Cyber – Threat and Opportunity

8th Conference on Global Insurance Supervision

Dr. Jürgen Reinhart
Chief Underwriter Cyber

Munich RE

Cyber Security in 2022

Some stats, facts and noteworthy developments

Munich RE

Global cyberattacks across all sectors increased by **38%** in 2022, compared to 2021.
(Checkpoint research)

The global cost of cybercrime is expected to surge in the next five years, rising from **$8.44 trillion** in 2022 to **$11 trillion** in 2023, reaching **$23.84 trillion** by 2027.
(www.statista.com)

Top 3 most attacked sectors in 2022 were

1. Education/Research
2. Government
3. Healthcare

(Check Point Research)

Top five affected industries in the SME sector in number of insurance claims:
(Net Diligence "2022 Claims Study")

1. Professional Services
2. Healthcare
3. Manufacturing
4. Financial Services
5. Retail

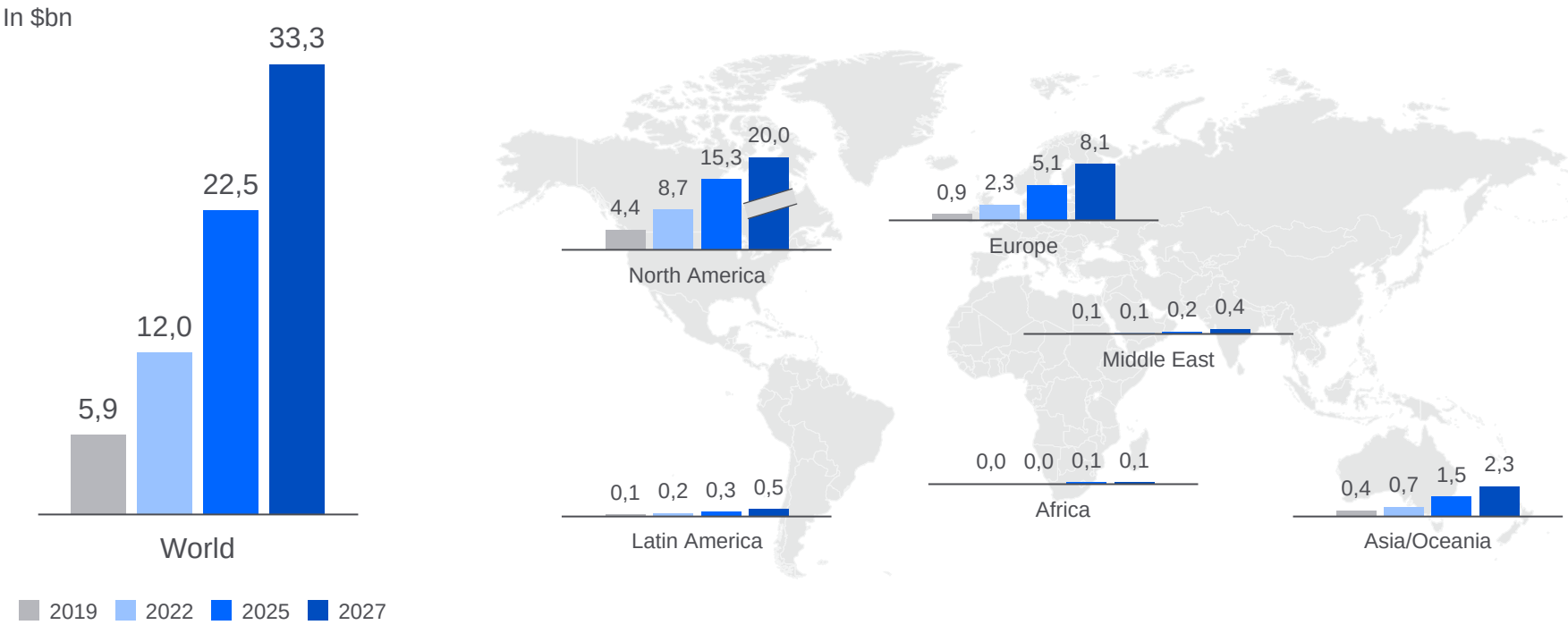
339,000 new malware variants are created every day. **92%** are delivered via email.
(Security Boulevard/Astra)

It is estimated that nearly **1.2%** of all emails are malicious in nature. This would amount to ca. **3.4bn** mails per day.
(Astra "Phishing attack statistics 2022)

The number of disclosed **zero-day vulnerabilities** in 2022 was on par with those from the previous year – the highest on record.

Cyber insurance market with strong expected growth

Worldwide cyber premium to increase from ~$12bn (2022) to ~$33bn (2027)



Source: Estimates by Munich Re

Cyber insurance – What is it?

or

$$For\ weak\ law:$$
$$\lim_{n\to\infty} P(\ |Y_n - Y| < \epsilon) = 1$$

$$For\ strong\ law:$$
$$P(\ \lim_{n\to\infty}\ ||Y_n - Y|| < \epsilon) = 1$$

Accumulation risk management is key

Accumulation Risk

The core problem with respect to systemic accumulation risk is the potential for a **cyber event to have severe effects on the entire cyber portfolio** affecting more than one insured.

Objectives of Accumulation Control

- Identification of worst-case scenarios
- PML quantification and accumulation management
- Modeling of accumulation loss distributions for the Munich Re Capital Model (MRCM)

Virus/Malware

Global outbreak of widespread, untargeted self-reproducing malware

Data Breach

Multiple insureds are affected by a large-scale data breach attack

IT Service Provider Outage

Large-scale outage of services such as cloud causing widespread business impacts

To be excluded

Failure of (critical) infrastructure

War

Data – the new gold?

Source: mauritius images

Cyber War Exclusion

Munich RE

A specific Cyber War exclusion must prevent **uncontrollable accumulation risk** and at the same time consider the interest of the insured being sufficiently protected against any Cyber-attack(s) and furthermore **not to jeopardize the cyber insurance value proposition** by taking a too strict or unclear approach.

Conventional War

Including cyber-attacks as a means of warfare

Attribution

Linking cyber-attacks to a sovereign state (“…by or on behalf of…”)

Intolerable impact

Severe disruption of essential services resulting in serious threats to the functioning of the public sector (e.g., administration, financial services, healthcare)

Collateral damage

Threshold to be set to not exclude losses from “low level events” elsewhere

Ransomware in 2021 vs drug trafficking 20 years ago

Munich RE

	Ransomware	Cocaine Trafficking in 1992
Revenue/Unit	$140,000/attack	$60,000/kilo
Operating Costs/Unit	$2,500/attack*	$5,000/kilo
Profit Margin	98%	91%
Arrests/Unit	0.0008**	0.50
Deaths/Unit	0	0.25
Barriers to Entry	None	Very High

Source: https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts

*Estimate based on reported costs of network access credentials, and amount of hours a threat actor expends on the average attack
**Estimated roughly 25,000 ransomware attacks of impact in 2020. Research found evidence of less than 20 total arrests globally

Under Control?

Source: RichVintage

Thank you for your attention

Dr. Jürgen Reinhart

Munich RE