

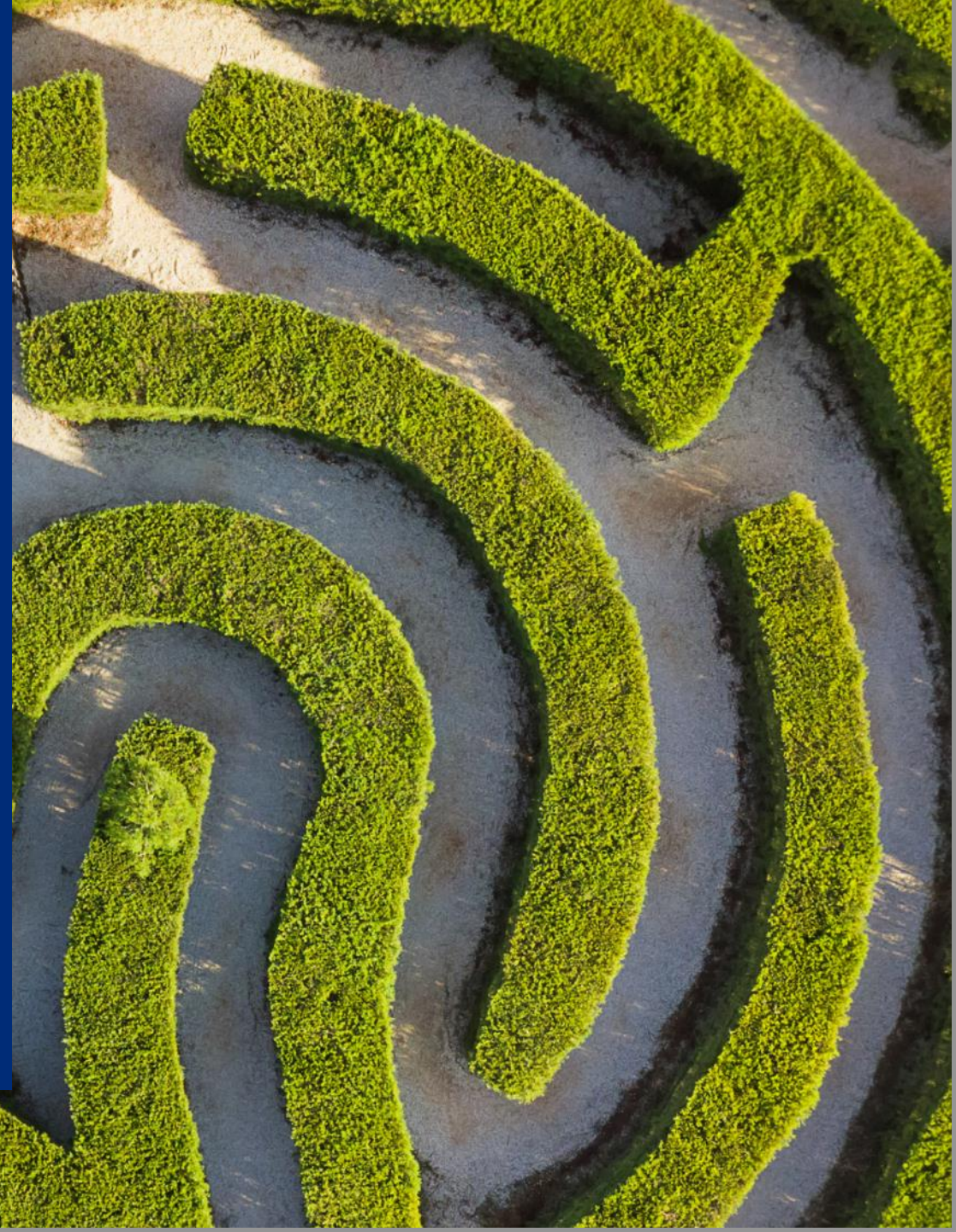
Why cyber insurance is (not) a waste of money

ISACA

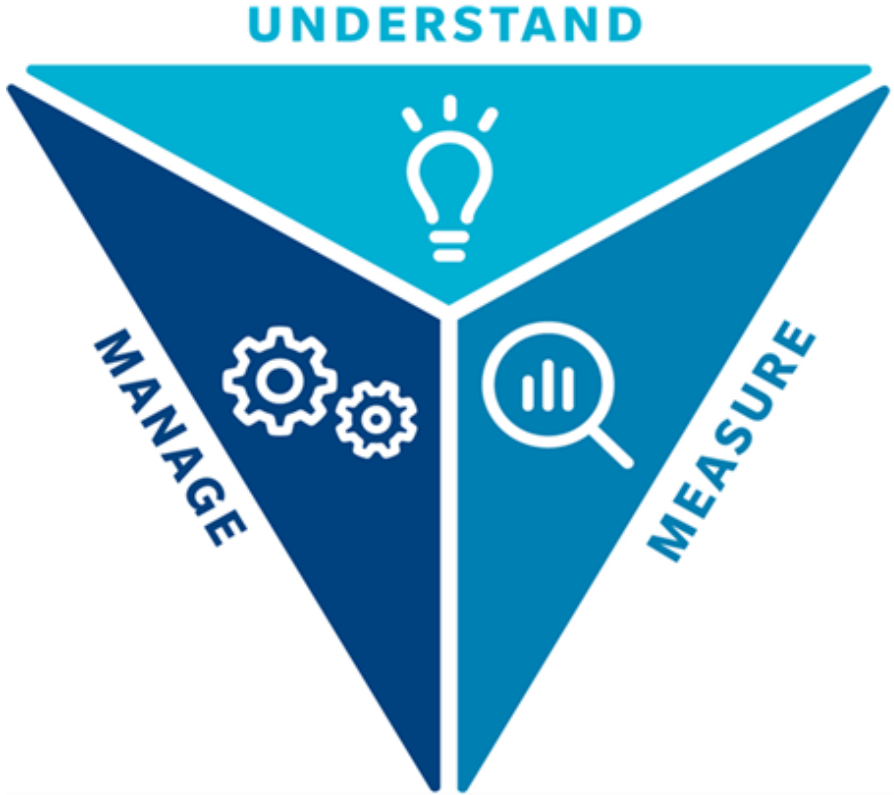
Sjaak Schouteren

Cyber Growth Leader, Europe

July 2024



Role of a cyber risk advisor



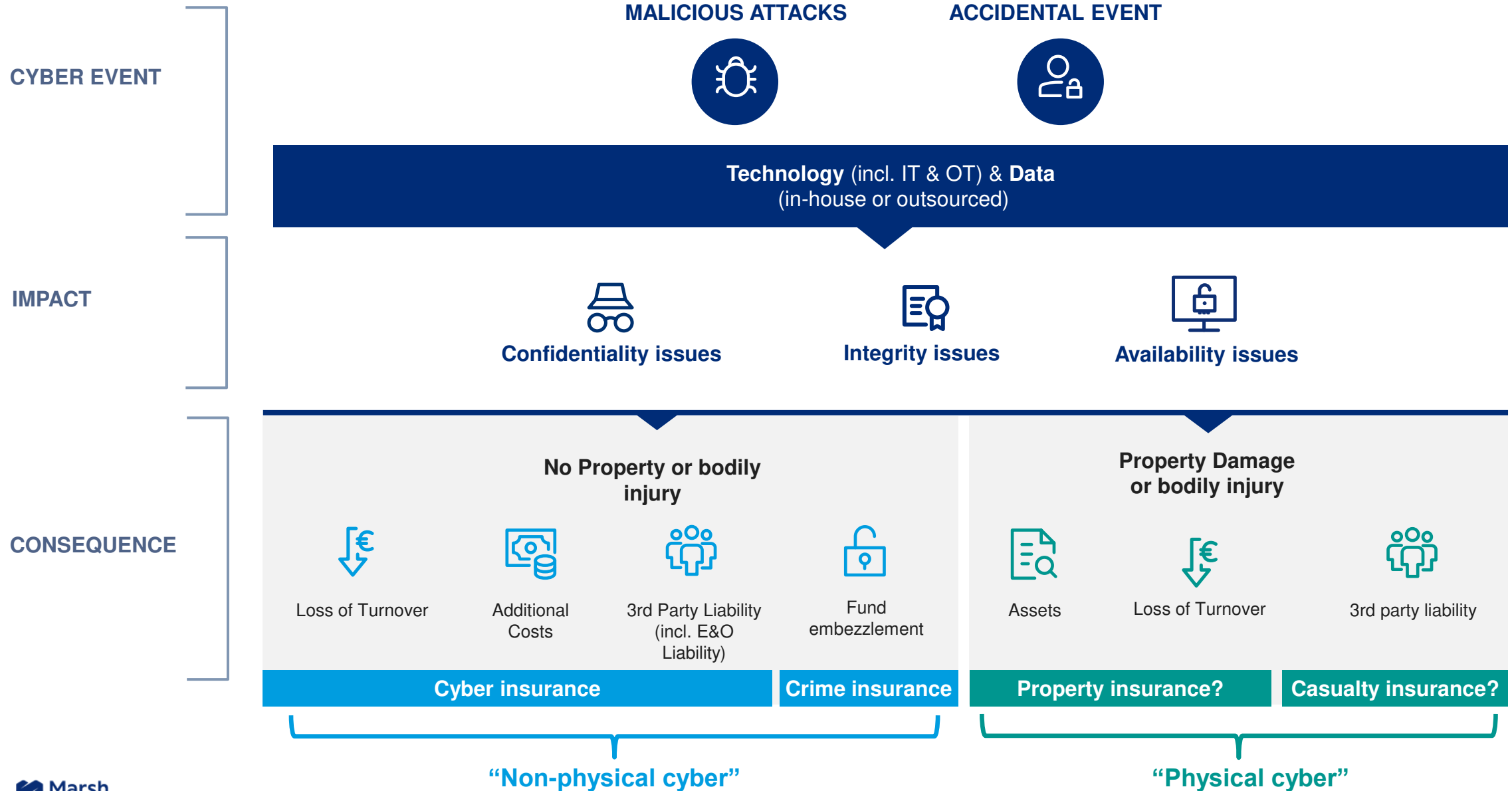
- **Understand**
 - Provide **cyber context** within a **business perspective**.
- **Measure**
 - Quantify the **financial impact** of cyber exposures.
- **Manage**
 - Actionable steps to **secure, insure** and **recover**.

Our Goal

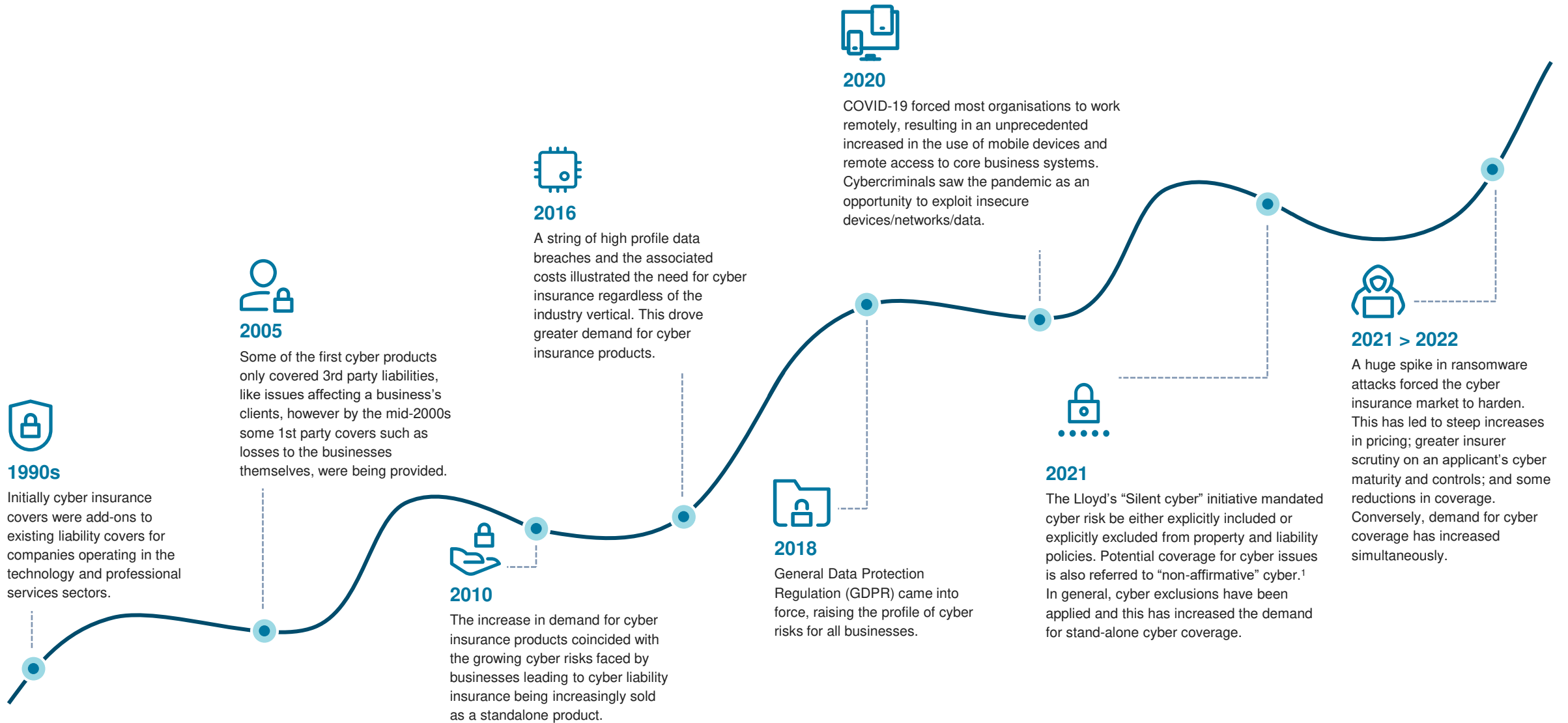
Bringing value at each steps.

Fit with your needs.

Understand the Impact and Consequence of a Cyber Event



History of cyber insurance



Looking forward: Cyber market moderation

2015 – 2018

2019

2020

2021

2022

2023

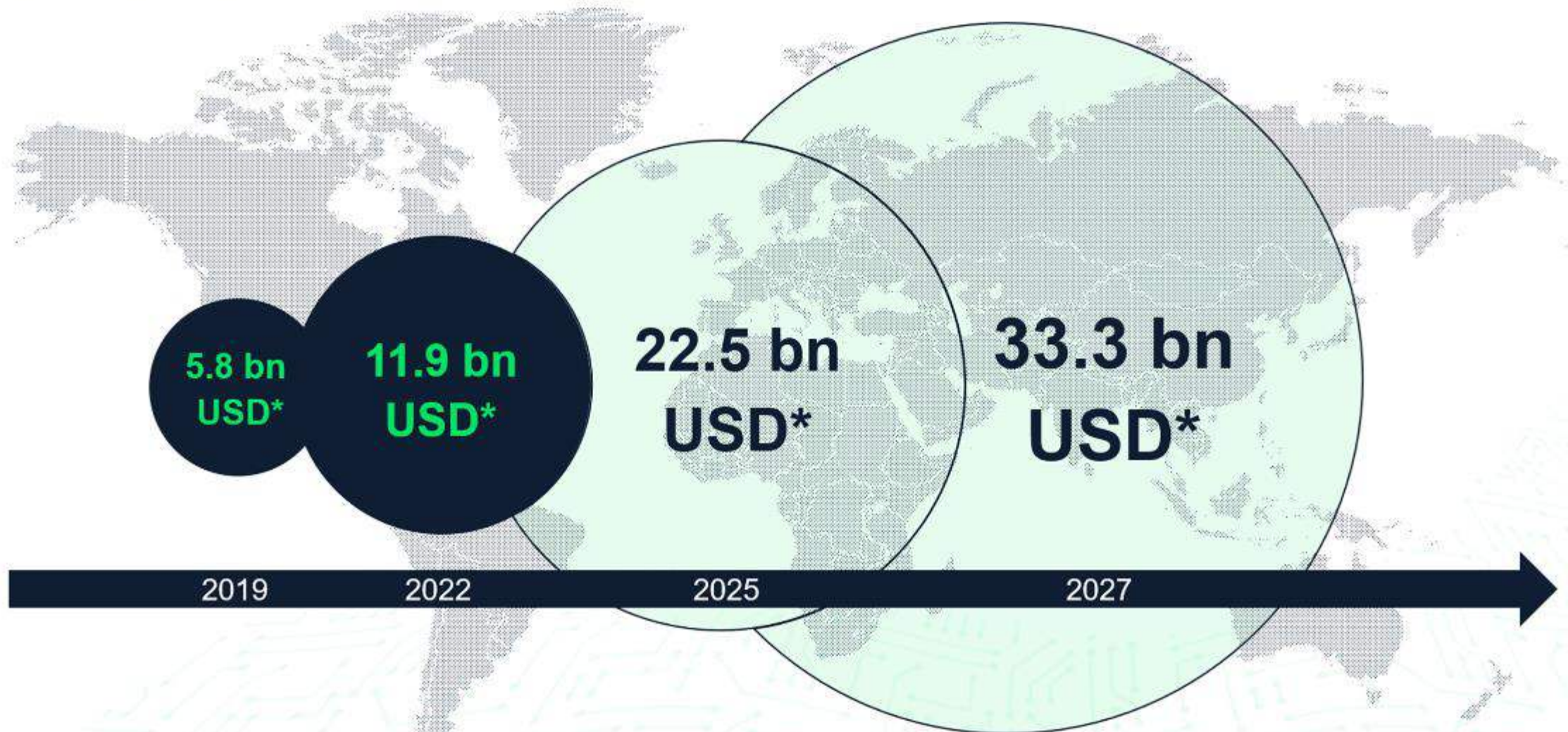
WE ARE HERE

- Catastrophic risk concerns
- The cloud = SPOF (single point of failure)
- Global cyber supply chains
- Data sovereignty
- Ransomware
- Geopolitical tensions

- Improved cyber hygiene
- Risk engineering
- Predictive modeling
- Active / gov't regulation
- Private / public partnerships

Global cyber insurance market: Demand continues to grow

*Estimates by Munich Re



Cyber security and Cyber insurance are complementary

Implement the right risk solutions

Risk Mitigation

Owner: CISOs

Estimated cost: 5-6 % of IT budget

Target: Reducing frequency

Risk Transfer

Owner: Finance / Risk Management

Estimated Cost: 1% - 5% RoL

Target: Reducing severity

Cybersecurity

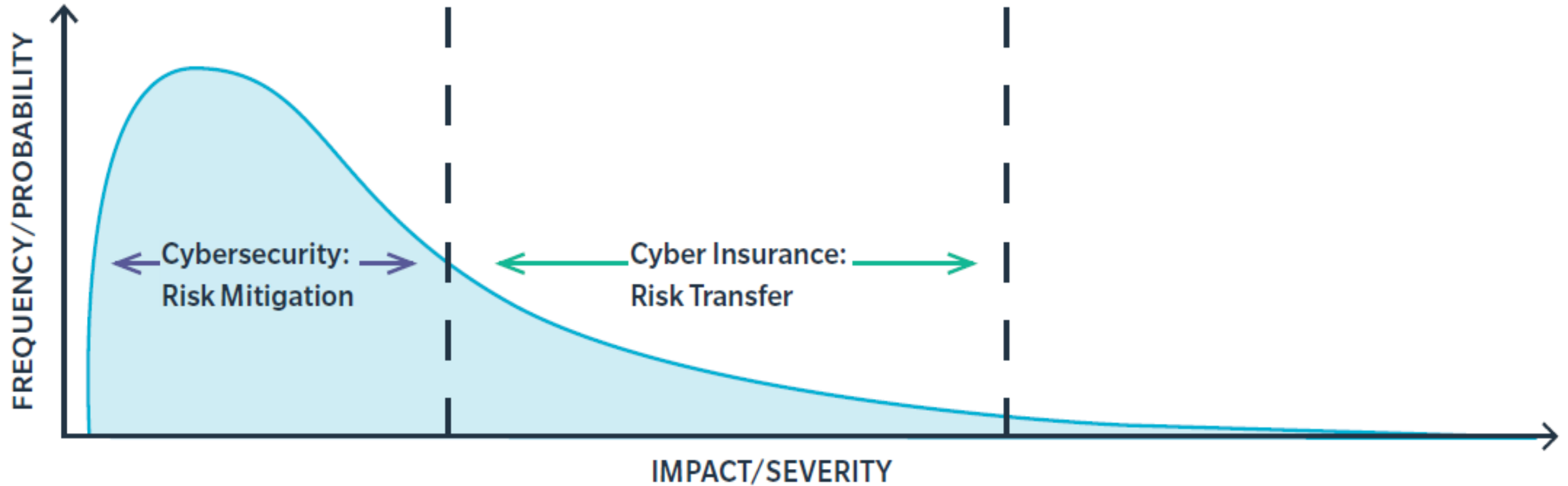


Cyber Insurance

Mitigate/Transfer

Risk Management Optimization

Cyber Insurance and Cybersecurity are Complementary



Coverage of Cyber Insurance

Cyber Risk Insurance

General Coverage Overview

Cyber Liability (third party loss)

Claims clients & suppliers
Claims other third parties
Legal assistance and advice

First Party Losses (direct and indirect)

Insurable fines GDPR / PCI-DSS
Extra PR, Customer service
Reputational protection
Reconstruction data, systems
Other costs caused by event

Ransom Money
Negotiation Costs

Business Interruption (loss of gross profit, loss of hire), Extra expenses to prevent stagnation

Incident response

Investigation costs / IT Forensics
Legal assistance and advice
Notification regulator, persons
Extra PR, Customer service

Preventive services

Regular Phishing Simulation Campaigns
Phishing resistant MFA keys (YubiKeys)
Crisis simulation workshop
Cyber Insights Session
Risk Management discussions
Port scanning and monitoring

Triggers for coverage:

Malicious Attack Malware (virus, etc.) Hacker, DDoS, Trojan, Data privacy violation

Accidental Event Human error, System outage, Data breach

Impact on Confidentiality and/or, Integrity and/or Availability

Claims

Financial impact as seen in cyber claims

Assistance & Emergency measures 20%

Cost and expenses related to;

- ☑ Identification, assessment and containment of security event (IT Forensic)
- ☑ Provision of legal assistance (Data breach of confidentiality)
- ☑ Provision of crisis management or communication assistance

Financial loss 70%

Cost and expenses related to;

- ☑ Business interruption and Extra expenses (like a PD/BI claim)
- ☑ Restoring the IT system to its state prior to the claim (PD/BI = costs to rebuild or replace)
- ☑ Maintaining operability of the IT system
- ☑ Restoring or replacing data
- ☑ Preparing the claim (Eg.: FAS)
- ☑ Preventing or mitigating a liability exposure/ detect and control any improper use of personal data (data breach)
- ☑ Communication strategy
- ☑ Ransom
- ☑ Notification to the authority or to individuals (Data breach)
- ☑ Defense costs resulting from an investigation by a regulator

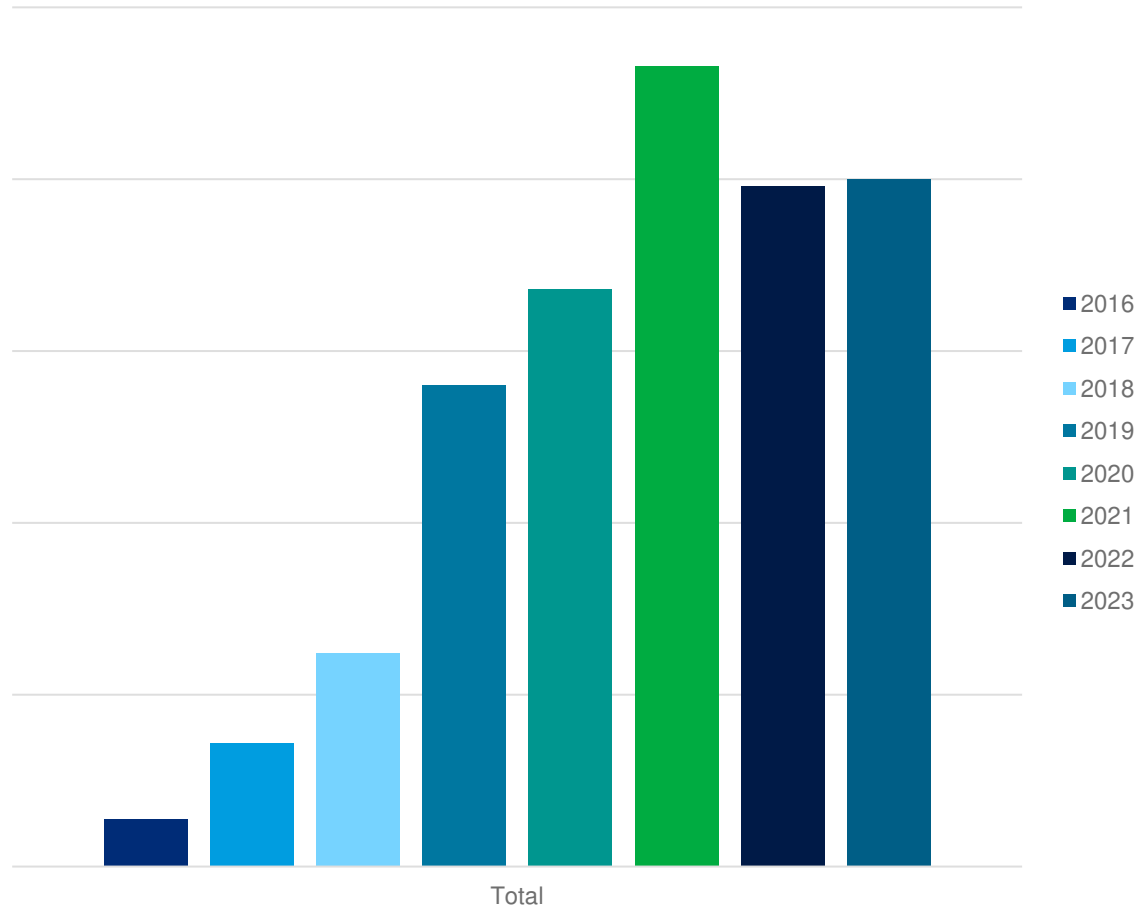
Liability coverage 5%

Defense costs and damages arising out of claims made by 3rd parties due to;

- ☑ A security event
- ☑ A breach of confidentiality of personal data
- ☑ Defamation, damage to reputation, breach of intellectual property, violation of privacy etc...

Cyber Claims Data Analysis

Claims Notifications by Year



The overall upward trend in cyber claims notifications continues.

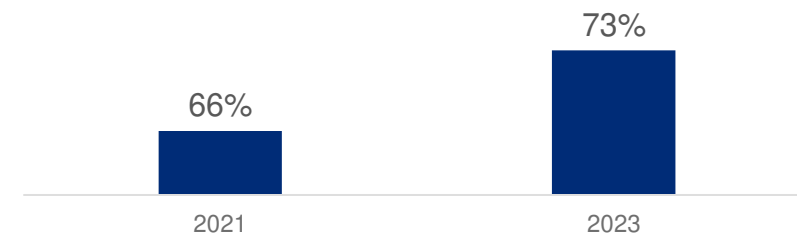


Only slight growth in claims notifications between 2022 and 2023, despite a significant increase in the number of cyber insurance policies



An increase in retentions and IT security maturity led to a relative decrease of number of claims notifications

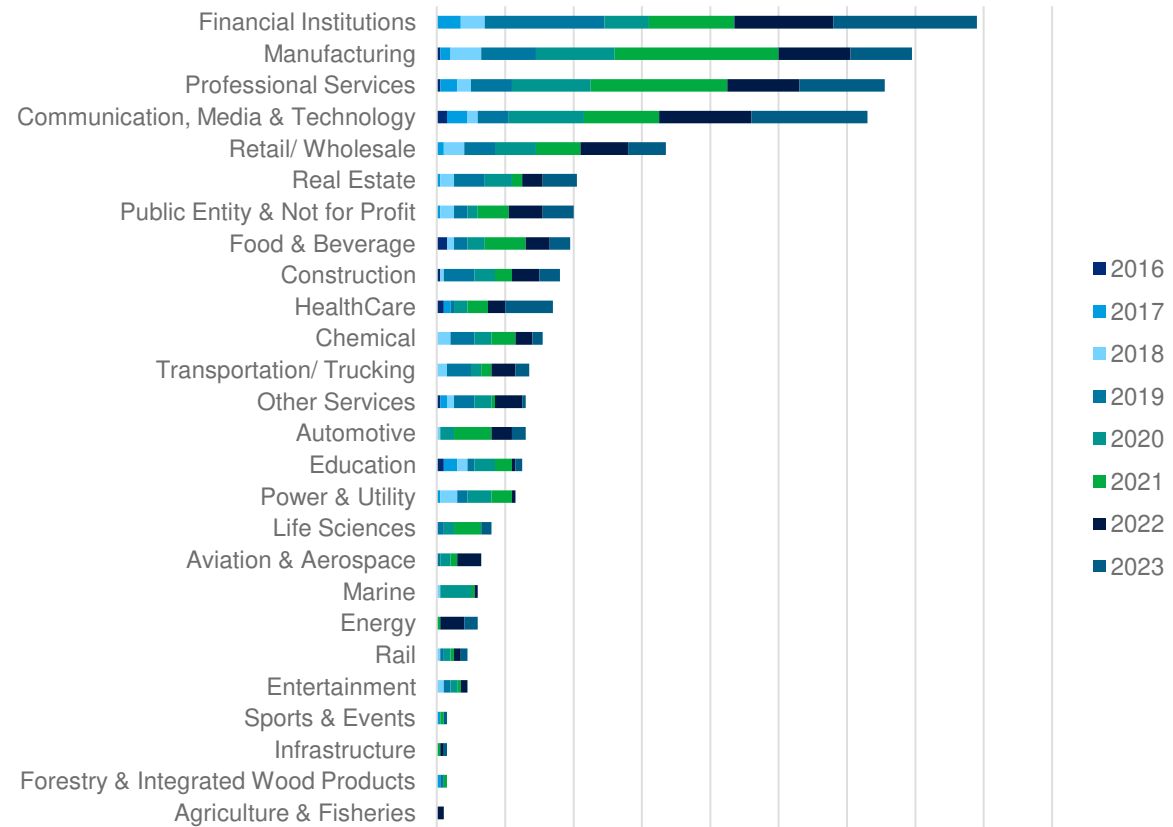
Average IT security maturity score evolution on 10 critical controls



Source: Marsh Global CSA

Cyber Claims Data Analysis

Claims notification by industry and year



2016-2023 Marsh Europe Cyber Claims Data



Manufacturing organizations' increase in maturity and resilience led to a decrease in claims notifications



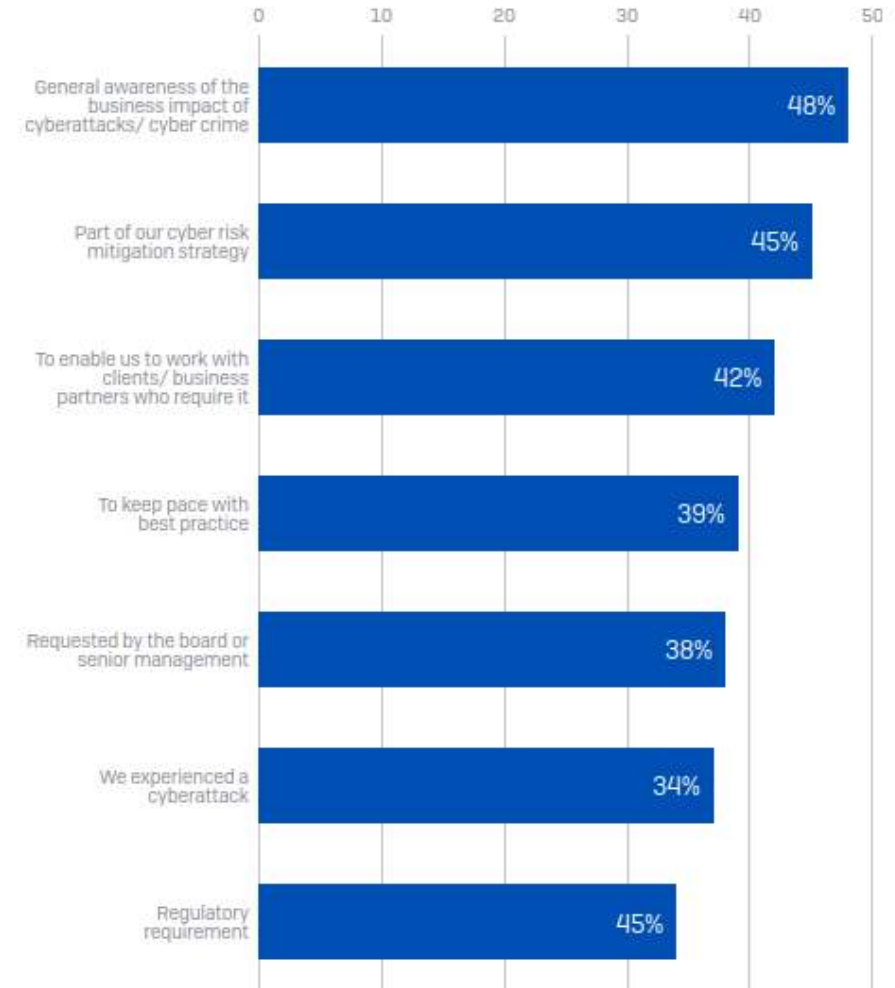
Increase in threat actors' focus on particularly vulnerable organizations from the technology sector



Digital supply chains remain under attack with effects for both technology providers and downstream users / customers

Reasons organizations purchase cyber insurance

Factors driving cyber insurance purchases



What main factor(s) drove the decision for your organization to purchase cyber insurance? n=4,498 organizations with cyber insurance.

Source: Cyber Insurance and Cyber Defenses 2024

The report is based on an independent survey commissioned by Sophos of 5,000 IT/cybersecurity leaders across 14 countries. The survey was conducted by Vanson Bourne between January and February 2024.

When is it not worth it?

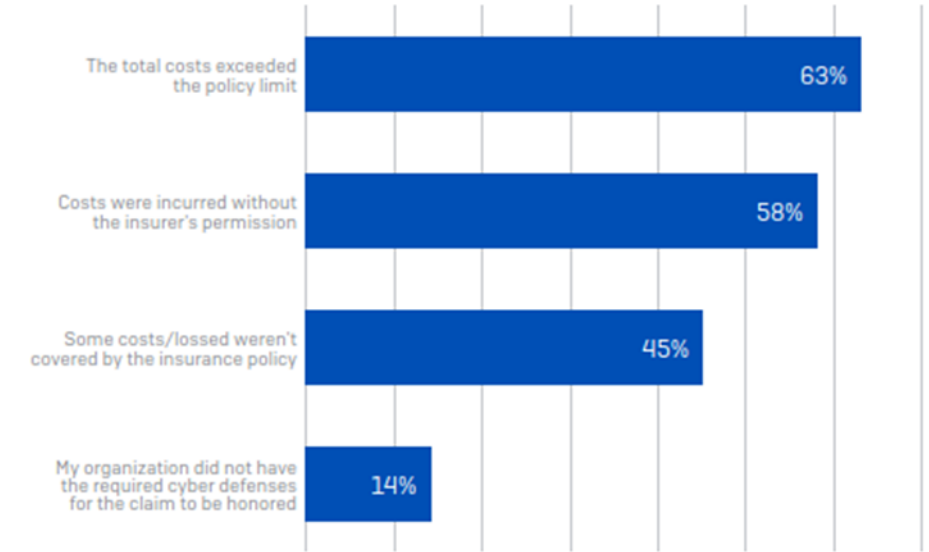
Room for improvement in understanding

A cyber insurance is not worth the money if you do not know **why**, **how much** you need it and **what** it covers!

We need to improve on:

- Onboarding with different stakeholders to explain cyber insurance and claims handling: Two of the most frequently seen reasons for coverage not getting triggered are the use of unapproved vendors and activity without insurer consent.
- Explaining what the intent of the cyber coverage is
- Explaining what is not the intent of the cyber insurance
- Make a risk-based approach on the need of a cyber insurance

Reasons why cyber insurance did not cover the full incident cost



Why didn't your organization's cyber insurance cover the total incident cost? n=3,886 organizations that did not have their full claim covered by the insurance provider

Policy coverages

	RANSOM PAYMENTS	DATA RECOVERY SERVICES	BREACH NOTIFICATIONS	PR SUPPORT/ REPUTATION MANAGEMENT	INCIDENT RESPONSE SUPPORT	BREACH NEGOTIATIONS	INCOME LOSS	COMPUTER SYSTEM RESTORATION
I know it covers this	50%	58%	47%	47%	54%	48%	49%	55%
I think it covers this, but it might not	40%	35%	43%	42%	38%	42%	41%	38%
I know it doesn't cover this	10%	7%	9%	11%	8%	10%	10%	7%
Don't know	0%	0%	0%	1%	0%	1%	0%	0%

What does your organization's cyber insurance policy cover in the event of a cyber incident? n=4,498 organizations with cyber insurance.

Real life claims

Some claim examples (1/5)

Norsk Hydro claims a further \$20.2mn from its cyber insurance in Q4

⚡ 7th February 2020 - Author: Luke Gallin

Aluminium manufacturing giant Norsk Hydro has announced that during the fourth-quarter of 2019, it recognised NOK 187 million (USD 20.2 million) of insurance compensation in relation to the cyber-attack on its operations in March, 2019.

The firm detected unusual activity on its servers that disabled part of its smelting operations, leading Norsk Hydro to isolate all plants and operations and switched to manual operations and procedures.

At first, Norsk Hydro said that the attack could cost as much as USD 41 million, with this figure jumping to USD 52 million and then to USD 69 million at the start of June.

The firm then said that the cyber-attack was likely to have a financial impact of up to NOK 650 million (USD 75 million) in H1 2019, noting that the majority of the operational challenges and financial losses hit its Extruded Solutions unit.

Norsk Hydro later revealed that during the third-quarter of 2019, it had recognised NOK 33 million (USD 3.6 million) in insurance compensation, with additional compensation expected to be recognised “when deemed virtually certain.”



Some claim examples (2/5)

A Car Dealership received an email from a threat actor (“TA”) stating that a system vulnerability from CRM vendor's side was exploited and TA had access to customer data such as SSNs, addresses, photographs of licenses, etc.

TA threatened to inform customers and foster reputational damage unless a ~ EUR 45,600 demand was met.

Through incident response panel of the insurer, the company engaged Legal Counsel, Forensic Experts, Credit Monitoring, Notification, and Call Centre Services.

Digital Forensic and Incident Response (“DFIR”) services found indicators of compromise in an employee’s email.

DFIR services requested and received loggings from the CRM and did not find any other unauthorized access. Therefore, the insured was advised against paying TA.

The policy paid EUR 50,000 in Cyber Services.

Some claim examples (3/5)

Following a ransomware attack the Insured's logistics software was encrypted, and their website through which they sell their products was down for nearly 9 days.

The Insured did not respond to the Threat Actors demands and no ransom was paid.

The Insured retained legal counsel, IT forensic specialists and a PR company, through the insurers' panel, in order to respond to and manage the incident.

Regulators in 4 countries were notified. The Insured also received formal complaints from 2 customers who claimed damages for their own expenses in connection with the incident.

The costs incurred were:

- Legal costs relating to breach response and for regulatory investigation;
- PR consulting costs;
- IT forensic costs;
- Costs for notification of the data subjects and
- Business interruption loss.

The payment by insurer was in excess of EUR 6Mio.

Some claim examples (4/5)

On 10 October 2018, food manufacturer Mondelez filed a lawsuit in Cook County Circuit Court of Illinois against Zurich North America after the insurance company denied a claim made under the company's all-risk **Property** insurance policy. Mondelez, says the incident damaged some 1,700 servers and 24,000 laptops, halting production and disrupting sales.


The complaint says the property insurance provided by Zurich covers “physical loss or damage to electronic data, programs, or software” caused by “the malicious introduction of a machine code or instruction”. The policy also extends cover to include business interruption and additional expenses “resulting from the failure of the insured’s electronic data processing equipment or media to operate resulting from malicious cyber damage”.

The Mondelez dispute highlights diverging views on cyber risk between the property and cyber insurance markets.

It is important to remember that the property insurance market, in all likelihood never intended to cover losses from events like NotPetya.

Ritz cracker giant settles bust-up with insurer over \$100m+ NotPetya cleanup

Deal could 'upend the entire cyber-insurance ecosystem and make it almost impossible to get meaningful cyber coverage'

 [Jessica Lyons](#)

Wed 2 Nov 2022 // 07:29 UTC

Mondelez International has settled its lawsuit against Zurich American Insurance Company, which it brought because the insurer refused to cover the snack giant's \$100-million-plus cleanup bill following the 2017 NotPetya outbreak.

Some claim examples (3/5)

The insured said that they overlooked an entity when answering the application form of the insurer, partly because the IT management for this specific company was outsourced to a professional party.

Insurers state in their application form:

*Where "Insured" is used in this form, it includes **the entire organization applying for coverage and all subsidiaries**. When the form is used to apply for a new insurance policy, "Insured" should be read as the prospective policyholder (including all subsidiaries).*

Despite the warning, it seemed that the insured made an error. Nevertheless, given the transparent explanation provided by the insured, For the insurer, it was established that the duty of disclosure under Article 7:928 of the Dutch Civil Code was not intentionally breached. However, it remains that the duty of disclosure under Article 7:928 et seq. was unintentionally breached.

This means that, pursuant to Article 7:930 of the Dutch Civil Code, **we need to assess what would have happened if the duty of disclosure had not been breached and our underwriters had received the correct information.**

In this case as the entity was small in size and some other circumstances the insurer has not attached any consequences to the insured's unintentional breach of the duty of disclosure.

Therefore, the insurers indemnified the insured in accordance with the policy terms and conditions.

Total: ~ EUR 240K

How to handle a cyber claim properly – feedback from our financial experts

Compensation period

Documenting and **retracing the events** from the infraction to the total recovery of the activity in order to precisely determine the compensation period.

Proof

Collecting and **keeping all evidence** related to the cyber attack as a proof of the means put in place to carry out the cyber attack.

Other costs related to the claim

Collecting as soon as possible all **evidence related to other costs** related to the claim:

- ✓ Discounts made to reduce the impact of the incident
- ✓ Costs related to crisis management, communication, notifications, legal advice, etc.
- ✓ Costs related to external experts intervention with detailed scope of work

Business interruption & additional costs

From the accidental/malicious event, collecting and keeping all **information regarding the business perturbation**:

- ✓ Information regarding loss of revenue
- ✓ Additional cost paid to reduce the business interruption period

Claims from third party

Listing the **potential claims from third party** affected by the cyber incident and potential penalties due to the non respect of the terms and conditions.

Search for responsibility

Exploring the **potential liability** of an accountable third party, if this one can be identified.

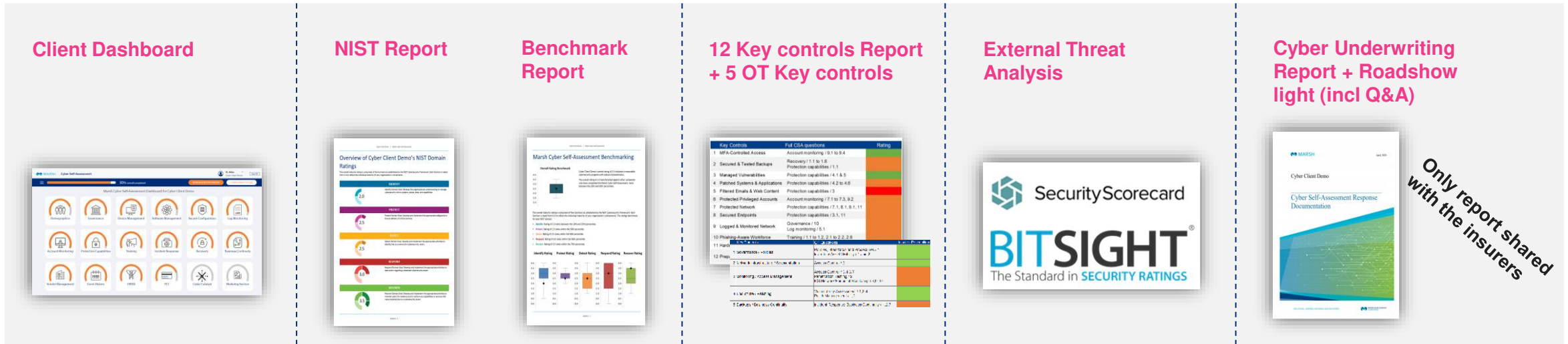
Financial information historic

Listing all the **financial records** of the 3 past years of all entities affected by the claim.

APPENDIX

The underwriting process for larger companies

Marsh's underwriting tool providing a 360 degree look at your organization's cybersecurity posture



Cyber Self Assessment, Marsh's underwriting tool providing 360° view of your organization's cybersecurity posture + OT CSA for manufacturing clients

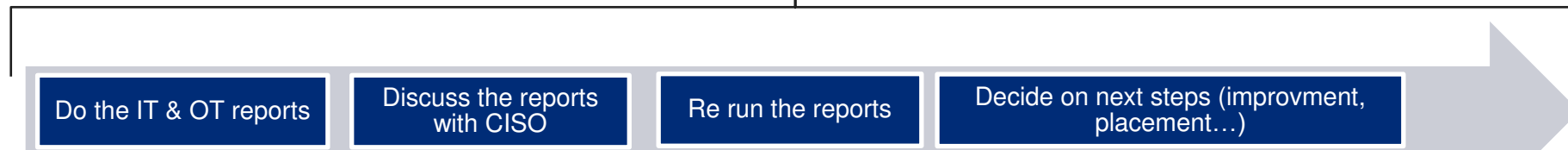
Reports produced based on the NIST framework (IT focussed)

Ransomware analysis based on the key 12 IT controls & 5 Key OT controls, from an underwriter's lens to preempt their questions

Non-intrusive external threat analysis of the information publicly available.

All of the demographic information and answers to the questionnaire, in a format understood and already accepted by cyber insurance underwriters.

Roadshow to answer to Q&A and no more questions from insurers



Top Cybersecurity Controls

The key to insurability, mitigation, and resilience

Preparation for the underwriting process:

1. Start early! Without positive responses in the top control categories, coverage offered and insurability may be in question.
2. Evaluate your cybersecurity maturity by completing Marsh's Cyber Self-Assessment – see appendix where improvements are needed.
3. Expect more rigorous underwriting and more detailed questions from underwriters.



Multifactor authentication for remote access and admin/privileged controls



Endpoint Detection and Response (EDR)



Secured, encrypted, and tested backups



Privileged Access Management (PAM)



Email filtering and web security



Patch management and vulnerability management



Cyber incident response planning and testing



Cybersecurity awareness training and phishing testing



Hardening techniques, including Remote Desktop Protocol (RDP) mitigation



Logging and monitoring/network protections



End-of-life systems replaced or protected



Vendor/digital supply chain risk management

Marsh Cyber Self-Assessment

Output: 12 Key IT ransomware controls & 5 Key OT ransomware controls

Key ransomware control; how did you score on IT?

	Key Controls	CSA Questions	Insurer Perception
1	MFA-Controlled Access for remote access & admin / privileged access	Account monitoring / 8.1 to 8.4	
2	Secured, encrypted and tested backups	Recovery / 1.1 to 1.8 Protection capabilities / 1.1	
3	Patched Systems and Managed Vulnerabilities	Protection capabilities / 4.1, 4.2 to 4.6, 5.1	
4	Filtered emails & web content	Protection capabilities / 3.1 to 3.2	
5	Privileged Account Management (PAM)	Account monitoring / 7.1 to 7.3, 9.2	
6	Endpoint Detection and Response (EDR)	Protection capabilities / 3.1, 11	
7	Logging & Monitoring / Network Protections	Governance / 10.1 to 10.2 Log monitoring / 5.1	
8	Cybersecurity awareness training and phishing training	Training / 1.1 to 1.2, 2.1 to 2.2, 2.6	
9	Hardening techniques including Remote Desktop Protocol (RDP)	Secure configuration / 1.1, 2.1	
10	Cyber Incident Response planning and testing	Business continuity / 1,1 Incident response / 1.2 to 1.3, 2.4, 4.1	
11	End-of-life systems replaced or protected	Protection Capabilities / 6.1	
12	Vendor / Digital Supply Chain Risk Management	Governance / 11.1 to 11.3, 12.1 to 12.2	

Key ransomware control; how did you score on OT (when relevant)?

	Key Controls	OT Questions	Insurer Perception
1	Governance / Policies	Policies, Standards and Procedures / 1 Inventory Asset Visibility / 1 and 2	
2	Network Infrastructure / Segmentation	Access Control / 2	
3	Monitoring / Access Management	Access Control / 3,4,6,7 Penetration Testing / 2 ICS Network/Endpoint Monitoring / 3,9,10	
4	End-of-life / Patching	Vulnerability Assessment / 1,3,4 Patch Management / 1,2	
5	Backups / Business Continuity	Incident Response Business Continuity / 1,2,7	



This document and any recommendations, analysis, or advice provided by Marsh (collectively, the “Marsh Analysis”) are intended solely for the entity identified as the recipient herein (“you”). This document contains proprietary, confidential information of Marsh and may not be shared with any third party, including other insurance producers, without Marsh’s prior written consent. Any statements concerning actuarial, tax, accounting, or legal matters are based solely on our experience as insurance brokers and risk consultants and are not to be relied upon as actuarial, accounting, tax, or legal advice, for which you should consult your own professional advisors. Any modeling, analytics, or projections are subject to inherent uncertainty, and the Marsh Analysis could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy. Marsh shall have no obligation to update the Marsh Analysis and shall have no liability to you or any other party with regard to the Marsh Analysis or to any services provided by a third party to you or Marsh. Marsh makes no representation or warranty concerning the application of policy wordings or the financial condition or solvency of insurers or reinsurers. Marsh makes no assurances regarding the availability, cost, or terms of insurance coverage. All decisions regarding the amount, type or terms of coverage shall be your ultimate responsibility. While Marsh may provide advice and recommendations, you must decide on the specific coverage that is appropriate for your particular circumstances and financial position. By accepting this report, you acknowledge and agree to the terms, conditions, and disclaimers set forth above.

Copyright © 2023 Marsh LLC. All rights reserved.

A business of Marsh McLennan