



Image: cosmin4000-GettyImages

# Cyber Insurance

## Still infant or grown up?

Dr. Jürgen Reinhart  
March 2021

# Questions about cyber we want to answer today

1. Cyber Risk – what is it?
2. What does this mean for insurance?
3. What keeps a Chief Underwriter awake at night?
4. Why are actuaries concerned with this?

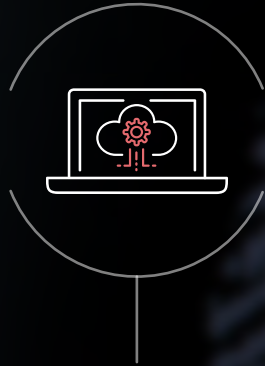
A person wearing a dark hoodie is holding a tablet computer. The background is dark with green digital code overlaid, suggesting a cyber or hacking theme. A white rectangular box is positioned in the upper left quadrant, containing the number '1' and the text 'Cyber Risk – what is it?'.

1

Cyber Risk – what is it?

# What does it mean “Cyber”?

The term “Cyber” is used in different ways



The term “Cyber” is a prefix used to describe a person, thing, or idea as part of the computer and information age. Taken from *kybernetes*, Greek for “steersman” or “governor”

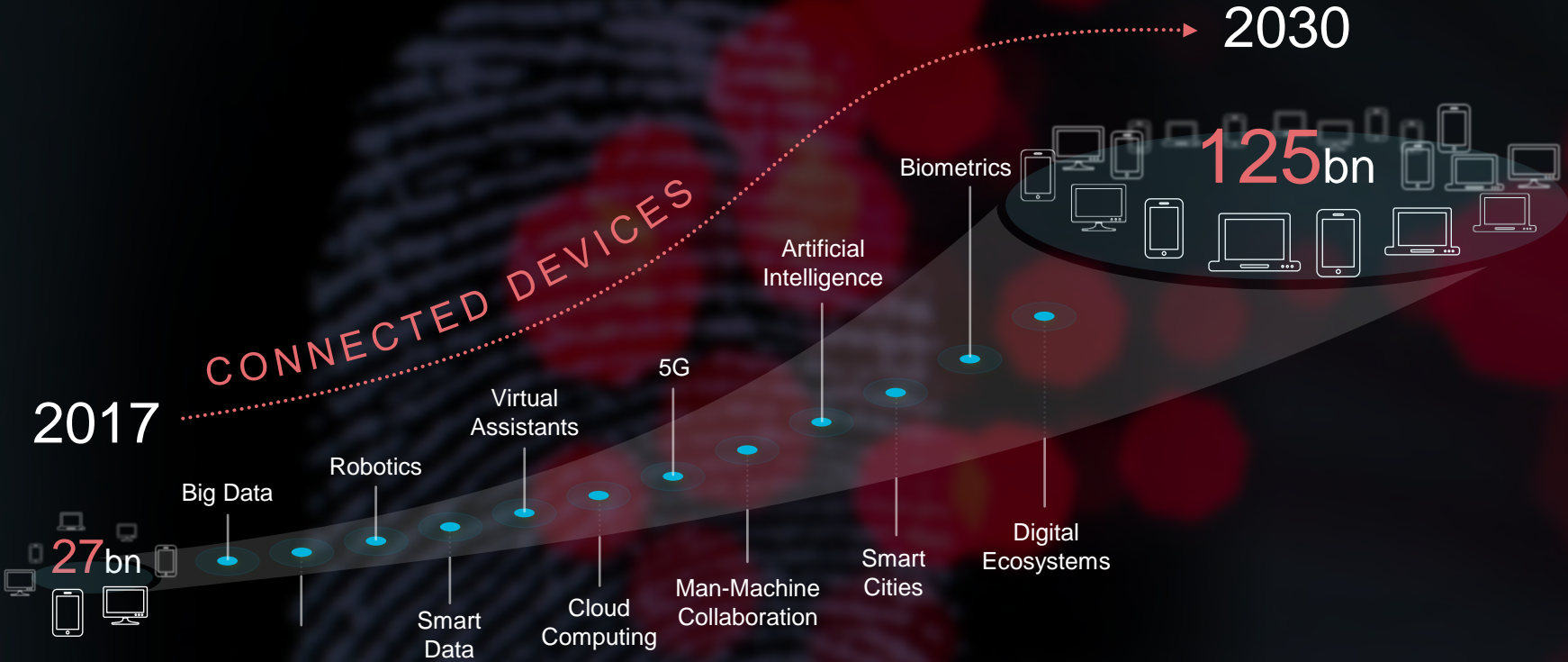


Currently, the adjective “cyber” relates to or characterizes the interconnectivity and culture of computers, information technology, and virtual reality (‘the cyber age’)



In the insurance industry the term “Cyber” is used for all risks which arise out of or stem from the usage of computer systems, hardware, software, data, the internet, networks and any other components of any information technology (IT) and Operational Technology (OT)

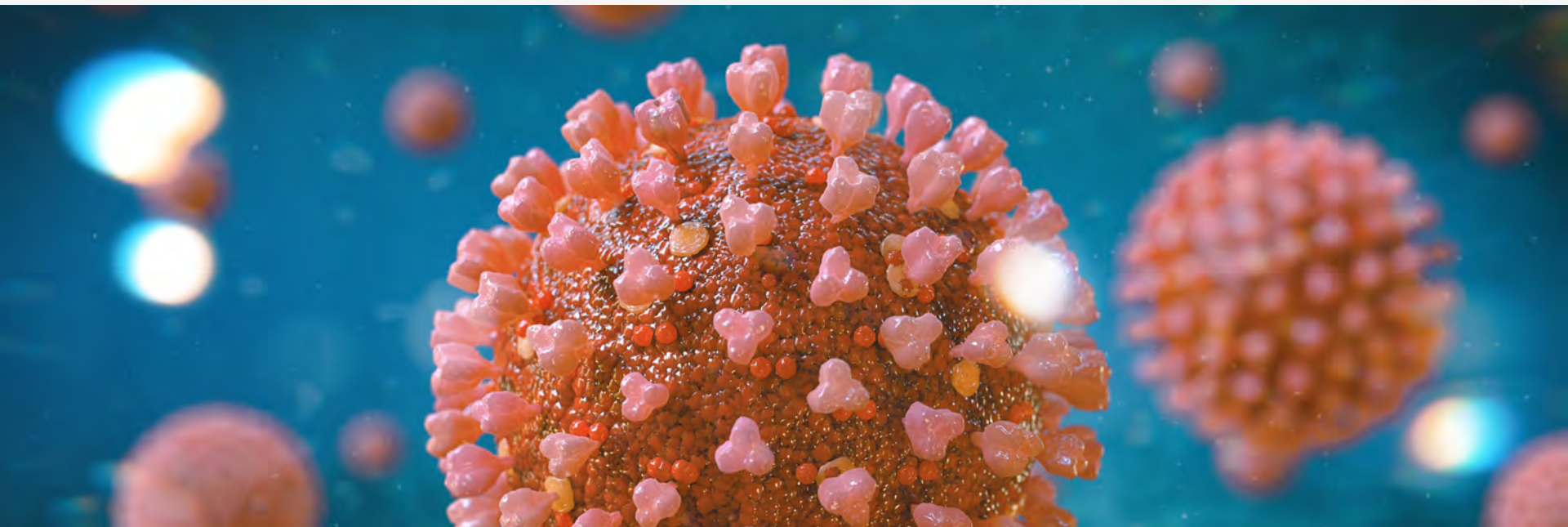
# Digital revolution bears a hyper-connected world



# Operational Technologies



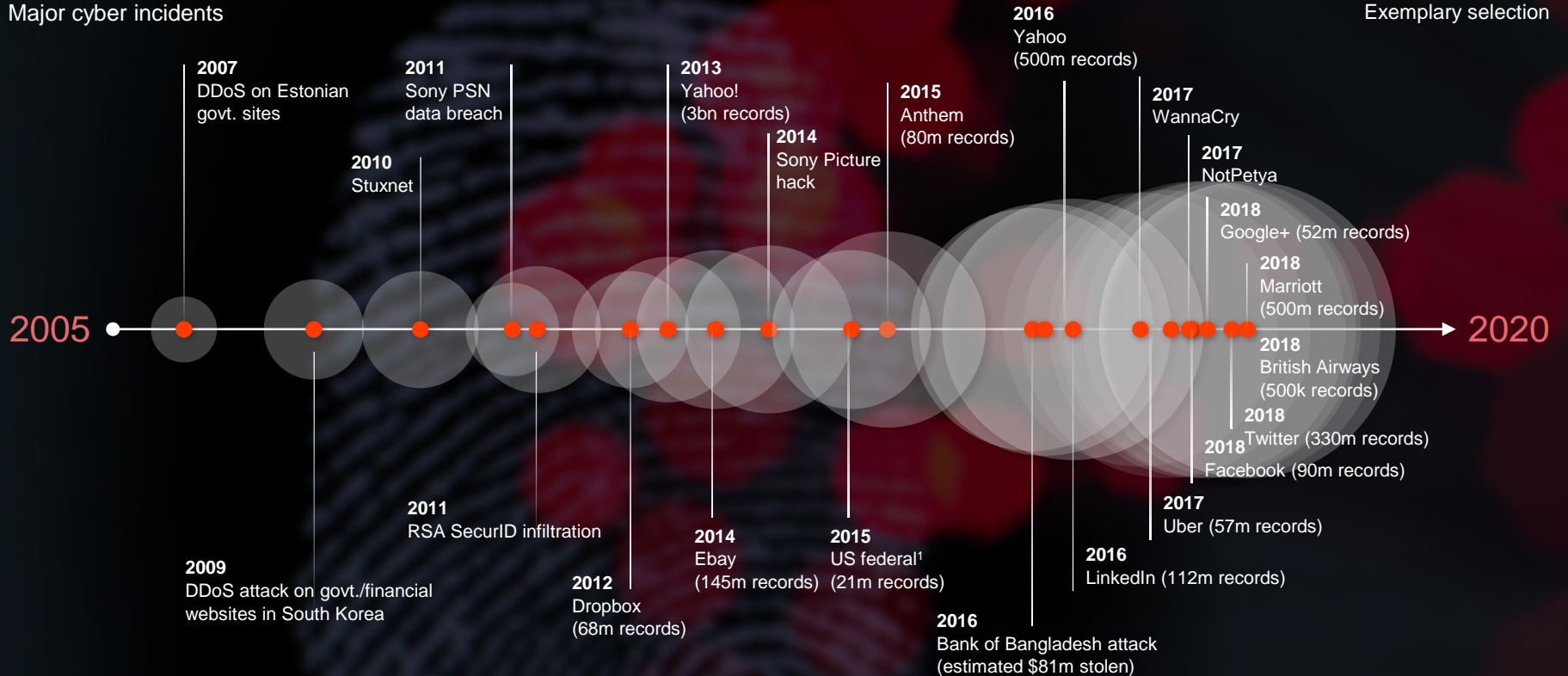
Operational technology (OT) is hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events.



# Evolution and exponential growth in cyber incidents

## Major cyber incidents

Exemplary selection



<sup>1</sup> Sensitive personnel data stolen from US govt. employees gone through security clearance background checks



# Top 10 Global Business Risks 2021

Allianz Risk Barometer



Source: Allianz Global Corporate & Specialty. Figures represent the number of risks selected as a percentage of all survey responses. The 2,769 respondents could provide answers for up to three risks. Photos: Adobe, iStock, Shutterstock

<sup>1</sup> Pandemic outbreak ranks higher than cyber incidents based on the actual number of responses <sup>2</sup> Market developments ranks higher than changes in legislation and regulation based on the actual number of responses <sup>3</sup> Macroeconomic developments ranks higher than climate change based on the actual number of responses KEY = RED Risk higher than 2020 GREEN risk lower than in 2020

# Evolving threat landscape and cybercrime perspective

Estimates of global cybercrime costs differ with cybersecurity ventures being at the upper end assuming these costs to reach \$**10.5**tn p.a. by 2025!  
In 2021 the number will be around \$**6**tn up from \$**3**tn in 2015

Attacks and payloads will get even **more sophisticated** and **targeted** wherever an extra effort seems promising

Just one example: Spear phishing is a rather high and manual investment. Automated tools combined with scanning programs will reduce efforts.  
**Distribution and customization will be more easy**

**Phishing attacks** will remain the major entry door

**Development and adoption of top technologies** like 5G, artificial intelligence, automation, edge computing or the shift to clouds will add new attack surfaces

## Munich Re global cyber risk and insurance survey

- 81% of global respondents (5.507) believe in an increase of cyber crime
- Fraud, Data Breaches and Ransomware Top 3 concerns of C-Level respondents
- 30% of global C-Level respondents are “extremely concerned” about a potential cyberattack. 38% are at least “concerned”





2

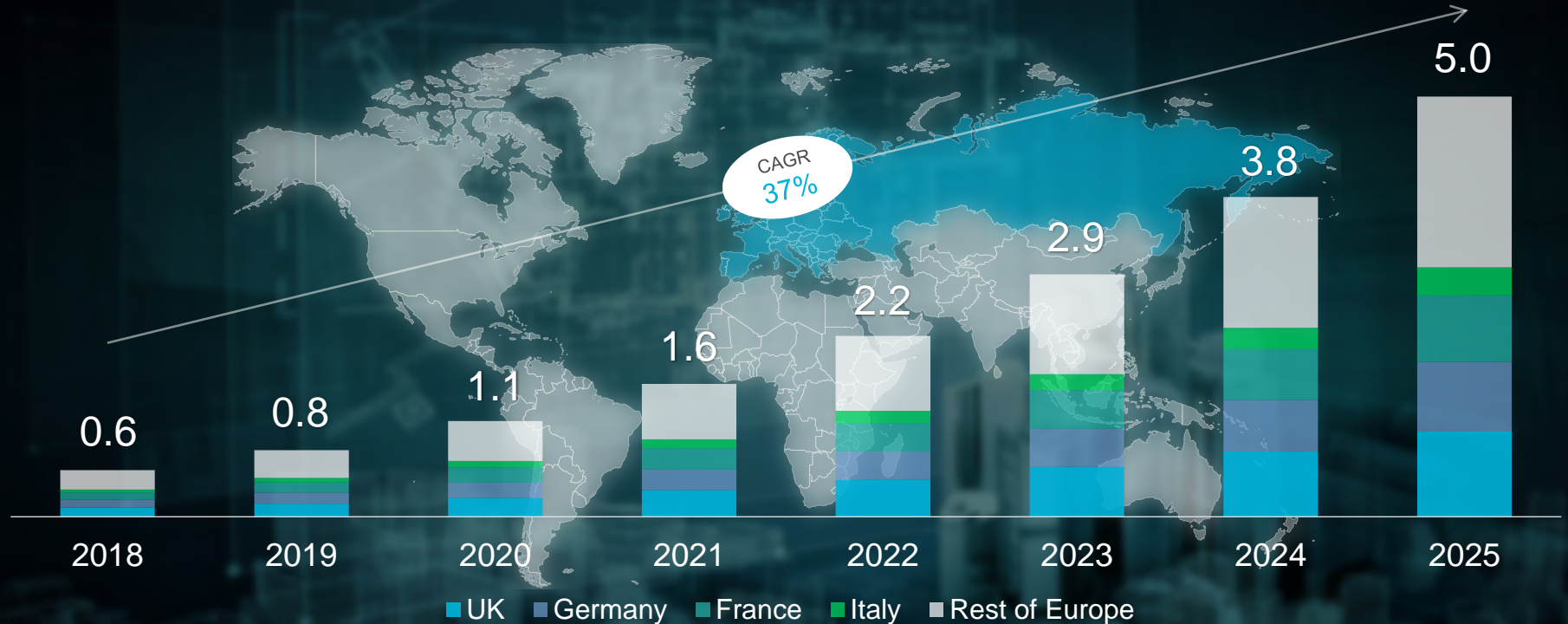
What does this mean for insurance?

# Cyber insurance market with strong expected growth

Worldwide cyber premium to increase from ~\$5bn (2018) to ~\$20bn (2025)



# For Europe a CAGR of 37% is expected (2018–2025)



# 3

What keeps a Chief Underwriter awake at night?



# Cyber (re-)insurance outlook

Significant expansion of coverage types





- Infrastructure failure exclusion/limited to BI (not applicable to data restoration)
- Blanket Contingent BI for supply chain
- Open peril system failure/any unplanned outage/“Act of God trigger”
- “Bricking”
- “Voluntary shutdown” covered in BI section
- BI Indemnity period (180 days or more?)



# Ransomware is getting a problem


[EXTERNAL] LockBit

  < >  
Wed 10/7/2020 11:59 AM








Hello Everybody.

Lockbit here. Because you are unable to respond to messages sent to  all stolen data is being uploaded to blog and will be sent to all media. You tried to hide the breach and ignore this so we have included media in this email for proof.

You have cyber insurance. We do not want your money. We want insurance money. Your cover is \$1m USD and we will cause more damage over \$1m USD if you do not contact.

Time is ticking. You have 12 hours. See you soon.

Lockbit.

  Sr. Systems Engineer  


# Major Cyber Accumulation scenarios<sup>1</sup>

## 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<sup>2</sup>

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



## External networks failure<sup>3</sup>

- Electrical power supply
- Telecommunication & Internet
  - Infrastructure
  - Software Failure



<sup>1</sup> MR has investigated other scenarios (e.g., corrupted software) as well, which turned out to be lower in terms of PML magnitude <sup>2</sup> Scenario/model under development  
<sup>3</sup> This scenario is deemed not within appetite and are only written by exception, if specific permission ("dispensation") is granted by the highest underwriting authority

UPDATED

**ALERT**

**APT Compromise of Government  
Agencies, Critical Infrastructure,  
and Private Sector Organizations**



On **December 13**, 2020 CISA determined that this exploitation of SolarWinds products poses an **unacceptable risk** to Federal Civilian Executive Branch agencies and requires emergency action. Multiple versions of **SolarWinds Orion** are currently being exploited by malicious actors. This tactic permits an attacker to gain access to network traffic management systems. **Disconnecting affected devices**, as described in Required Action 2 of the ED, is the **only known mitigation measure currently available**.



4

Why are actuaries concerned with this?

# Topics where we need actuaries



Pricing

Exposure Analysis

Risk Quantification

Accumulation Risk Modelling

Data analytics and Artificial Intelligence



or

*For weak law :*

$$\lim_{n \rightarrow \infty} P( |Y_n - Y| < \epsilon ) = 1$$

*For strong law :*

$$P( \lim_{n \rightarrow \infty} ||Y_n - Y|| < \epsilon ) = 1$$





# Q&A

Image: cosmin4000-GettyImages

Cyber is a challenge...  
...but also an opportunity!