Swiss Re

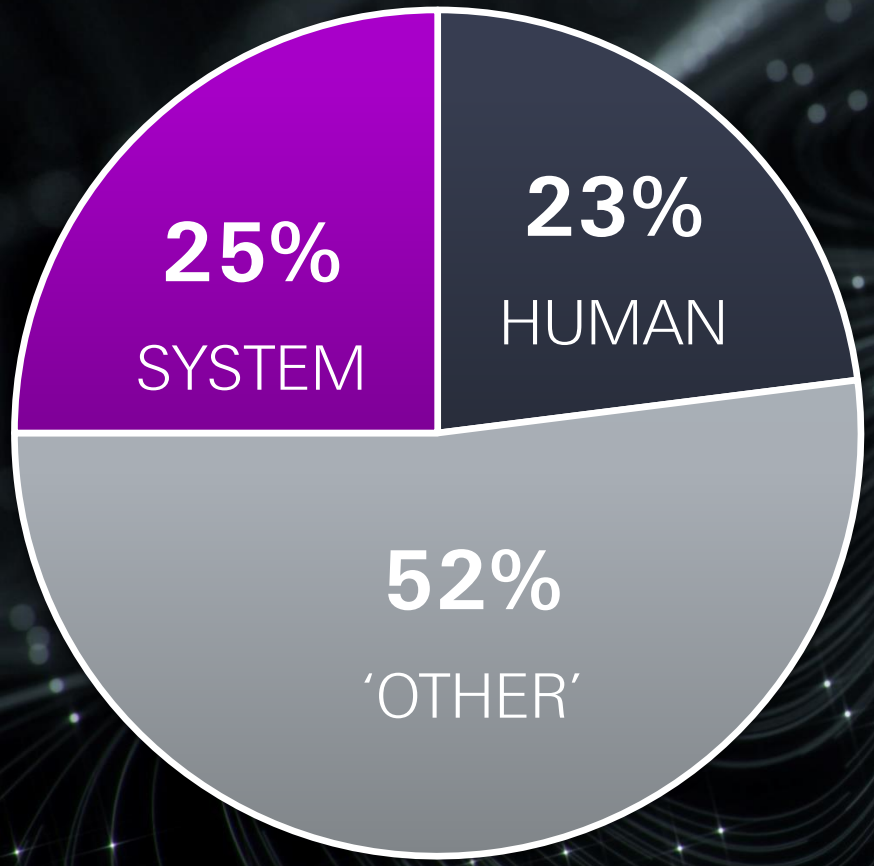
EMEA Contracts Expert Circle 2022

Shaping Contracts for a Resilient Future

Cyber Guiding the Future – Resilient Products

Brett Nakano, Peter Wedge, Swiss Re

Table of Contents



Source: IBM Cost of a data breach 2020

WHO/WHY

- Hacktivists
- State-sponsored

Political / religious

Rogue / disgruntled employee

Revenge / personal gain

Cyber Criminals

Financial gain

- Script kiddies
- Nerds
- White Hats

Fun / educational

HOW

<CRYPTOJACKING>

<PHISHING>

<SOCIAL ENGINEERING>

<MALWARE>

<RANSOMWARE>

<TROJAN HORSE>

<DDoS>

<...>

Standard cyber coverage elements in the direct market

Affirmative cyber cover

1st party cover

- ✓ Social engineering
- ✓ Crisis management costs (IT forensics, notification, public relations, credit monitoring, legal)
- ✓ Extortion/Ransom payment
- ✓ Data restoration
- ✓ Business interruption (BI)
- ✓ Contingent business interruption (IT CBI)
- ✓ Legal costs to defend a regulatory investigation
- ✓ Regulatory fines (if insurable by law)

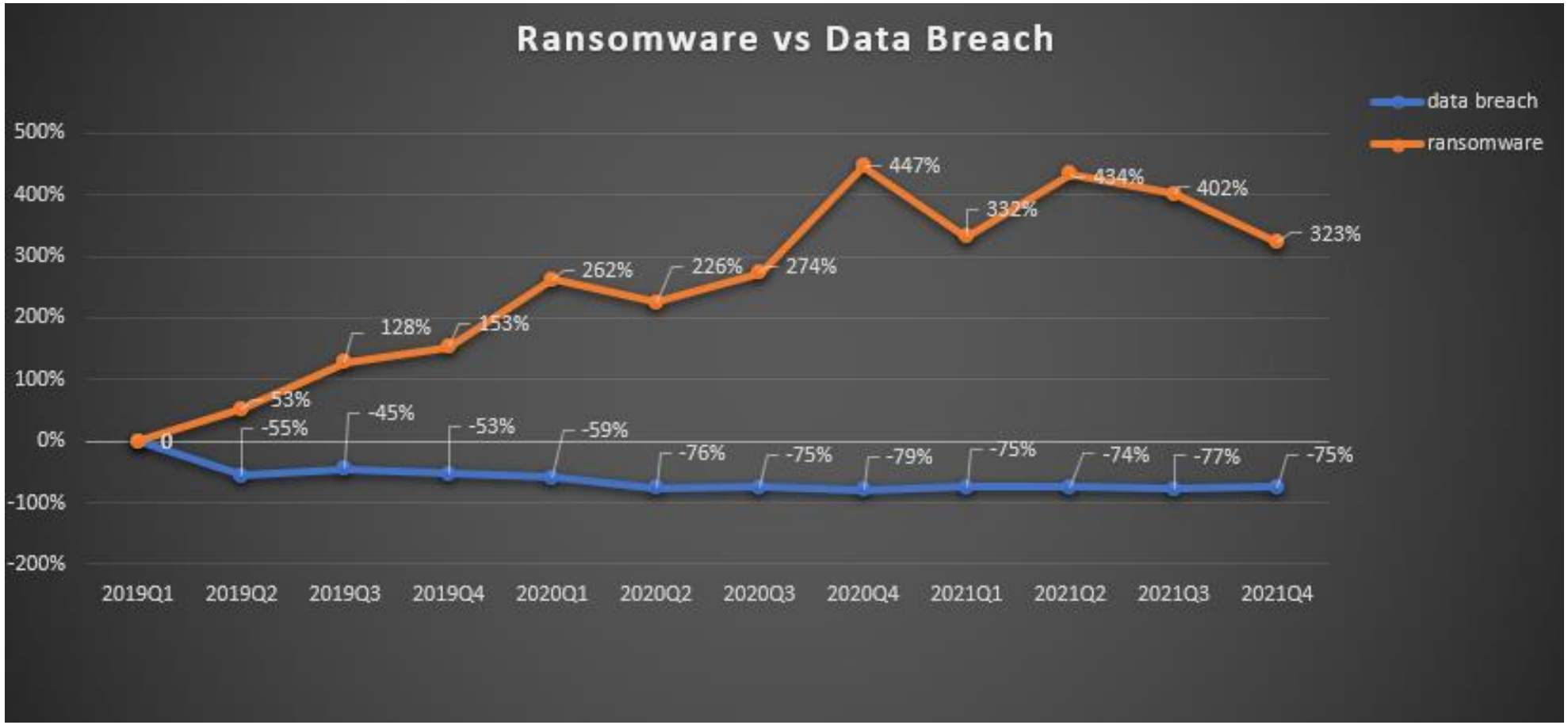
3rd party cover

- ✓ Privacy liability
- ✓ Network security liability
- ✓ Communication and media liability

Frequent exclusions

- ☒ War
- ☒ Bodily injury
- ☒ Property damage
- ☒ Intellectual property, patent infringement, trade secret misappropriation
- ☒ Critical Infrastructure

Ransomware versus Data Breach incident rates – since 2019

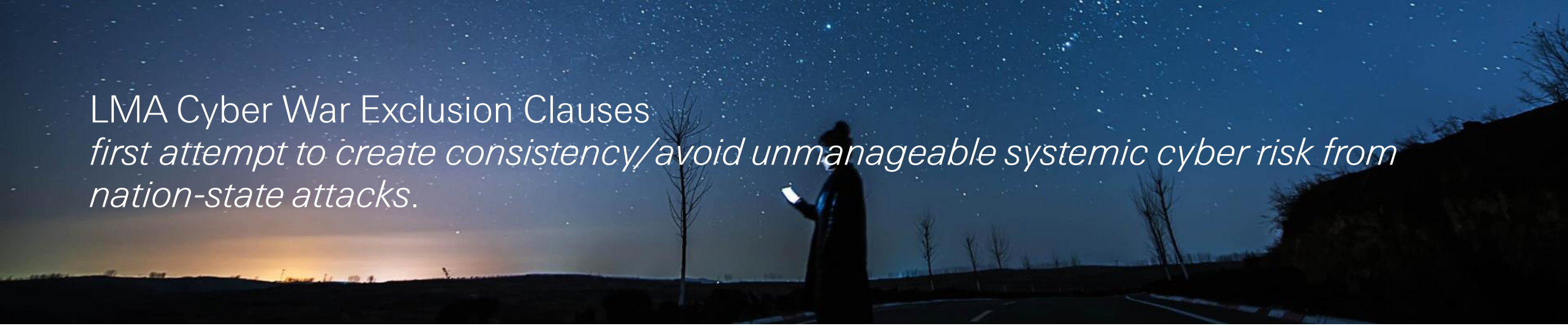


Source : Aon

Supply chain breach: “a cyber hurricane”? *Cyber cat aggregation*?

LMA Cyber War Exclusion Clauses

- **Status quo: NMA 464 (or similar) + “Cyber Terror writebacks”**
- NMA 464 (1/1/1938):
  - “Notwithstanding anything to the contrary contained herein this Policy does not cover Loss or Damage directly or indirectly occasioned by, happening through or in consequence of war, invasion, acts of foreign enemies, hostilities (whether war be declared or not), civil war, rebellion, revolution, insurrection, military or usurped power or confiscation or nationalisation or requisition or destruction of or damage to property by or under the order of any government or public or local authority.
- Example **Cyber Terrorism writebacks:**
  - “However, this (terror) exclusion shall not apply to ‘Cyber Terrorism’”
  - “However, this (terror) exclusion does not apply to a cyber event affecting your critical systems or a technology supply chain partner’s computer systems.
  - Cyber terrorism: ... any act or threat of force or violence (against your computer system) by an individual or group ... committed for political, religious, ideological or similar purposes ...



LMA Cyber War Exclusion Clauses

first attempt to create consistency/avoid unmanageable systemic cyber risk from nation-state attacks.

LMA5564

Aims to exclude all "war" and all nation-state "cyber operations"

LMA5565 & LMA5566

Aims to exclude all "war", nation-state "cyber operations" above an impact threshold, and retaliatory cyber operations between major powers

LMA5565 - Coverage limits can be specified for losses stemming from cyber operations below those thresholds

LMA 55666 - Coverage limits CANNOT be specified for losses stemming from cyber operations below those thresholds

LMA5567

Identical to LMA5566 but with a write-back for "bystanding cyber assets".

Losses borne by insureds who are located outside of an "impacted state" are not excluded (*e.g. where Ukraine is deemed to be the impacted state, NotPetya losses for insureds outside of the Ukraine – e.g. USA - are not excluded*)

LMA5564 (No.1) *Broadest exclusion*	LMA5565 (No. 2)	LMA5566 (No. 3)	LMA5567 (No. 4) *Narrowest exclusion*
War (all)	War (all)	War (all)	War (all)
Cyber Operations ('CO') - (all)	1.1. CO in the course of war	1.1. CO in the course of war	1.1. CO in the course of war
	1.2. Retaliatory CO b/w Specified States	1.2. Retaliatory CO b/w Specified States	1.2. Retaliatory CO b/w specified states leading two or more sp. states becoming Impacted States
	1.3. Major Detrimental Impact CO (Sub-limits for "any other" CO)	1.3. Major Detrimental Impact CO	1.3. Major Detrimental Impact CO (except for effect of CO on a Bystanding Cyber Asset)

Interplay with the Critical Infrastructure Exclusion

- Three connected tools to deal with unmanageable systemic cyber risk:
  1. the infrastructure exclusion, which excludes all losses stemming from cyber attacks against critical infrastructure such as power networks.
  2. the war exclusion
  3. other wide-event restriction language being developed by some of the leading cyber insurers
- There has been research on the need for the public sector to prepare itself for systemic risk that the insurance market is unable to provide cover for, but no solutions so far.

Two schools of thought about adding a cyber war clause with obvious flaws.

Any questions?

Swiss Re

Thank you!

Contact us

Peter Wedge
Reinsurance Contracts Counsel
peter_wedge@swiss re.com
+41797780182

Brett Nakano
Senior Casualty Treaty U/wr
Brett_Nakano@swissre.com
+81 3 5219 7927

Follow us

Legal notice

The information and opinions contained in the presentation are provided as at the date of the presentation and may change. Although the information used was taken from reliable sources, Swiss Re does not accept any responsibility for its accuracy or comprehensiveness or its updating. All liability for the accuracy and completeness of the information or for any damage or loss resulting from its use is expressly excluded.