1 ORX News: coverage of cyber crime and data breaches

1.1 Instruction and FAQs document

Due to demand from subscribers, ORX News is increasing its coverage of significant cyber crime losses and data breaches at non-financial services firms. This document outlines the coverage. See section 2.1 of ORX News coverage rules for more information.

1.1.1 Coverage summary

ORX News cyber coverage thresholds summary		
Scenario category	**Financial services firm**	**Non-financial services**
Cyber data breach	no lower limit	>1 million records
Cyber business disruption	no lower limit	not covered unless particularly noteworthy or example of new type of business disruption
Cyber-related fraud	if there is reasonable evidence that there is over $1 million loss to bank or customer, or if there is something novel about the fraud.	> $1 million loss

1.2 What is a cyber event?

Penetration of a firm's IT Security defences that results in sensitive information being stolen. Includes access of customer personal identifying information from 3rd party vendors and retailers where customer card details may be stored.

or

Penetration of a firm's IT Security defences, from either external or internal actions, or theft of customer account details from third party vendors or retailers that results in the fraudulent removal of funds from customers' accounts, or payment systems.

or

Disruption to IT systems, mainframes or services caused by perpetrators infiltrating, or denying access to, computer systems, such that it prevents the firm from conducting normal operations.

These events may have multiple impacts, including data loss, direct financial losses and regulatory fines, including those relating to any breaches of data protection legislation such as the European Union's General Data Protection Regulation (GDPR).

1.3 Does ORX News include cyber events from non-financial firms?

Yes.

For the purposes of this document, non-financial firms include accountancy companies and credit ratings agencies. We will also cover related topics of interest. See the table below for a summary.

Financial services company examples	**Non-financial services company examples**
Bank Insurer Asset Manager Cryptocurrency platform Third party payments processor, eg credit card payments processor	Retailer Accountancy firm Credit ratings agency Management consultancy Computer Manufacturer Cloud computing provider

1.4 What are the thresholds for the inclusion of these cyber losses?

Data breaches – over 1 million records compromised, where a record will typically include a name, an email address or physical address for an individual, plus other information. Records do not necessarily include usernames and passwords or financial records.

Direct financial loss – over USD 1 million of operational risk losses attributable to the firm, as reported in reputable media, or confirmed by the company or law enforcement.

> *(nb these thresholds were changed on 1 October 2018 from 10 million records compromised and/or direct loss of USD 10 million. This is to provide more data points for analysis of cyber losses in the ORX News database).*

Denial of Service attacks (DDOS) – very significant disruption, ie website completely disabled for over 24 hours, company unable to conduct web-based business, customer contact or content distribution for over 24 hours.

For non-financial companies, we will not cover disruption to IT systems, unless the disruption is as a result of malicious cyber activity AND is particularly noteworthy or example of new type of business disruption.

Flexibility is allowed. For example, if a cyberattack utilises a novel form of malware or a new approach, ORX News may chose to cover the event as it will be of interest to risk managers. ORX News will continue to focus on attacks on firms, rather than individuals.

Coverage according to these thresholds will commence on 1 January 2018.

1.5 How can I filter these losses out of the data?

On the CSV export, you can use column D “Industry Sector” to filter out “Non-financial services company” to remove these losses. (see figure 1)

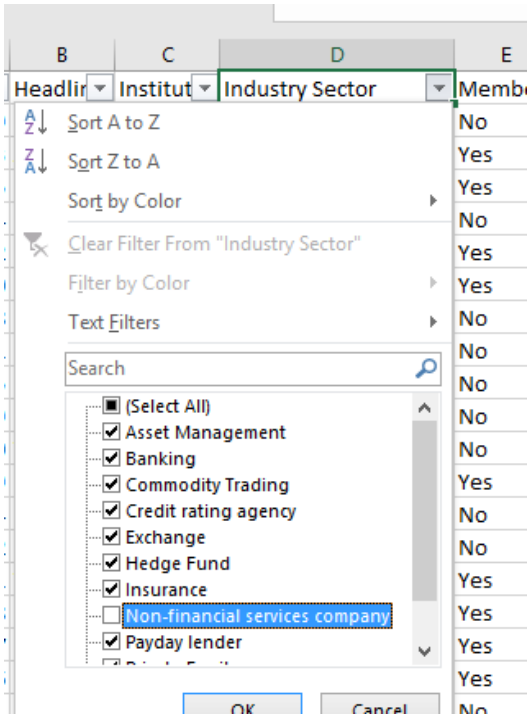

Figure 1 Menu selection to remove non-financial services company cyber losses from ORX News CSV data export

1.6 How are these losses categorised?

To fit into the ORX News database, some fields such as product must be populated, even if they are not directly relevant to a non-financial services firm.

Categorisation will be as follows:

Category	**Options for cyber events at non-financial services firms.**
Business Line	BL1001 – Corporate Items
Event Type	EL0202 – System Security External – Wilful Damage EL0201 – External Theft & Fraud if money is taken EL0401 – Suitability, Disclosure & Fiduciary if data is accidentally exposed on an Internet connected server such as a cloud services server.
Scenario Category	SC0023 – Cyber-Related Data Breach or SC0024 – Cyber-Related Fraud or SC0025 – Cyber-Related Business Disruption For data left exposed on publicly accessible servers, SC0011 – Data Breach
Product	PD9900 – Not Product Related
Process	PC9900 – Not Process-Related
Alleged Cause	CS0102 Assault by Criminals / Terrorists, CS0503 Software – Inadequate Maintenance
Boundary Risk	Other Risk
Jurisdiction	LS0106 - Unidentifiable
Counterparty Claimant	LS0212 – Not identifiable
Role of Firm	LS0308 – Not Identifiable
Environmental Volatility	LS0406 – Not Identifiable
ORX Standard	Banking
Loss Amount	Recorded

1.7 What about cyber events at financial firms?

The above policy applies to cyber events at non-financial firms.

We will cover a cyber fraud at a financial firm if the loss amount or amount reported stolen is over USD 1 million.

Financial services firms will include every value in Column D of the CSV export (industry sector) *except* "Non-Financial Services Firm".

We will cover data breaches of any size at a financial firm (and 3rd parties/outsourcers), if they are reported in reputable media sources.

We will cover cryptocurrencies such as Bitcoin in a similar way to financial institutions. This means that we will also cover any cyber losses or breaches that impact cryptocurrency exchanges or similar institutions, for example if a firm underwriting an initial coin offering (ICO) suffers an operational risk event.

For financial firms, we will cover business disruption, such as an IT outage, if the service is unavailable for four hours or more. If the disruption is less than 4 hours, we will not cover in ORX News.

For business disruption, we will cover if online banking services, mobile banking services or transaction systems are unavailable for more than 4 hours, even if the cause of the outage is not reported.

We will cover disruption to a bank's website (not including its online banking system) if the cause is reported as hacking (rather than a datacentre failure or other non-cyber cause).

1.8 Revision history

Version 1, 13 December 2017

Version 2, 1 October 2018, Includes information on recording loss amount in non-financial services firms, and reducing the threshold for collection of losses in non-financial firms from 1 October 2018 from 10 million records lost and/or USD 10 million losses to 1 million records lost and/or USD 1 million in losses

Version 3, 6 November 2018. Section 1.7 revised, cyber fraud covered if loss amount is over USD 1 million. Previously this coverage document had erroneously said that all events were covered, even if no loss amount. Summary table in section 1.1.1 added.

Version 4, 13 December 2018. Section 1.4 revised. "AND is particularly noteworthy or example of new type of business disruption" added to business disruption in non-financial services companies. Event Type EL0401 added to categorisation table in Section 1.6 to cover data exposure events.

Version 5, 16 January. Section 1.6 revised. Scenario Category – SC0011 – Data Breach included as an option for data left accidentally exposed on publicly accessible servers.