



The Future of Cyber Risk

Dr Christos Mitas
VP of Model Development
Risk Management Solutions

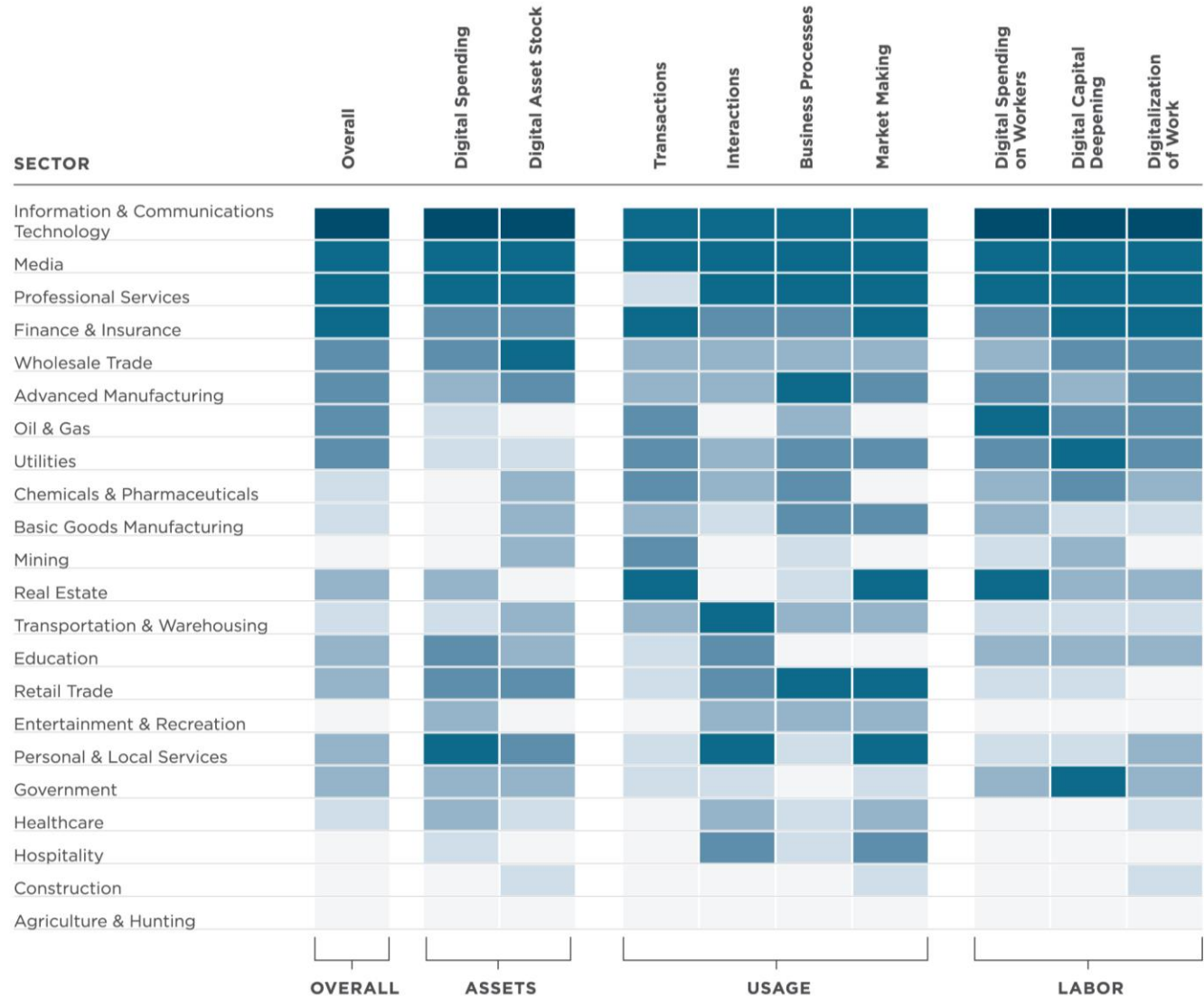
10th Risk Summit, Cambridge Judge Business School

June 20, 2019

CYBER RISK

- Why is it there?
 - Accelerated digitization (*software eats the world*)
- What is it?
 - Which components does it comprise of? (*physics*)
 - How do they change? (*dynamics*)
 - Is it systemic?
 - How can it be quantified?
- What to do about it?
 - At present
 - In the future

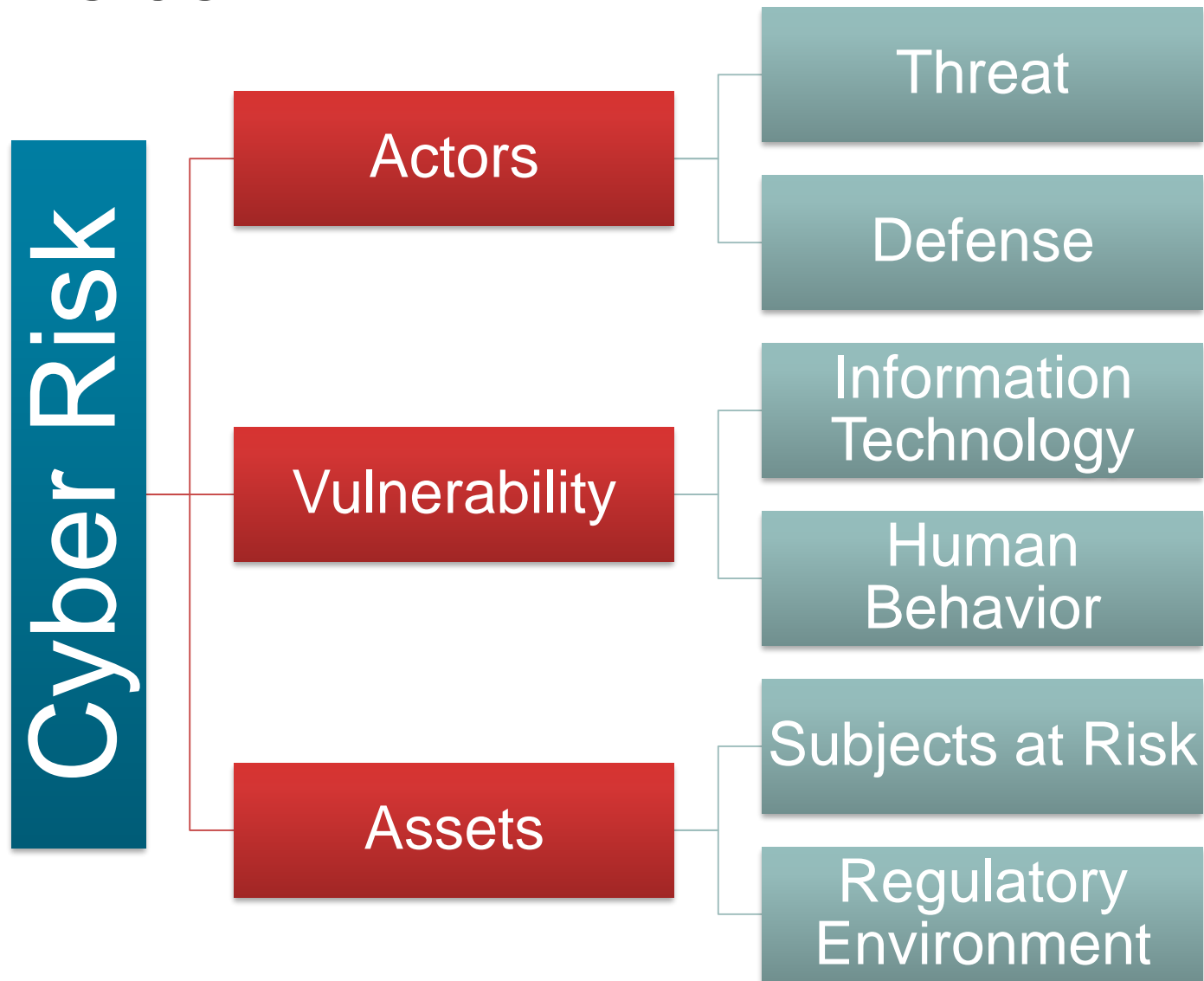
WHY?



Relative degree of digitization. *Harvard Business Review*.



WHAT - PHYSICS

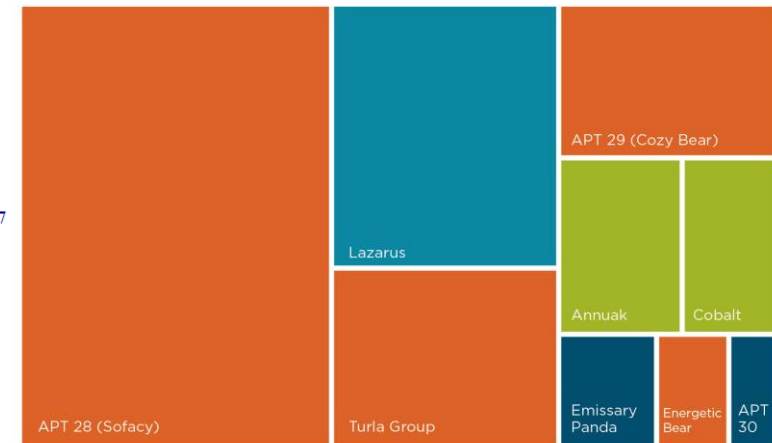
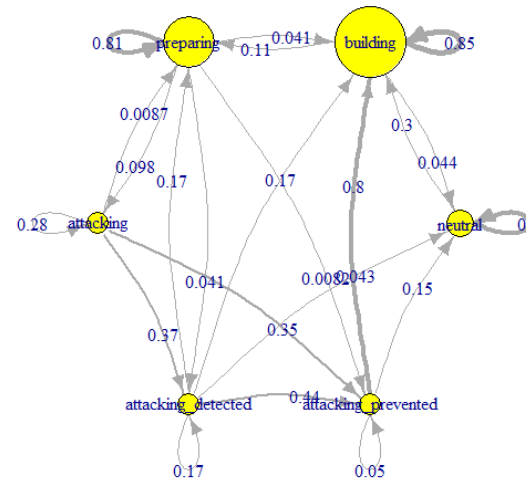


THREAT ACTOR DYNAMICS

- Taxonomy of APTs
 - Organized Crime (Hub & Hierarchical)
 - Nation-State
 - State-Sponsored
 - Mercenary
 - Hacktivist

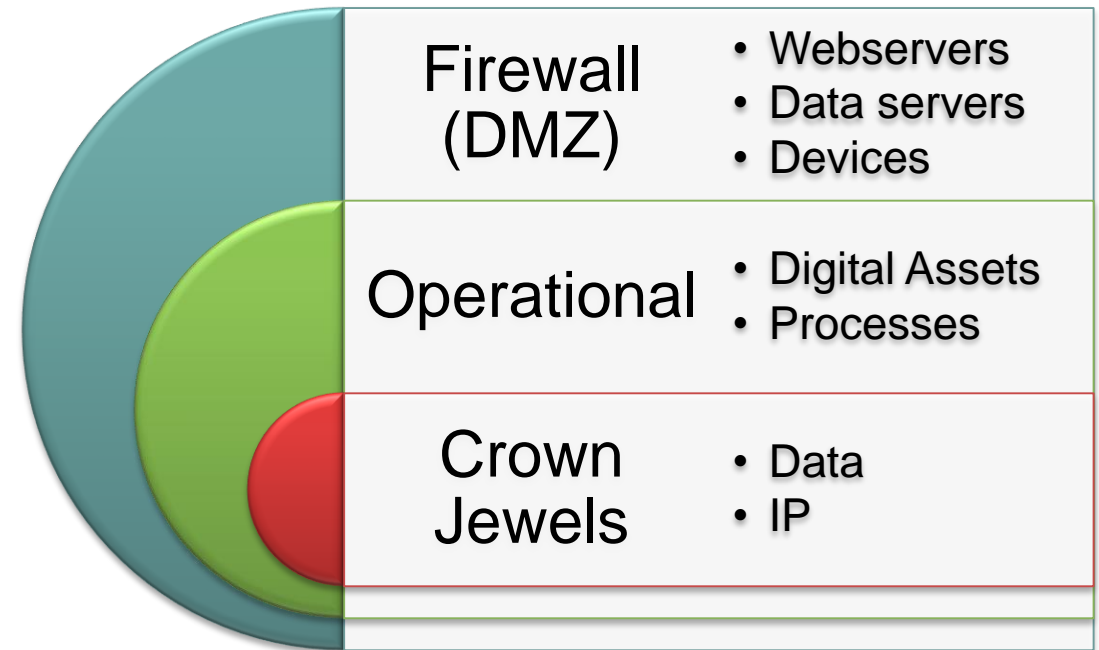
- Motivation
 - Political/Geopolitical
 - Financial

- Skills, Capabilities, Size



DYNAMICS OF SECURITY DEFENCES

- IT Security
 - Budget
 - Team
 - CISO
 - Skills, Capabilities, Size
- Endpoint security
 - Signature-based
 - ML/AI (i.e. pattern-recognition)
- Patching cadence
- Cryptographic Encryption



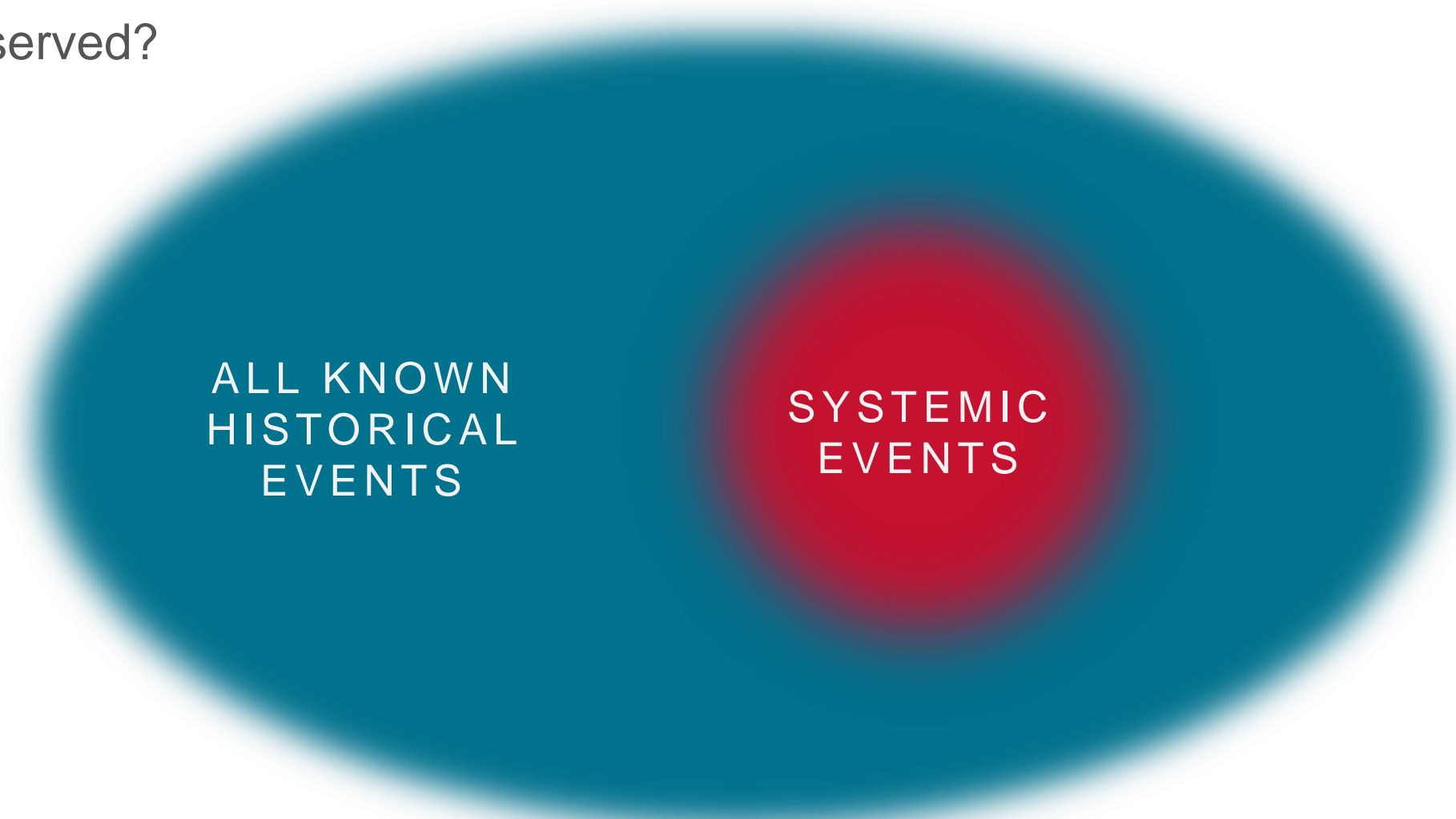
IS CYBER RISK SYSTEMIC?

SYSTEMIC CYBER RISK

- How it is defined and how it arises:
 - *Inter-connectedness*
- Quantification of cyber risk is required to determine
 - How cyber risk flows through businesses?
 - How cyber risk accumulates across the industry?
 - How various cyber risks are correlated?
 - How can the business community plan for and defend against it?
 - How can the re/insurance industry help create a stability?

SYSTEMIC CYBER RISK

- What have we observed?



SYSTEMIC CYBER RISK

- What have we observed?



June 24, 2019

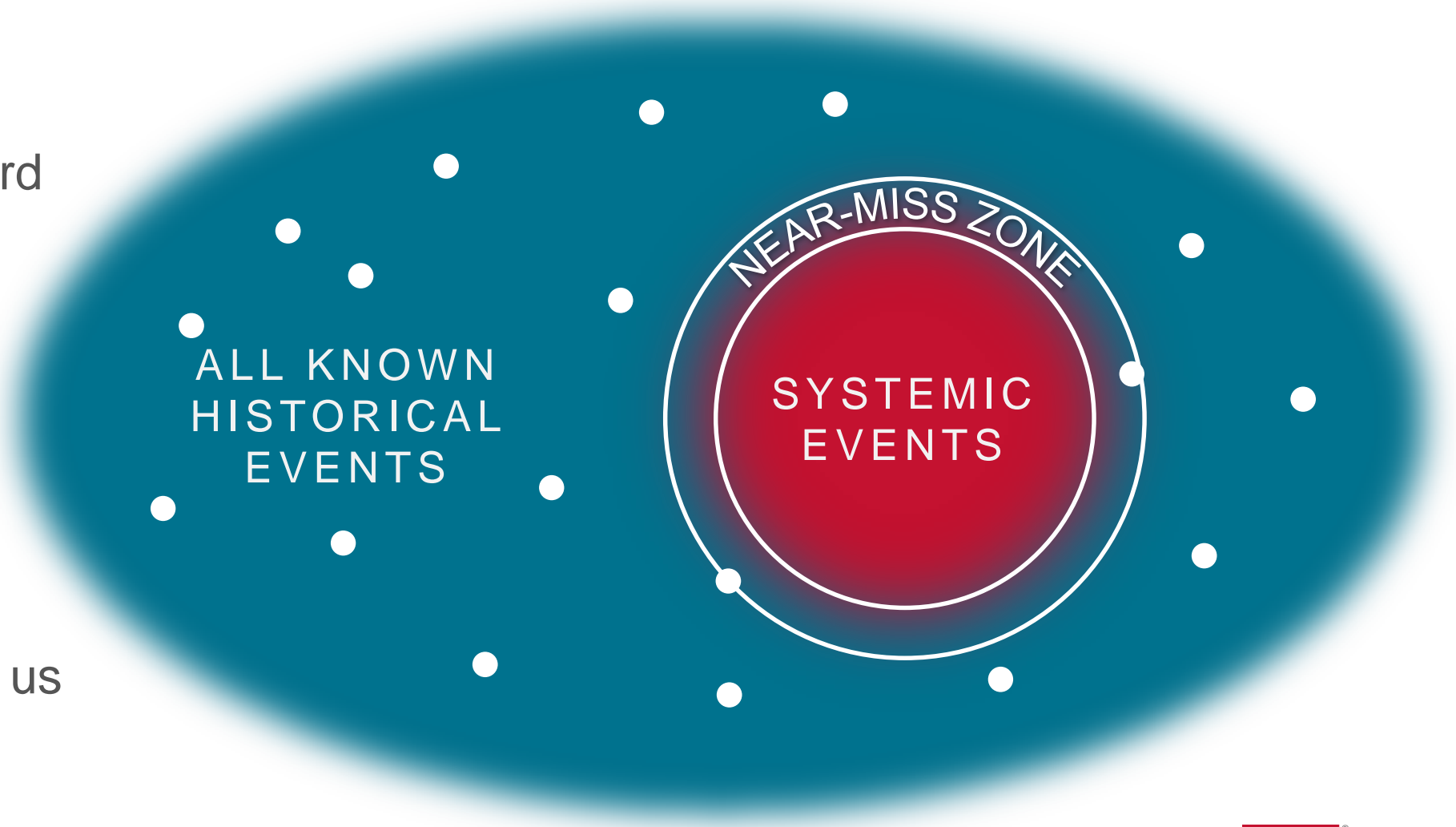
ALL KNOWN
HISTORICAL
EVENTS



Confidential - Not for general distribution

SYSTEMIC CYBER RISK

- What have we observed?
- Short historical record
- “Τα πάντα ρει”
- Threat landscape, attack vectors, vulnerabilities and digital assets are constantly changing
- History can only get us so far → need for cyber risk models



HOW CAN CYBER RISK BE QUANTIFIED?


BUILDING BLOCKS



Threat Landscape

Define threat actor groups, motivations, resources, skill sets & modus operandi


Example: State Sponsored Groups
- APT 28 / Sofacy



**Attack Vectors/
Loss Mechanism**

Categorise cyber loss processes including scalability and determine size and footprint of events


Example: Contagious malware event utilising operating system zero-day vulnerability



Company Vulnerabilities

Define susceptibility of a company to specific cyber attack considering:
1) Human vulnerabilities
2) IT vulnerabilities

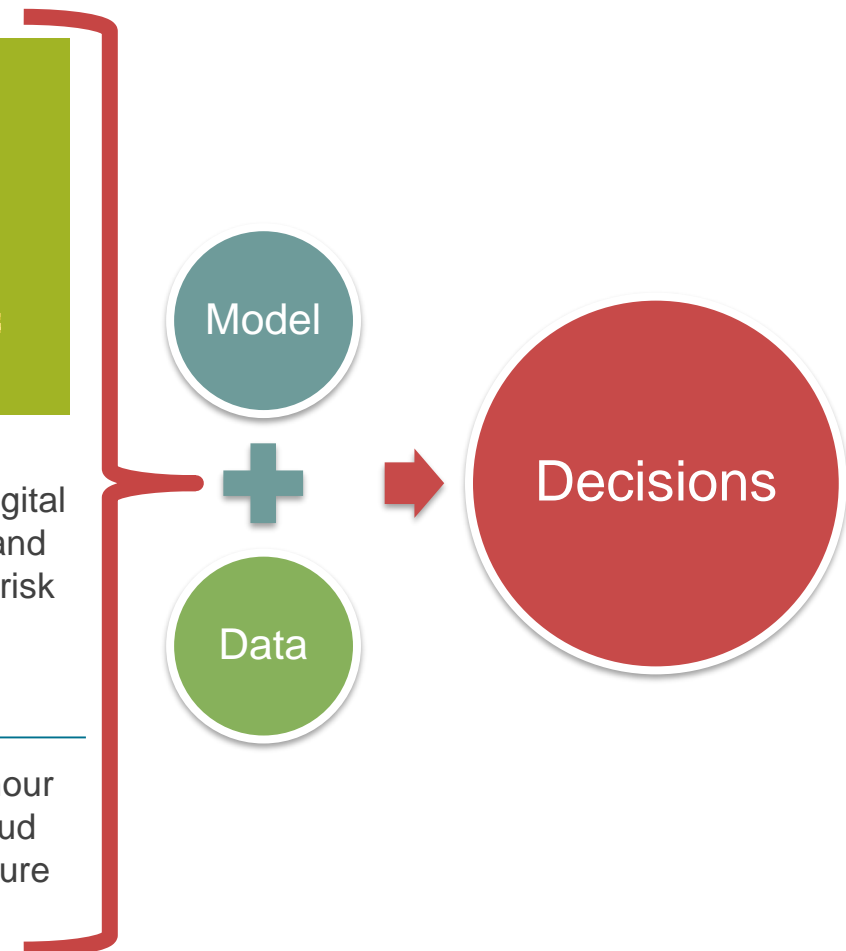
Example: Poor patching cadence detected through SSL certificate non-updates



Digital Assets

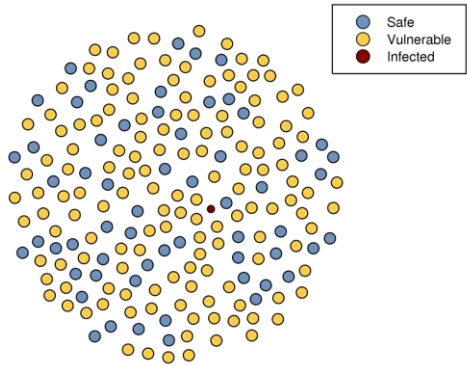
Quantify value of digital processes, data, and financial assets at risk

Example: x\$ per hour supported on cloud service infrastructure

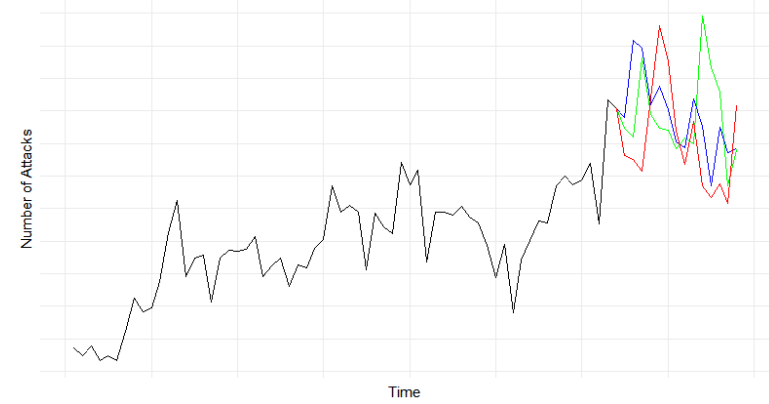
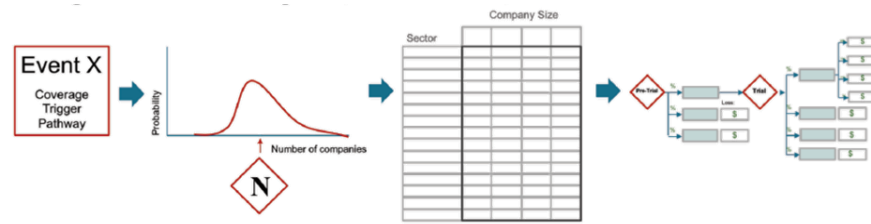
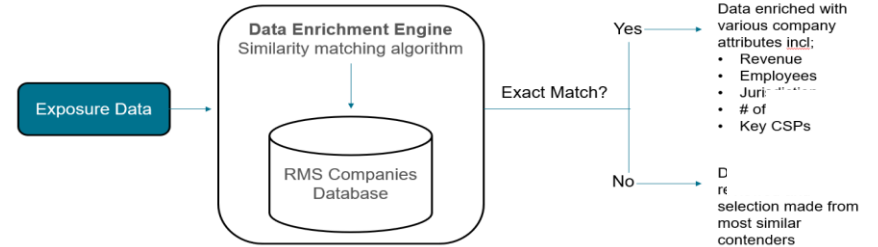
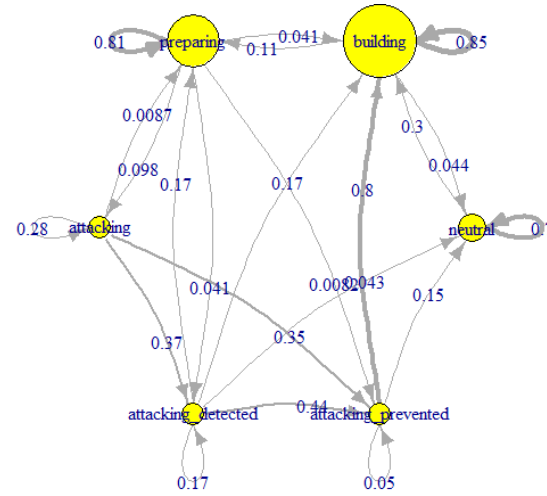


MODELLING TECHNIQUES

8 minutes



- Safe
- Vulnerable
- Infected



DON'T FORGET

CYBER-PHYSICAL

Industrial Facilities



Power Generation



Building fires



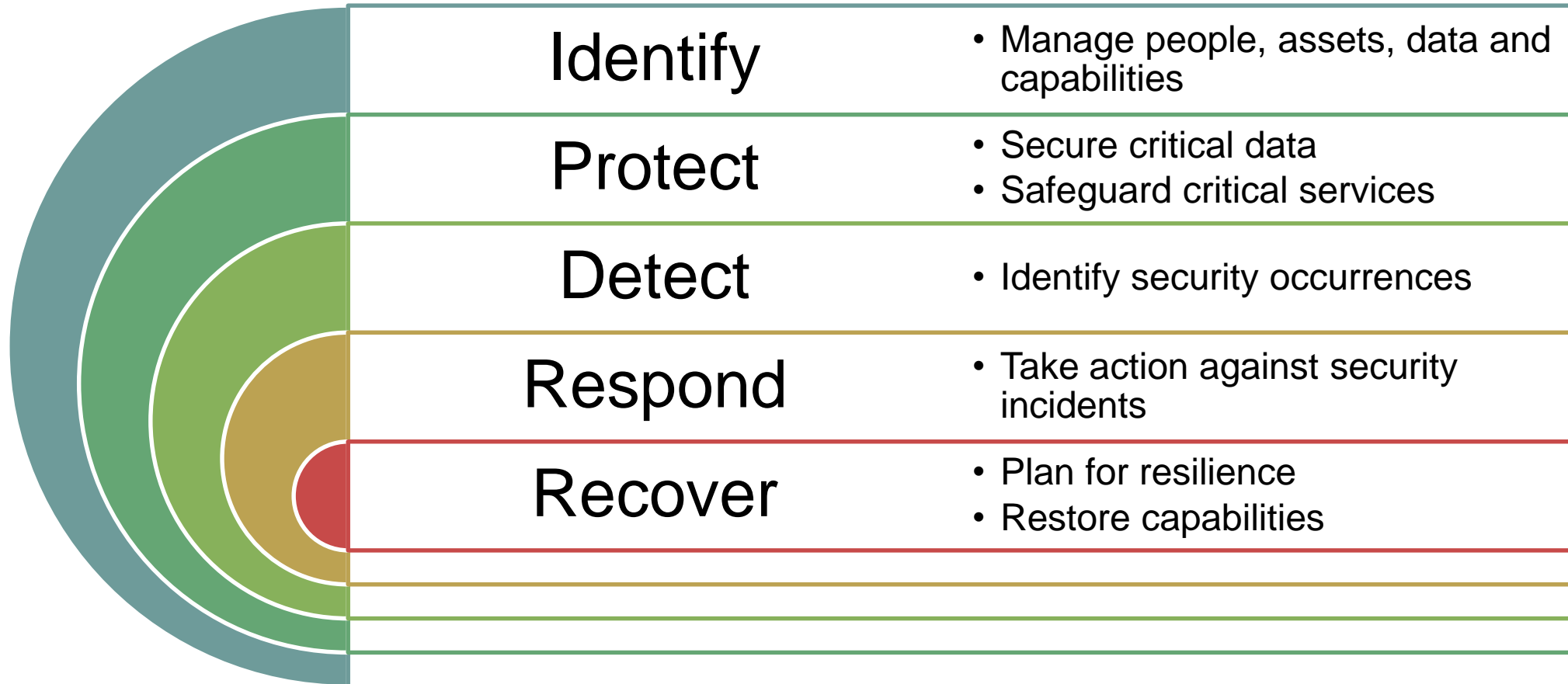
Upstream Energy – Oil Rigs





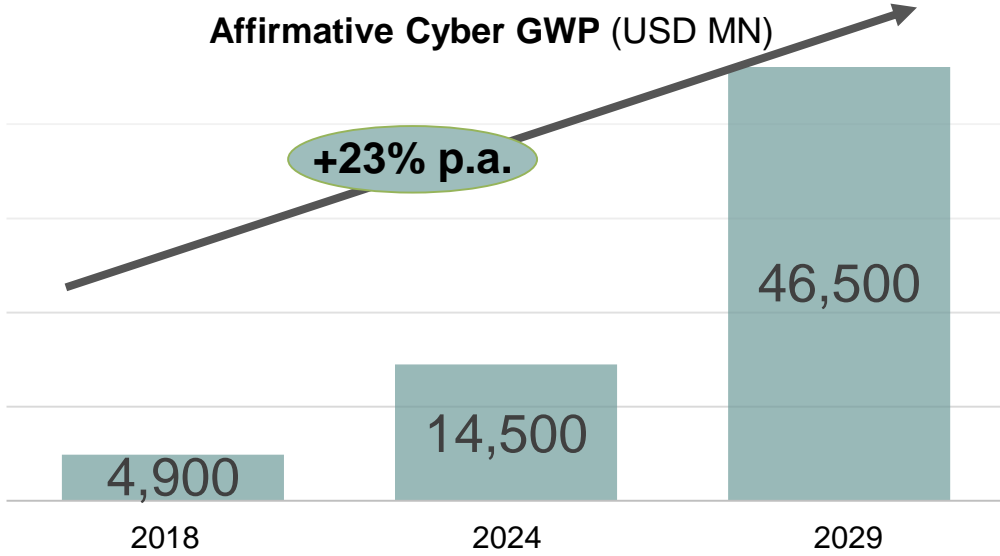
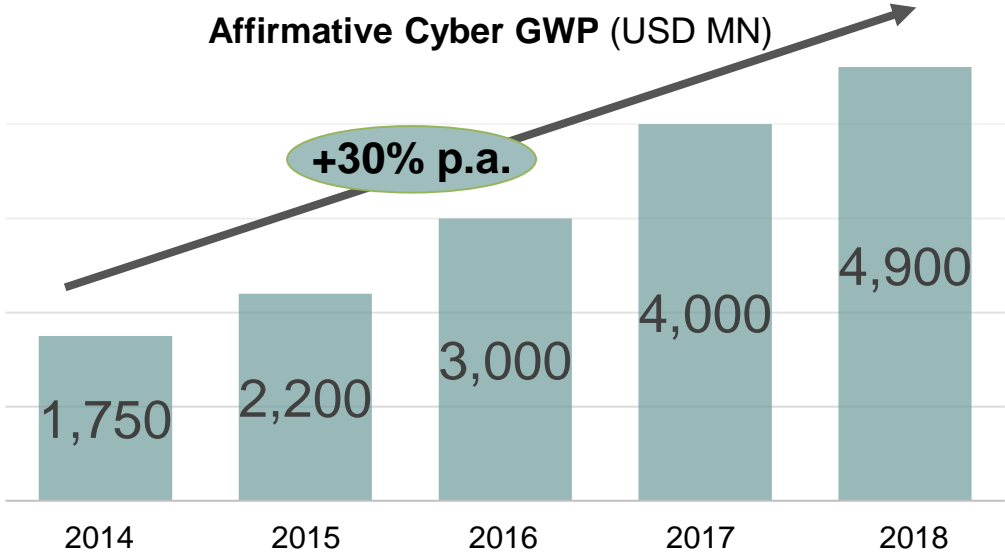
WHAT TO DO?

CYBER RESILIENT ORGANIZATION



National Institute of Standards & Technology (NIST)

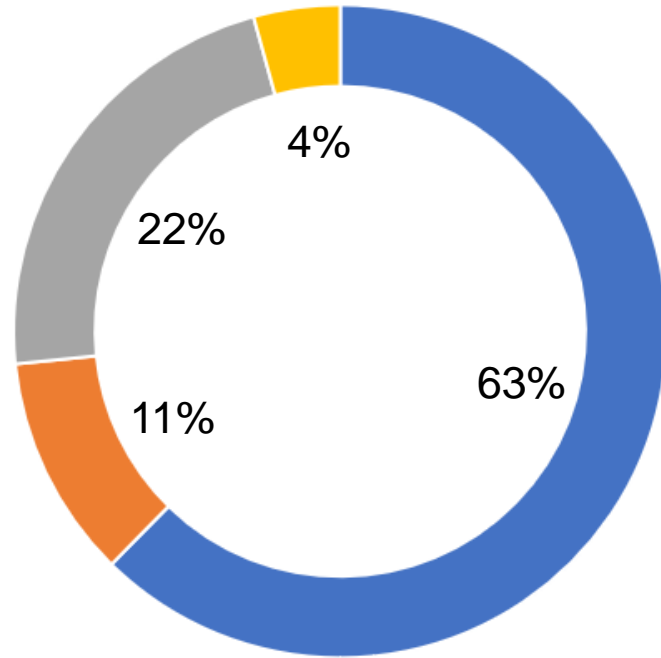
THE CYBER INSURANCE MARKET – GROWTH



VisionGain Cyber Insurance Market Report 2019-2029

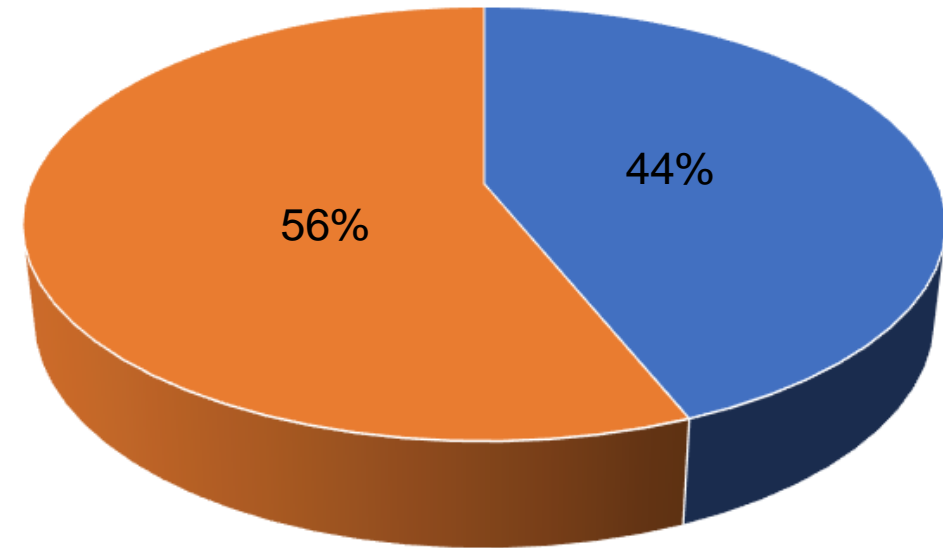
THE CYBER INSURANCE MARKET – KEY STATS

Global Cyber Insurance Market by Region 2019



- North America
- Asia-Pacific
- Europe
- Rest of World

Global Cyber Insurance Market by Cover Type 2019



- Standalone
- Packaged

TWO FUTURES

Cyber Armageddon

- Hacker hoards rise
- More powerful attacks
- No data is safe
- Splintered Internet
- E-commerce dies
- Cyber war

Cyber Utopia

- Exorcise the ghosts in the code
- Effective law enforcement
- “Geneva convention” for cyber operations

E.G. CRYPTOGRAPHY

- Paramount for a functioning Internet
 - Privacy
 - E-commerce
- “Prime number factorization”
 - Difficult (really, really difficult)
 - But hasn’t been proved impossible
- Shor’s algorithm (1994)
 - Very efficient doing so... **but** it needs quantum computers
 - Which are now real... **albeit** still not at capacity
 - Could reach required capacity by 2030 – 2040
- Quantum cryptography
 - Counters suspicious interceptions – detectable anomalies
 - But cannot work on the current Internet
- Quantum-resistant algorithms
 - In development; expected around 2025 (NIST)
 - Implementation might need another decade
- Equilibrium will be established
 - Will it be closer to Armageddon or Utopia?
 - And how long will it take?

Future-proofing the internet

Quantum computers will break the encryption that protects the internet

Fixing things will be tricky

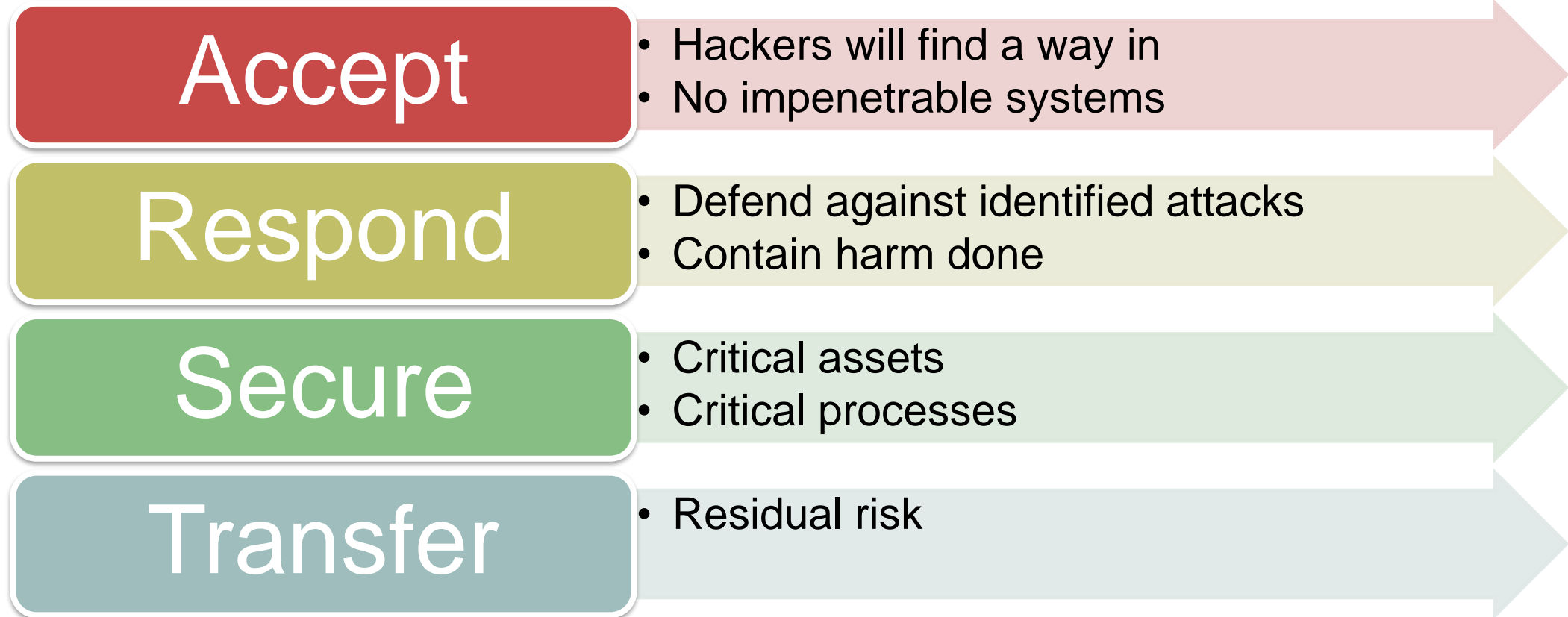


Print edition | Science and technology >

Oct 20th 2018

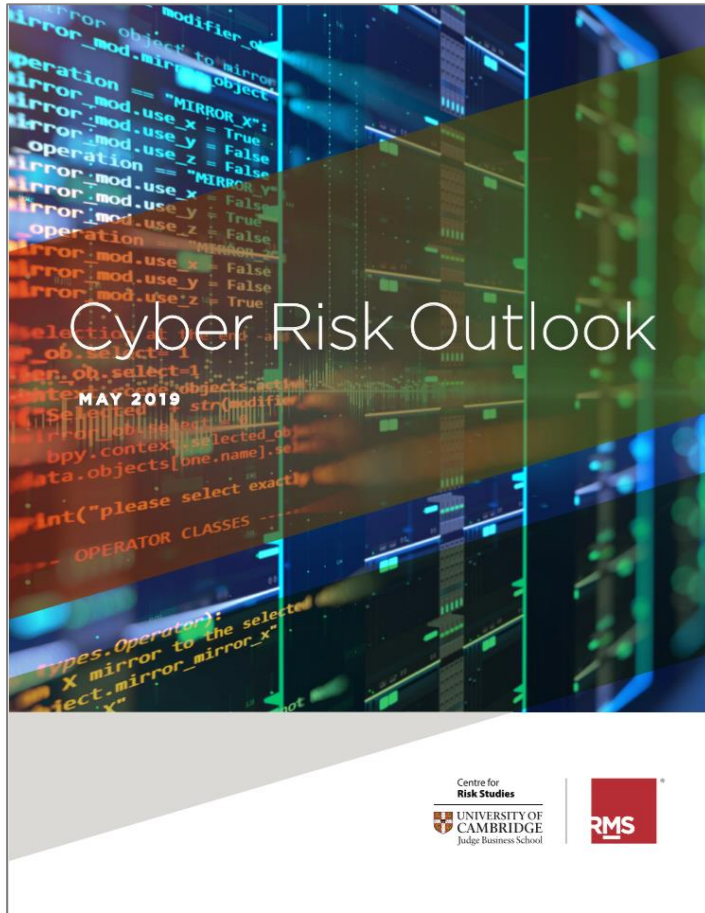


A PRUDENT RISK MANAGEMENT APPROACH



Regardless of Cybergeddon, Cybertopia, or something in between (most likely state)

RESOURCES



“The Future of Cyber Risk”
Workshop, Cambridge
July 24 2019

Centre for
Risk Studies

 UNIVERSITY OF
CAMBRIDGE
Judge Business School

