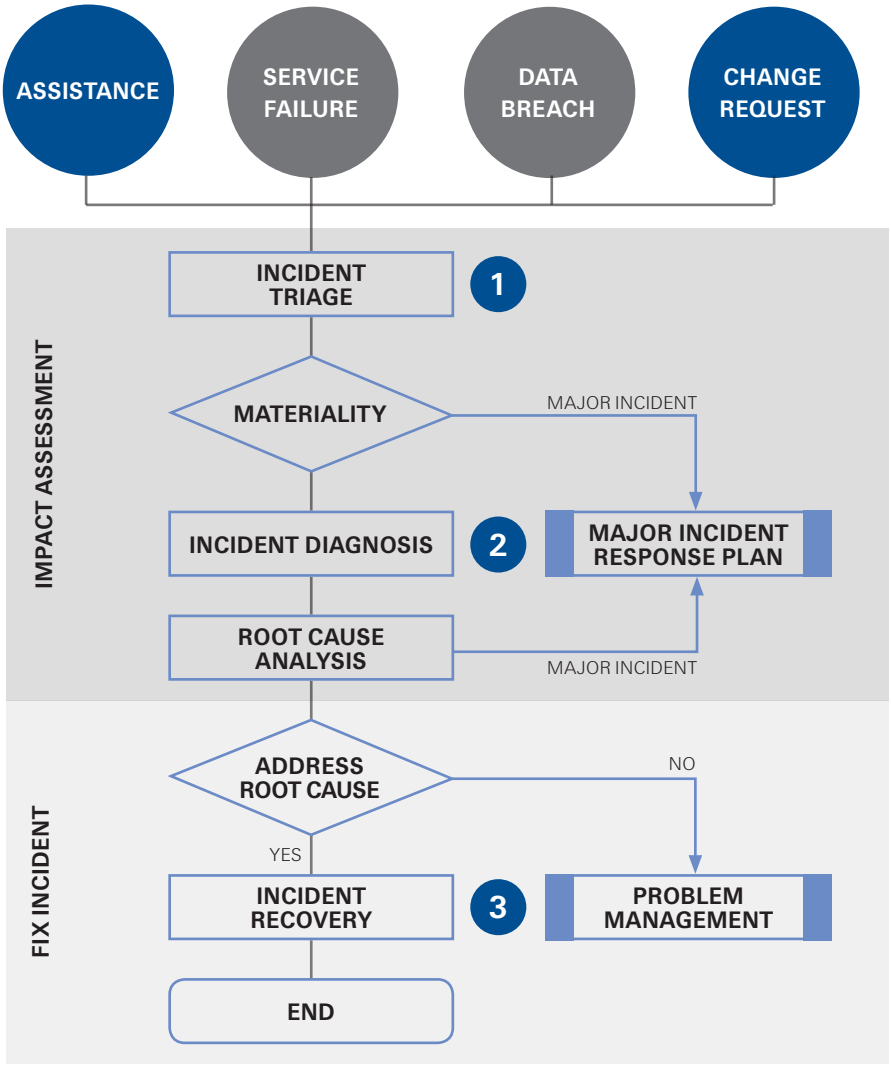
In adopting any Digital risk event taxonomy it is key for the organisation to have considered the relationship between Incident Management & Digital risk event reporting and set its own principles regarding the relationship between the two, irrespective of origin of the Incident.

3.3 Incident management process

Figure A represents a high-level schematic of the Incident Management process through which a range of Incident types can be managed. There are a number of industry recognised standards that describe the Incident Management process (e.g. ITIL or Information Technology Infrastructure Library which is a set of detailed practices for IT service management); however, for the most part they all follow broadly the same set of activities.

In many organisations the Incident Management process is supported through some form of supporting toolset (e.g. ServiceNow, IBM Resilient) and operating model that allows for the efficient and effective management and resolution of the Incident.

Figure A: High-Level Incident Management Process



3.4 What are the key risk event impacting decisions within the incident management process?

- **Step 1 Incident Triage:** An Incident may be identified by a user of a system (internal or external) or through the monitoring of an IT environment; however, irrespective of how the Incident is identified it must at first be captured and assessed. Triage is the first early impact analysis of the Incident to determine who is impacted, the nature of that impact and to determine the relative severity & materiality of the Incident. NOTE: It may be possible at this stage to identify that the materiality of the impact is so severe that it is necessary to invoke the Major Incident Response Plan. **Early determination of Impact and Materiality are key inputs to the Digital risk event reporting process.**

- **Step 2 Incident Diagnosis:** Once the Incident is categorised further detailed analysis of the Incident is completed to, where possible, diagnose the cause of the Incident and determine the appropriate remediation steps to take. The impact analysis is reviewed and in the most severe of cases it may be necessary to invoke the Major Incident Response Plan which could invoke the organisations Crisis Management team and/or Disaster Recovery plans. **Determination of the Root Cause is a key input to the Digital risk event reporting process**

- **Step 3 Incident Recovery:** It is possible that remediation of the Root Cause of the problem is not possible immediately and will need to be managed through an organisations Problem Management process. If this is the case alternative approaches have to be taken to restore Service and/or implement compensating controls to prevent the Incident from re-occurring. **The speed with which the Incident is resolved will influence the level of Impact of the event and determination of short- and long-term remediation actions will drive the overall scale of Loss.**

3.5 Who are the main stakeholders required to support the implementation of the Digital Risk Event taxonomy?

- The effective implementation of the Digital Risk Event taxonomy requires the harmonisation of Incident and, in some circumstances, Problem Management with the Risk Event reporting process. These two processes are, in general, managed by different parts of the organisation that perhaps have historically not collaborated regularly.

First and foremost the Stakeholders responsible for Incident Management, normally:

- Cyber Security (CISO)
- Operational IT Service (IT Operations Director)
- Data Privacy (Data Privacy or Protection Officer)

should be the focus of initial communications activity. This is in addition to the head of 2nd line (Chief Risk Officer) should they not be the sponsor of the initiative.

These Stakeholders should have the ability to lead any required changes to support the effective implementation of the taxonomy and any associated improvements required to the process to improve either the quality of the data collected[1] or its timely use within the Risk Event reporting process.

Strategically, the Chief Risk Office should be the Executive sponsor for more fundamental alignment between processes, particularly if Cyber, IT Service, Data Privacy Incident Management process are disparate following different paths and using different platforms. The minimum aspiration being that all three should have consistent points of integration with the Risk Event reporting process.

[1] Data completeness, quality & timeliness are critical for effective Digital risk event reporting and analysis. The Appendix 2 – Standards & guidelines for digital risk event reporting should be considered and could drive changes into the Incident Management and Digital risk event reporting process described above.

Section 4 – Conclusions and next steps

Main achievement of the trial is the development of a taxonomy that can potentially be used to capture data for better analysis and benchmarking, filling the existing gap of unavailability of digital event/cyber loss data. Companies are asked to engage with this taxonomy, use it and help feed a common digital event database that can fill this gap. This will require within each company the engagement and collaboration of different roles across a number of disciplines such as CISO, IT Operations Director and Data Privacy or Protection Officer.

Furthermore, in a situation in which the global security spending reached more than USD 86.4 billion in 2017, according to Gartner, data captured using this taxonomy can help Boards and top management make informed and timely enterprise-level cybersecurity decisions based on better analysis and benchmarking.

Moreover, beneficiaries also include those involved in Risk Transfer and Insurance coverage that have the challenge of entering a new business, designing new products with very little loss/event history available and evaluating possibilities for risk transfer.

The task fulfilled by the working group wouldn't have been successful without the commitment of all companies involved and a great cooperation and open communication among all participants. The wish for the future, that represents the main challenge as well, is to widen the audience to other industries and institutions in the hope that the work summarised in this document can support a constructive dialogue to a common language for capturing and sharing digital event data.

Consistency and normalisation of the digital event data collected will be an important factor that needs to be considered should the taxonomy be adopted across different industries to ensure capability to undertake valid benchmarking based on the captured event data.
However, reaching other industrial sectors and institutions should help enrich the discussion, address these challenges and potentially the value of the data analysis and contribute towards a better understanding of digital resilience and the improvement of digital security.

Appendix 1 – CRO Forum categorisation methodology for capturing Digital Risk Events

This table provides an overview of all the attributes taken into account in the CRO Forum categorisation methodology for capturing Digital Risk Events. The possible categories within each attribute are also depicted and further described in Appendix 2. In particular, the Root Cause and Event Type attributes –which follow the Basell II categorisation for Operational Risk- are shown here only at "Level 1". Further details on the "Level 2" categorisation are provided in Appendix 2.

Incident Type
Confidentiality
Integrity
Availability
Unknown

Dominant Threshold Triggered
Customer Detriment
Direct Financial Impact
Legal / Regulatory
Reputational Impact
Business Interruption / Employee Detriment

Threshold Rating
Medium
High

Near Miss
Yes
No

Event Type
External Fraud
Employment Practices and Workplace Safety
Clients, Products, and Business Practice
Damage to Physical Assets
Business Disruption and System Failures
Execution, Delivery, and Process Management

Root Cause
People
Systems
Processes
External Causes
Not Yet Reported

Discovery Method
Audit
Security Control
Third Party
User
Monitoring Service
Attacker
Other
Unknown

Action
Malware - Targeted
Malware - Generic
Malware - Unknown
Denial of Service
Environmental
Error
Hacking
Misuse
Physical
Social
Unknown

Asset*
Server
Network
User Device
Data Storage Media
User
Application/ Software
Business Process
External Provider
Data
Smart Device, IoT, ICS
Unknown

Actor Origin
External Actor
Internal Actor
Unknown

External Actor Selection
Ext Actor - Activist
Ext Actor - Nation State
Ext Actor - Organised Crime
Ext Actor - Former Employee
Ext Actor - Force Majeure
Ext Actor - Unaffiliated Hacker
Ext Actor - Terrorist
Ext Actor - Act of war
Ext Actor - Partner
Ext Actor - Other
Ext Actor - Unknown

Malicious Event
Yes
No

Affected Kind of Data*
Customer: PII (Personally Identifiable Information)
Customer: PCI (Payment Card Information)
Customer: PHI (Personal Health Information)
Corporate: Intellectual property
Corporate: Financial Data
Corporate: PII
Corporate: Other
Systems: Authentication
Systems: Published
Systems: Other
Not relevant / None

Financial Impact
Gross loss value
By indicated Business Impact area (up to 3 areas)

Business Impact*
Business Interruption, Interruption of Operations, Loss of Profit
Contingent Business Interruption (CBI) for non-physical damage, Loss of Profit
Data and Software Loss - Restoration, reconstitution
Financial Theft and/or Fraud - Pure financial losses
Cyber Ransom and Extortion
Intellectual Property Theft - Pure Financial Losses
Incident Response Costs
Breach of Privacy, Compensation costs
Network Security/ Security Failure, Compensation costs
Reputational Damage
Regulatory and Legal Defence costs
Fine and Penalties
Communication and Media
Legal protection – Lawyer fees
Assistance coverage – Psychological support
Products
Directors & Officers (D&O)
Technology Errors & Omissions (Tech E&O)
Professional Services E&O, Professional indemnity
Environmental Damage
Physical Asset Damage
Bodily Injury and Death

Status
Open
Closed

Date of Discovery
Discovery date

Occurrence Date
Date of first activity leading to the incident

Currency
Currency options

Impact Location
Country options

Event Description
Free field

Exposure Indicators
Number of Employees
Yearly Turnover
Minimal Financial Threshold

*Field is multiple selection

Appendix 2 – Standards and guidelines for digital risk event reporting

1 Overview

This appendix sets out standards and definitions to support the potential for consistent capture of digital event data.

The standards and definitions are derived from the categories defined in the CRO Forum "Concept Paper on a proposed categorisation methodology for cyber risk" and discussed in Chapter 2.

Certain aspects of an incident will only become apparent over time. The intention is that digital events recorded using the taxonomy can be refined as more becomes known or internal processes are refined.

2 Standards and definitions for digital event data categorisation

2.1 What to Report - Definitions

2.1.1 Digital event or incident

Definition: Digital Event covers:
Any incident

- 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 use of or dependency on electronic data/ systems or cyber-attack;
- 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 and governments.

Cross Reference: The CRO Forum looked into the issues around cyber resilience in the paper it published in 2014[2]. In this paper, cyber risk was defined as the risk of doing business in the cyber environment. In June 2016, the CRO Forum published a concept paper on a proposed categorisation methodology for cyber risk[3]. 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 intention is that all Digital Events or Incidents that meet the thresholds defined in accordance with chapter 2.5 can be captured consistently using the taxonomy and definitions to describe the Digital Event.

2.1.1.1 Near Miss Incidents

Definition: a Near Miss is an incident that occurred, but due to chance did not result in an actual adverse impact on the firm.

There must have been an underlying operational risk event that caused the event (i.e. a control failure). Near Misses shouldn't include circumstances where controls have operated successfully to prevent an incident occurring (e.g. via virus software).
Guidance: Expert / Institutional judgement should take in to consideration the actual circumstances of the Near Miss and given these, should identify the potential realistic outcome that could have occurred (considering previous similar incidents etc.).

Examples include

- A system outage caused by a hack that by chance impacts overnight and doesn't cause business disruption.
- A mass attack of phishing emails that breaches controls, but by chance doesn't cause damage.
- Near misses could also include incidents that, by chance didn't cause an actual impact, but did trigger an incident response or were escalated to senior management / risk committees.

[2] 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/

[3] http://www.thecroforum.org/concept-proposal-categorisation-methodology-for-cyber-risk/

2.1.1.2 Linked Incidents

Definition: A linked incident is a single Digital Risk Incident which has more than one action or impacts more than one location.

2.1.2 Date of Discovery

Definition: The date on which the firm became aware of the incident.

2.1.3 Financial Impact (Gross Loss Value)

Definition: Gross Loss equals the sum of all Profit and Loss (P&L) impacts related to a Digital Risk Incident before recoveries[4]. Operational Risk gains, opportunity losses, and internal costs (overtime, bonus etc.) are not included in the Gross Loss Value submitted to the consortium, although they may be collected internally by member firms.
Guidance: The Gross Loss Value can be indicated for each of the (max three) Business Impacts involved.

2.1.4 Currency

Definition: The Currency in which the Financial Impact is provided.

2.1.5 Status

Definition: Is the Digital Event and/or its categorisation finished?

2.2 Categorising Digital Events

2.2.1 Incident Type

Definition: The Digital Events types correspond to the first observation by the impacted company of the Digital Event, 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.

Table 1 Incident Type

Incident Type
Confidentiality
Integrity
Availability
Unknown

Refer to Section 3, for the full descriptions of the Incident Types.

2.2.2 Event Type

Definition: Event Types represent a description of what happened. The Event Types used by the consortium are as close as possible to the intent of the Basel Committee.

Essentially the Event Type label is a response to the question "What happened to give rise to this Digital Risk Incident financial loss/ business impact?" Why it happened would be part of causal analysis and is outside the scope of the Event Types.

[4] A recovery is an independent occurrence, separate in time from the original incident, in which funds are recovered or contributed, usually from or by a third party.

Table 2 Event Type Level 1 and 2

Level 1	Level 2
Internal Fraud	Unauthorised Activity
	Internal Theft & Fraud
	System Security Internal– Wilful Damage
External Fraud	External Theft & Fraud
	System Security External – Wilful Damage
Employee Practices & Workplace Safety	Employee Relations
	Safe Workplace Environment
	Employment Diversity & Discrimination
Clients, Products & Business Practices	Suitability, Disclosure & Fiduciary
	Improper Business or Market Practices
	Product Flaws
	Selection, Sponsorship & Exposure
	Advisory Activities
Damage to Physical Assets	Natural disasters
	Accidents & Public Safety
	Wilful Damage & Terrorism
Business Disruption and System Failure	Internal System Failure
	External System Failure
Execution, Delivery & Process Management	Transaction Capture, Execution & Maintenance
	Monitoring & Reporting
	Customer Intake & Documentation
	Customer / Client Account Management

Refer to Section 3, for the full descriptions of the Event Types.

2.2.3 Event Description

Definition: This is an explanation of what happened, including any aspects relevant for risk management.

The following aspects may be considered when describing a Digital Event:

- What happened?
- Why did it happen?
- How is the impact calculated? The type of costs that were included in the analysis, plus details of the calculation if necessary (whenever possible within the privacy boundaries).

2.2.4 Country Codes

Definition: The Country Code identifies the country in which the Digital Event occurred.

A 2-letter country code as provided by ISO can be used.
http://www.iso.org/iso/country_codes/iso_3166_code_lists.htm

2.2.5 Action (Threat Actions)

Definition: Threat actions describe what the threat actor(s) did to cause or contribute to the incident.

Table 3 Actions

Action
Malware – Targeted
Malware - Generic
Malware - Unknown
Denial of Service
Environmental
Error
Hacking
Misuse
Physical
Social
Unknown

Refer to Section 3, for the full descriptions of the Actions.

2.2.6 Asset

Definition: The information assets that were compromised during the incident. "Compromised" refers to any loss of confidentiality/possession, integrity/authenticity, availability/utility (primary security attributes). Naturally, an incident can involve multiple assets and affect multiple attributes of those assets.
Guidance: Incidents relating to laptops / mobiles / non-issue personal devices should be reported as "User Devices".

Table 4 Asset Types

Asset
Server
Network
User Devices
Data Storage Media
User
Application/ Software
Business Processes
External Provider
Data
Smart Devices, IoT, ICS
Unknown

2.2.7 Affected Kind of Data (Affected Assets)

Definition: The data affected as a result of the assets compromised and identified in Section 2.2.6 Asset.

Table 5 Affected Kind of Data Types

Affected Kind of Data
Customer: PII (Personally Identifiable Information)
Customer: PCI (Payment Card Information)
Customer: PHI (Personal Health Information)
Corporate: Intellectual Property
Corporate: Financial Data
Corporate: PII
Corporate: Other
Systems: Authentication
Systems: Published
Systems: Other
Not relevant / None

2.2.8 Actor (Threat Actors)

Definition: the entity (person) that caused or contributed to the Digital Event. There can be more than one actor involved in any particular incident, and their actions can be malicious or non-malicious, intentional or unintentional, causal or contributory.

Guidance:

- Actor selection uses a phased approach. The first step is to indicate whether the Actor is External or Internal, or whether this is Unknown. In case an External Actor is involved, the second step asks to select more detail on the External Actor.
- When an External Actor is involved, only categorise an incident to a specific External Actor category if you have evidence to support this. Otherwise, use 'External Actor – Unknown'.
- Only use 'External Actor – Other' when a person is not involved.
- Avoid the use of the 'Unknown' category.

Table 6 Actor Origin

Actor Origin
External Actor
Internal Actor
Unknown

Table 7 External Actor Types

External Actors
External Actor - Activist
External Actor - Nation State
External Actor - Organised Crime
External Actor - Former Employee
External Actor - Force Majeure
External Actor - Unaffiliated Hacker
External Actor - Terrorist
External Actor - Act of war
External Actor - Partner
External Actor - Other
External Actor - Unknown

2.2.9 Root Cause

Definition: This is the initiating cause of (what gave rise to) the Digital Event.

Table 8 Root Cause Level 1

Root Cause Level 1
People
Systems
Process
External Causes
Not Yet Reported

Refer to Section 3, for the full descriptions of the Root Cause Level 2 Categories.

2.2.10 Business Impact

Definition: Any reported Digital Risk Incident will have an impact on the company.

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.

An impact may become an insurance claim if a relevant insurance product has been purchased and covers the type of loss.

Table 9 Business Impacts

Business Impacts
Business Interruption, Interruption of Operations, Loss of Profit
Contingent Business Interruption (CBI) for non-physical damage, Loss of Profit
Data and Software Loss - Restoration, reconstitution
Financial Theft and/or Fraud - Pure financial losses
Cyber Ransom and Extortion
Intellectual Property Theft - Pure Financial Losses
Incident Response Costs
Breach of Privacy, Compensation costs
Network Security/Security Failure, Compensation costs
Reputational Damage
Regulatory and Legal Defence costs (excluding fines and penalties)
Fine and Penalties
Communication and Media
Legal protection – Lawyer fees
Assistance coverage – psychological support
Products
Directors & Officers (D&O)
Technology Errors & Omissions (Tech E&O)
Professional Services E&O, Professional indemnity
Environmental Damage
Physical Asset Damage
Bodily Injury and Death

Refer to Section 3, for the full descriptions of the Business Impacts.

2.2.11 Occurrence Date

Description: The date of the first malicious or causal activity that ultimately lead to the Digital Event.

2.2.12 Malicious Event

Description: A Digital Event may be initiated with the intention of creating harm to a company or individual.

2.2.13 Dominant Threshold Triggered

Description: The Threshold that was primarily triggered to categorise the Digital Event.

Table 10 Dominant Threshold Triggered

Dominant Threshold Triggered
Customer Detriment
Direct Financial Impact
Legal / Regulatory
Reputational Impact
Business Interruption / Employee Detriment

Refer to Section 3, for the full descriptions of the Dominant Thresholds Triggered.

2.2.14 Threshold Rating

Description: The Rating (Medium / High) of the reported Dominant Threshold Triggered.

2.2.15 Discovery Method

Description: The Method in which the firm became aware of the Digital Event.

Table 11 Discovery Method

Discovery Method
Audit
Security Control
Third Party
User
Monitoring Service
Attacker
Other
Unknown

Refer to Section 3, for the full descriptions of the Discovery Methods.

2.3 Exposure Indicators

Exposure Indicators are used to normalise incident data, for example X incidents per XX Employees. As a result, Exposure Indicators are a key element should data be submitted to a third party for anonymous aggregation. Without the Exposure Indicators, it is difficult to benchmark the performance of an individual company to all others providing data.

3 Detailed description

3.1 Incident Type

Incident Type	Description
Confidentiality	Confidentiality refers to limited observation and disclosure of an asset (or data). A loss of confidentiality implies that data was actually observed by or disclosed to an unauthorised actor rather than endangered, at-risk, or potentially exposed (the latter fall under the attribute of Possession and Control). Short definition: Limited access, observation, and disclosure. This also includes possession. Possession refers to the owner retaining possession and control of an asset (or data). A loss of possession or control means that the organisation no longer has exclusive (or intended) custody and control over the asset or is unable to adequately prove it. The concept of endangerment (exposure to potential compromise or harm) is associated with this attribute whereas actual observation or disclosure of data falls under confidentiality. Short definition: Exclusive ownership and control (and ability to prove it).
Integrity	Integrity refers to an asset (or data) being complete and unchanged from the original or authorised state, content, and function. Losses to integrity include unauthorised insertion, modification, manipulation, etc. Short definition: Complete and unchanged from original. This also includes authenticity. Authenticity refers to the validity, conformance, correspondence to intent, and genuineness of the asset (or data). Losses of authenticity include misrepresentation, repudiation, misappropriation, etc. Short definition: Valid, genuine, and conforms to intent.
Availability	Availability refers to an asset (or data) being present, accessible, and ready for use when needed. Losses to availability include destruction, deletion, movement, performance impact (delay or acceleration), and interruption. Short definition: Accessible and ready for use when needed. This also include utility. Utility refers to the usefulness or fitness of the asset (or data) for a purpose. Losses of utility include obscuration and conversion to a less useable or indecipherable form. Utility is distinguished from availability in that the data are still present but no longer (as) useable. Short definition: Usefulness or fitness for a purpose.
Unknown	The incident type is unclear at the time of first reporting the incident

3.2 Event Types

Level 1 Name & Description	
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.	
Level 2 Name & Description	**Examples**
Unauthorised Activity Breaches of authority which are not criminal activity. I.e. employee may be dismissed but not prosecuted. Includes the risk of loss caused by unauthorised employee activities, approvals or overstepping of authority.	▪ intentional mis-marking of positions ▪ Invalid authorisation of exposures or expenditures ▪ Mandate breaches
Internal Theft & Fraud Activity is criminal in nature and would result in prosecution. Includes the risk of misappropriation of assets, collusive and corruptive fraud and financial reporting fraud risk	▪ embezzlement, ▪ claim fabrication ▪ forgery ▪ kickbacks/bribes ▪ extortion ▪ expense reimbursement schemes ▪ payroll schemes ▪ Insider trading for personal gain ▪ deliberate misstatements or omissions of amounts or disclosures of financial statements (e.g. concealed liabilities, fictitious revenues, improper disclosures)
System Security Internal – Wilful Damage Includes the risk of financial loss due to activities going undetected such as unauthorised changes to key security settings, repeated unsuccessful attempts to log into a sensitive system, and insertion of malicious software	Possible activities done by internal employees or within the internal company network: ▪ Theft of data/files information ▪ Unauthorised appropriation of confidential information ▪ Unauthorised change to data ▪ Unauthorised change to applications or systems resulting in data integrity issues, data processing errors, incorrect functionalities and/or to disable monitoring and security functionalities ▪ Computer malevolence (e.g. viruses, files destruction, hacking, denial of service attacks) ▪ Social engineering (e.g. faking the account of a colleague)

Level 1 Name & Description	
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, with the goal of obtaining a personal benefit, damaging the Company or its counterparties (for which the Company pay), or damage Company's assets. Includes 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).	
Level 2 Name & Description	**Examples**
External Theft & Fraud Theft/Robbery of tangible and intangible assets by third parties (without violation of Company system). Fraud by third parties, including customers, vendors and outsource companies, for the purpose of personal economic advantage and causing damage to the Company. This does not include: a) collusion with a member of staff which is considered Internal Fraud b) System related fraud which is categorised as EL0202	■ Theft of Company's assets such as personal computer or vehicles ■ Sale of confidential information to third parties, Industrial espionage, Intellectual property theft ■ Cheques theft ■ Fake claims, ■ Fraudulent surrenders, ■ False certificates or medical records, ■ Fake car theft, ■ Fraudulent estimation of damage ■ Non-existent damaged reported in claims request ■ False witnesses ■ Fraudulent change of beneficiary, ■ Policy written by false agents or false agencies, ■ Misrepresentation on risk assets by customers
System Security External – Wilful Damage Hacking or the attempt to access the Company systems for the purpose of theft, improper use and manipulation of information or to steal or damage data on systems	Possible activities done by externals (e.g. hackers) outside the company network: ■ Theft of data/files information ■ Unauthorised appropriation of confidential information ■ Unauthorised change to data ■ Unauthorised change to applications or systems resulting in data integrity issues, data processing errors, incorrect functionalities and/or to disable monitoring and security functionalities ■ Damage caused whilst gaining access to the company network and spying on the network traffic ■ Computer malevolence (e.g. malware, files destruction, hacking, denial of service attacks) ■ Social engineering (e.g. faking the account of a colleague)

Level 1 Name & Description

Employment Practices & workplace Safety
Events related to mistakes or impermissible actions towards employees in the relationships with the Company, due to the failure to comply with the existing rules, laws, and regulations related to employment relations, internal codes of conduct and due to incidents related to Internal labour disruptions.

Level 2 Name & Description	Examples
Employee Relations Events related to mistakes or impermissible actions towards employees in the relationships with the Company, due to the failure to comply with the existing rules, laws, and regulations related to employment relations, internal codes of conduct and due to incidents related to Internal labour disruptions.	■ Breach of arrangements concerning the protection of a staff member's private life ■ Breach of human resource regulations (labour rights, collective conventions) ■ Employee without any employment contract ■ errors in employment contract ■ change of contract without employee's agreement ■ Recruitment cancelled after contract signed ■ contract termination without justifications ■ lawsuits in case of an employee's illness or injury ■ •lawsuits related to calculation of tax and benefit positions ■ lawsuits related to calculation of salary ■ invasion of privacy
Safe Workplace Environment Events related to employee claims for personal injury and lack of safety in the workplace for employees and third parties, due to the failure to comply with the existing laws on health and safety in the workplace. Under this category falls the failure to comply with mandatory worker insurance programs	■ Employee health and safety rules events (e.g. accidents at work or occupational diseases) ■ Events relating to general liability (e.g. slips and falls of customers, partners or suppliers) ■ Failure to comply with a relevant health and workplace safety regulation ■ Workers compensation
Employment Diversity & Discrimination Events related to workplace equality and discrimination arising under employment laws or internal company rules. Workplace and employment discrimination events should be distinguished from "public" diversity or discrimination events involving clients or citizens in general. The latter should be recorded under the "Improper Business or Market Practices" sub-category.	■ The bullying, harassment, abuse or molestation of a member of staff ■ Lawsuits related to discrimination (related to gender, race, religion, age, nationality, etc.) ■ favouritism towards some employees (hiding their bad behaviour)

Notes

Main features:

- Involvement of employees with the Company's liability (meaning only employees not internal parties as defined in the category ET_01, e.g. agents are excluded)
- The ''Safe Workplace Environment'' category includes third parties involved in events occurred on property for which the Company is responsible

Main distinctions

- Robbery events are excluded (ET_02)
- Disaster events are excluded (ET_05)

Only employees are meant and not the internal parties in general sense as defined for the ET_01.

Level 1 Name & Description	
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.	
Level 2 Name & Description	**Examples**
Suitability, Disclosure & Fiduciary The suitability, information disclosure and fiduciary duty sub-category covers operational risk events arising from regulatory breaches or failures that impact customers, clients or trading partners	■ Shareholder's liability ■ Fiduciary breaches / guideline violations ■ Suitability / disclosure issues ■ Retail consumer disclosure violations ■ Breach of privacy ■ Misuse / non-intentional disclosure of confidential information ■ Aggressive sales, deceptive sales practice, concealment ■ Miss-selling ■ Account churning
Improper Business or Market Practices The improper business or market practices sub-category covers operational risk events arising due to alleged improper business practice.	■ Anti-trust behaviour ■ Improper external reporting practices ■ Improper trade / market practices ■ Market manipulation ■ Insider trading (on the firms account / for the companies benefit. If for individual benefit it is internal fraud) ■ Unlicensed activities whether products or services ■ Money laundering activities ■ Inappropriate discrimination / diversity events in the marketplace or applying to the general public ■ Violation of substantive business contractual reserves ■ Lack of compliance with regulations or industry standards
Selection, Sponsorship & Exposure The selection, sponsorship and exposure sub-category covers events arising due to a failure to properly investigate a client in accordance with internal guidelines or arising due to unplanned costs	■ Losses incurred due to a company exceeding client exposure limits ■ Client fact-finding failures ■ Missing compulsory risk assessment in P&C underwriting (i.e. commercial business)
Advisory Activities The advisory activities sub-category should be used where an operational risk event arises due to a failure to meet obligations.	■ Client is not given the service that they have been led to believe they would receive ■ Inappropriate performance or advisory activity

Level 1 Name & Description	
Damage to Physical Assets Losses arising from loss or damage to physical assets from natural disasters or other events.	
Level 2 Name & Description	**Examples**
Natural disasters Losses to physical assets as a consequence from adverse event from nature or climate.	■ Earthquake ■ Tsunami ■ Flood ■ Storm ■ Hail ■ Storm surge ■ Mudslide ■ Landslide
Accidents & Public Safety Accidents, leading to damage of physical assets, or are a threat to employees or the public. A visitor to the premise is injured as a result of one of these events	■ Fire ■ Explosion ■ Pipe break ■ Malfunction of infrastructure ■ Collapse of buildings
Wilful Damage & Terrorism Damage to physical assets through wilful damage by terrorists or individual or groups.	■ Terrorist attack ■ Arson ■ Explosion (wilful, rather than accidental) ■ Threat to employee wellbeing by a 3rd party ■ Political demonstrations ■ Rioting (civil unrest)

Level 1 Name & Description	
Business Disruption and System Failure 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.	
Level 2 Name & Description	**Examples**
Internal System Failure Loss events associated with the interruption of business activity due to internal system dysfunction, EUC dysfunction or breakdown and/or internal communication system failures and/or the inaccessibility of information and/or loss of data A wholly owned subsidiary managing IT is considered internal	Operational failures due to technology or accidental event. For example: ■ Internal Software failures ■ Internal System unavailability/downtimes due to system bugs ■ Internal System performance problems ■ Internal Server or host performance problems ■ Internal Hardware outages ■ Internal Network outage ■ Internal Loss of data
External System Failure Loss events associated with the interruption of business activity due to external system, external IT supplier failures and/or external communication system failures, and/or unavailability of public utilities	Operational failures due to technology or accidental event. For example: ■ External Software failures ■ External System unavailability/downtimes due to system bugs ■ External System performance problems ■ External Server or host performance problems ■ External Hardware outages ■ External network outage ■ External Loss of data ■ Utility disruptions, external telecommunications network outage ■ Transportation disruptions ■ Pandemic, epidemic related disruptions

Level 1 Name & Description	
Execution, Delivery & Process Management Losses from failed transaction processing or process management, from relations with trade counterparties and vendors	
Level 2 Name & Description	**Examples**
Transaction Capture, Execution & Maintenance	■ Failed mandatory reporting obligation e.g. reporting to Stock Exchanges ■ Inaccurate external report (loss or fine incurred) e.g. quarterly fillings
Customer Intake & Documentation	■ Client permissions / disclaimers missing ■ Legal documents missing / incomplete / not "fit for purpose" / inadequately executed
Customer / Client Account Management	■ Unapproved access given to accounts ■ Incorrect client records (loss incurred) ■ Negligent loss or damage of client assets

3.3 Actions

Name	Description
Malware-Generic	Generic Malware is any malicious software, script, or code run on a device that alters its state or function without the owner's informed consent. It is broadly applicable and it's operators intend for it to be spread as widely as possible to maximise victims. Examples include viruses, worms, spyware, keyloggers etc.
Malware-Targeted	Targeted malware is often customised to a particular victim and associated with threat actors who actively pursue and compromise a target entity's infrastructure. Malware-Targeted attacks often employ similar methods found in traditional online threats such as malicious emails, compromised or malicious sites, exploits, and malware. However they are usually conducted as campaigns to get deeper into the target´s network, they target specific industries and have long-term goals and motives in mind.
Malware-Unknown	Malware which purpose can't be determined
Denial of Service	Attack to make a machine, network resource, website or user account unavailable
Environmental	The Environmental category not only includes natural events such as earthquakes and floods, but also hazards associated with the immediate environment or infrastructure in which assets are located. The latter encompasses power failures, electrical interference, pipe leaks, and atmospheric conditions.
Error	Error broadly encompasses anything done (or left undone) incorrectly or inadvertently. Includes omissions, misconfigurations, programming errors, trips and spills, malfunctions, etc. It does NOT include something done (or left undone) intentionally or by default that later proves to be unwise or inadequate.
Hacking	Hacking is defined within VERIS as all attempts to intentionally access or harm information assets without (or exceeding) authorisation by circumventing or thwarting logical security mechanisms. Includes brute force, SQL injection, cryptanalysis, etc.
Misuse	Misuse is defined as the use of entrusted organisational resources or privileges for any purpose or manner contrary to that which was intended. Includes administrative abuse, use policy violations, use of non-approved assets, etc. These actions can be malicious or non-malicious in nature. Misuse is exclusive to parties that enjoy a degree of trust from the organisation, such as insiders and partners.
Physical	Physical actions encompass deliberate threats that involve proximity, possession, or force. Includes theft, tampering, snooping, sabotage, local device access, assault, etc.
Social	Social tactics employ deception, manipulation, intimidation, etc. to exploit the human element, or users, of information assets. Includes pretexting, phishing, blackmail, threats, scams, etc.
Unknown	

3.4 Root Cause

Level 1 Name	Description
People	**Actions arising from individuals within the firm**
Level 2 Name	**Description**
Employee qualification, technical skills, competences	■ Inadequate identification of competences required for an organisational role ■ Ineffective evaluation of personnel competences and technical skills ■ Inadequate recruiting and selection of human resources ■ Inadequate personnel training ■ Lack of internal risk awareness such as insecure disposal, lack of clean policy, missing data classification, etc.
Employee availability (composition of team, overwork, illness)	■ Capacity problems ■ Inadequate workforce planning
Employee conduct (lack of: motivation, integrity, honesty)	■ Inadequate mobility plans, job rotation plans ■ Inadequate identification of talents and key personnel ■ Inadequate verification of references and ethical profile of the applicant ■ Inadequate valuation of human resources performances ■ Inadequate incentives and compensation systems ■ Lack of due care such as insecure disposal, lack of clean policy, missing data classification, etc.
Human error, oversight error	■ Misunderstanding, exceeded deadline, incorrect data input or storage of data ■ Inadequate diffusion of control culture ■ Transfer of confidential data to the wrong recipient ■ Loss of confidential data (e.g. user device) in public area
Other	

Level 1 Name	Description
Systems	
Level 2 Name	**Description**
Insufficient IT/Infrastructure, hard- and software availability, capacity	■ Including software or programming errors ■ Lack/inadequacy of maintenance and updating of IT infrastructure (hardware or software) ■ Inadequate technical support - Lack/inadequacy of appropriate measures and processes for reporting IT failures, for managing incidents and data security issues ■ Lack/inadequacy of IT infrastructure (software or hardware) licensing management ■ Lack of capacity management (e.g. application sizing, workload mgmt. demand mgmt. capacity planning, resources mgmt., performance mgmt.)
Insufficient IT/Infrastructure security	Insufficient or missing IT/Infrastructure controls. For example: ■ Insufficient network controls, malware detectors, building and facility security controls ■ Missing or inappropriate security architecture/configuration (e.g. security patches) ■ Missing secure functionalities and/or tools (e.g. encryption functionality for confidential data) ■ Missing IT services and/or IT solutions leading into use of public unsecure IT services (e.g. unmanageable cloud services, google translator, public storage, etc.) ■ Lack/inadequacy of security monitoring ■ Lack/inadequacy of measures for controlling logical access and for tracking activities/ operations ■ Lack/inadequacy of backup procedures of archives and software ■ Lack/inadequacy of a disaster recovery plan
Insufficient supply (energy, electricity, telecommunications, etc.)	■ Outages of telecommunication, outlook outages - Inadequate selection and management of telecommunication infrastructures and utility service ■ Lack/inadequacy of maintenance and technical support for the telecommunication infrastructure and utility service
Other	

Level 1 Name	Description
Processes	
Level 2 Name	**Description**
Inadequate process/control design and workflows	▪ Organisation, clarity of roles and responsibilities, too many interfaces, complexity, insufficient product development, inadequate project management, quality management, change management ▪ Lack of alignment between IT and Business Strategy (e.g. keeping outdated legacy systems and "toxic" IT components) ▪ Missing clear definition and categorisation of problems and incident ▪ Inadequate evaluation of a problem and/or incident ▪ Inadequate procedure to handle a problem and/or incident
Inadequate process/control documentation, procedures, policies -	▪ Including escalation procedures, ambiguous assignment of tasks, competencies or responsibilities (e.g. inadequate incident management process, inadequate problem management process, etc.) ▪ Inefficiencies in the measurement and reporting of process performances
Inadequate business continuity & crisis management	▪ Inappropriate plan, inappropriate recovery site (e.g. too near to main office), lack of regular testing, lack of proper communication plans. ▪ Lack of business continuity plan related to human resources.
Inadequate vendors/outsourcing agreements & management	▪ Inadequate preliminary evaluation of the nature and importance of activities to be outsourced. ▪ Inadequate outsourcing contracts and monitoring of Service Level Agreements (SLA).
Inadequate data quality	▪ Data pollution within a system (duplicate and inconsistent records) ▪ Data inconsistency between systems ▪ Missing data
Lack of automatisation	▪ Insufficient end-user computing management, manual interfaces and hand-offs. ▪ Excessive use of spreadsheet.
Other	

Level 1 Name	Description
External Causes	
Level 2 Name	**Description**
Natural disaster	▪ Flood, fire, storm, earthquakes, etc.
Epidemic/Pandemic	▪ Diseases
Default/Misconduct of third party (vendor/service provider/ outsourcer)	▪ Includes fraud and bankruptcy of a third party, counterparty, provider.
Inferior quality or unsatisfactory adherence to delivery deadlines of a third party	▪ Outsourcer, vendor, service provider or counterparty, actions or inaction.
Man-made catastrophe	▪ Terrorism, vandalism, criminal acts, etc.
Changes in political environment	▪ Strikes, civil war.
Changes in legal or regulatory environment or practices	▪ Unfavourable court decisions, retroactive changes of law.
Client fraud	▪ Claims fraud. Premium fraud - the intentional concealment or misrepresentation of information when obtaining insurance
Intermediary fraud/misconduct	▪ Fraud, misconduct, data leakage, mis-selling of sales intermediaries like brokers, financial advisors where the company is liable for.
Others	

3.5 Business Impact

Name	Description
Business Interruption, Interruption of Operations, Loss of Profit	Coverage scope: Reimbursement of lost profits caused by a production interruption not originating from physical damage.
Contingent Business Interruption (CBI) for non-physical damage, Loss of Profit	Coverage scope: 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.
Data and Software Loss - Restoration, reconstitution	Coverage scope: 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.
Financial Theft and/or Fraud - Pure financial losses	Coverage scope: 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.
Cyber Ransom and Extortion	Coverage scope: 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).
Intellectual Property Theft - Pure Financial Losses	Coverage scope: loss of value of an Intellectual Property asset, resulting in pure financial loss.
Incident Response Costs	Coverage Scope: Compensation for crisis management/remediation actions requiring internal or external expert costs, but excluding regulatory and legal defence 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
Breach of Privacy, Compensation costs	Coverage scope: compensation costs after leakage of private and/or sensitive data, including credit-watch services, **but excluding incidents response costs.**
Network Security/Security Failure, Compensation costs	Coverage scope: 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.
Reputational Damage	Coverage scope: compensation for loss of profits due to a reduction of trade/clients because they lost confidence in the impacted company.
Regulatory and Legal Defence 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 Defence costs: coverage for own defence costs incurred to the observed company or related third-parties facing legal action in courts following a cyber-attack**.**
Fine and Penalties	Coverage scope: Compensations for fines and penalties imposed on the observed company. Insurance recoveries for these costs are provided only in jurisdictions where it is allowed.
Communication and Media	Coverage scope: 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.
Legal protection – Lawyer fees	Coverage scope: 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.
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
Products	Coverage scope: 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.

Name	Description
Directors & Officers (D&O)	Coverage scope: 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.
Technology Errors & Omissions (Tech E&O)	Coverage scope: compensation costs related to the failure in providing adequate technical service or technical products resulting from a cyber-event.
Professional Services E&O, Professional indemnity	Coverage scope: 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).
Environmental Damage	Coverage scope: compensation costs after leakage of toxic and/or polluting products consecutive to a cyber-event.
Physical Asset Damage	Coverage scope: 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.
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).

3.6 Dominant Threshold Triggered

Severity Driver	Characteristics for consideration
Customer Detriment	■ Impact of incident on Customers – considering a % or number of customers (thresholds depends on size and type of insurance business). ■ Financial loss to customers in aggregate or as a percentage of income. ■ Number of complaints received from customers. ■ Type and scale of non-financial detriment to customers. ■ Breaches of customer Service Level Agreements (SLAs).
Direct Financial Impact	■ Adverse impact on P&L
Legal / Regulatory	Based on the volume and type of data breach, as well as level of public declaration: ■ Size of litigation loss or regulatory sanction (financial, reputational or business impact). ■ Qualitative regulatory threshold – internal severity definition. ■ Regulatory notification level (e.g. Group vs. local regulator). ■ Type of regulatory action, i.e. notifications, investigations or enforcement action.
Reputational Impact	■ Qualitative thresholds defined in line with those suggested in CROF December Paper (i.e. level of media / social media coverage from local to international coverage). ■ Qualitative thresholds considering the level of response required to an incident (e.g. global press release, client communication etc.). ■ Number of customers lost as a result of a specific incident. ■ Impact on an organisation's share price as a result of an incident (e.g. size of movement).
Business Interruption / Employee Detriment	■ Loss of productivity, including system downtime, backlog increases, project delays and / or employee hours lost as a result of an incident. ■ Impact on sales, such as impact on the sales plan (e.g. delay, loss of sales or loss of profit). ■ Impact on employees, such as reduction in morale, an increase in turnover or reduction in productivity. ■ The requirement to trigger an incident or business continuity response. Whereas there is not an expectation that a specific value is calculated for the 'opportunity cost' of an incident, the above or other related thresholds should be included in participants' matrices and should be considered in the identification and reporting of incidents (including Near Misses).

3.7 Discovery Method

Name	Description
Audit	■ Internal and/or external audit ■ Technical expertise review
Security Control	■ Warning, alert or notification coming up from a security control (e.g. malware defence or access control tools) ■ Secure Configurations Review
Third Party	■ Customer or Clients ■ Service Provider ■ Others
User	■ Business User ■ IT User
Monitoring Service	■ Audit Logs Review ■ Operational Failure Logs Review
Attacker	■ Hacker
Other	■ Other Discovery Method not mentioned above
Unknown	■ The Discovery Method is not known

Order no: 150709x_18_EN

CRO FORUM

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