Allianz

Cyber Claims excellence – before, during and after a Cyber hack

Allianz Commercial Webinar

Munich | October 4, 2023

We are Cyber & Cyber Claims Ready!

1. Experience
2. Expertise
3. Passion
4. Support: we help you before, during and after a cyber-attack!

Agenda & Team

1. What are the biggest Cyber risks evolving in 2023?
   - A Cyber Claims Trends 2023 – The attackers are back
   - B The toxic cocktail of data exfiltration and tightening data privacy regulation
2. How can companies best prepare against cyber-attacks?
   - A The new key to Cyber defense: Detection and Response capabilities
   - B Detection and Response in practice – key learnings and insights
3. What are success factors when dealing with such an attack?
4. How will Allianz and our partners assist and how can you benefit from our knowledge?
   - A Managing a Cyber Crisis as a team
   - B Closing the loop – using Cyber Claims intelligence for enhanced client benefit


Thomas Sepp


Joerg Ahrens


Michael Daum


Sabrina Sexton


Rishi Baviskar


Robin Kroha


Rosehana Amin


Henning Schaloske


Alexander Fink


Roberta Morrell


Alexander Pabst


Dominik Geistanger


Michael Sauermann


Robert Feser


Tilmann Ohlinger

Please support us with your views and expertise

Please share your views directly in **Webex** using the window on the right side.

Or scan the **QR code**:

Or share online at **slido.com** ('Join as a participant') and enter the passcode: **azc-cyber**

Agenda & Team

1. **Cyber Claims trends 2023 – the attackers are back**
2. The toxic cocktail of data exfiltration and tightening data privacy regulation
3. The new key to Cyber defense: Detection and Response capabilities
4. Detection & Response at Allianz Group – our key learnings and insights
5. Success factors of handling and mitigating Cyber Claims
6. Managing a Cyber Crisis as a team!
7. Closing the loop – using Cyber Claims intelligence for enhanced client benefit

Thomas Sepp
Chief Claims Officer
Allianz Commercial

Your participation: Please share your views

Allianz

What is the average ransom demand as of Q2 2023?

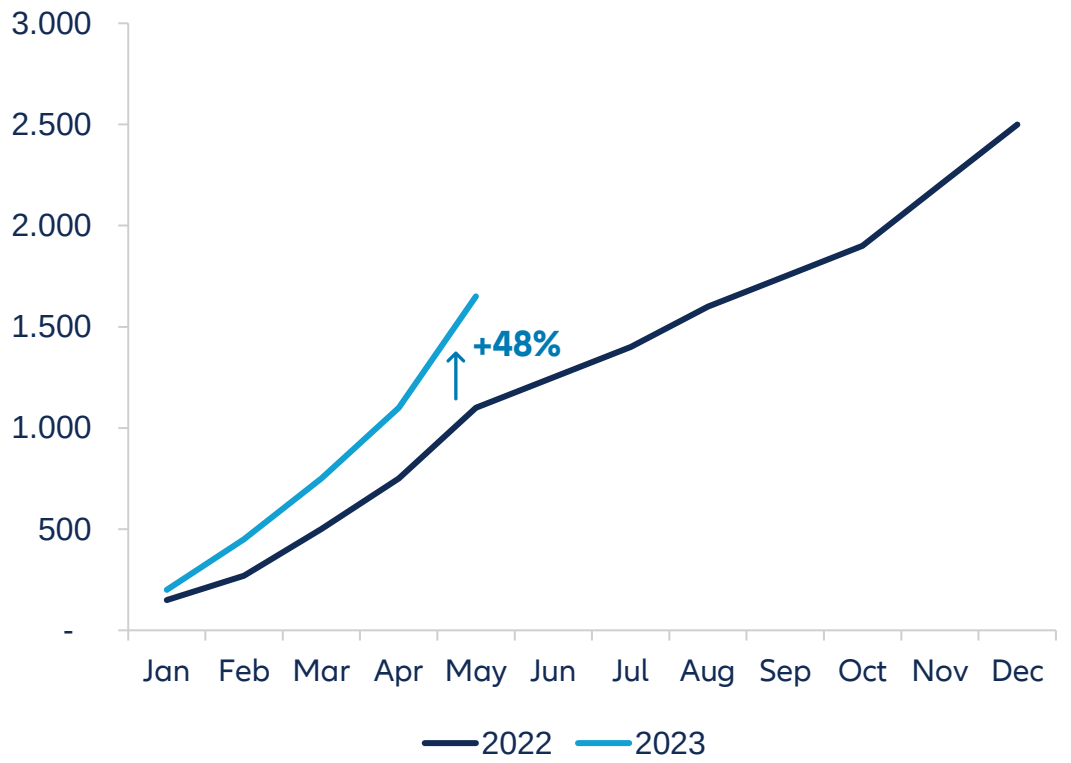
- A $1M
- B $2.5M
- C $5M
- D $10M

Please go to slido.com and use code #azc-cyber

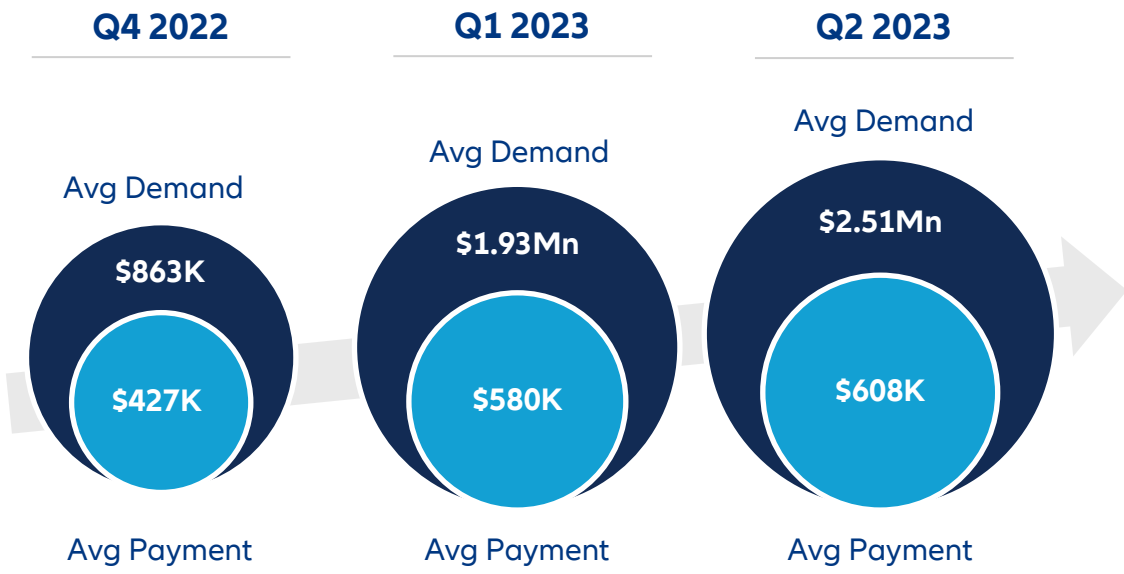
Ransomware activity is up nearly 50% to last year

Allianz

Market data shows ransomeware activity is up ~50%[1] ...



...and ransom payments are getting more expensive[2]

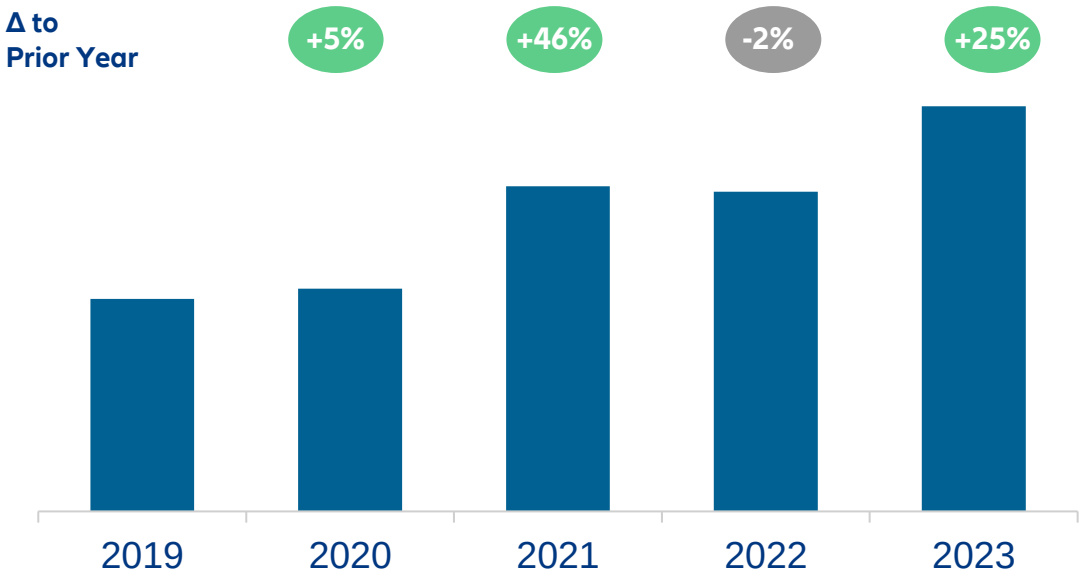


- CL0P group Mass Exploits of a single vulnerability in Q1 & Q2
- More active ransomware groups

1. Source: Howden Analysis based on data from NCC Group
2. Source: Corvus Q2 Ransomeware Report: Global Attacks at All-Time High

Allianz sees a cyber uptick in 2023, but not to the same extent

Based on 6M 2023 figures, we expect a ~25% increase in number of claims YoY at the end of 2023



Focus remains on risk appetite & risk improvement with clients

Key defenses required today to fight severity

- Strong Detection
- Fast Response Capabilities
- Ransomware Protection Checklist:

Ransomware Identification	Backups	Segmentation
Business Continuity & Incident response	Endpoints	Monitoring patching & vulnerability policies
Anti-phishing and awareness training	Email, web, office document security	Mergers & Acquisitions

1. Cyber LoB (excluding Coalition, Tech, OEs)

New tactics to 'turn up the heat', driving severity in large losses

Allianz

Emerging tactics from attackers	Analysis of our own large loss data confirms this trend
Data exfiltration *(In addition to encryption)*	**75%** of cases involve successful sensitive data exfiltration Increased from ~40% in 2020
Making cases public	**Almost 100%** of cases become public Increased from 75% in 2020
Higher willingness to pay the ransom	**50%** of companies finally pay the ransom Increased from ~40% in 2020

Various underlying trends support the attractivity of Data exfiltration to attackers

Attractivity of Data exfiltration

1. Scope and amount of personal information collected is increasing
2. Use of Outsourcing/Cloud and remote access lead to more interfaces/APIs
3. Tightening data privacy laws around the globe + increased public sensitivity

! Companies are **2.5x more likely to pay a ransom** if data is exfiltrated, in addition to encrypted

Agenda & Team

1. Cyber Claims trends 2023 – the attackers are back
2. **The toxic cocktail of data exfiltration and tightening data privacy regulation**
3. The new key to Cyber defense: Detection and Response capabilities
4. Detection & Response at Allianz Group – our key learnings and insights
5. Success factors of handling and mitigating Cyber Claims
6. Managing a Cyber Crisis as a team!
7. Closing the loop – using Cyber Claims intelligence for enhanced client benefit

Rosehana Amin
Partner, specialized in Cyber & Data protection in coverage matters, breach incident response and litigation
Clyde & Co

Henning Schaloske
Partner, Head of Continental European Insurance practice
Clyde & Co

2018

New horizons

New Risks

Your participation: Please share your views

What is the amount of GDPR fines levied on companies for GDPR breaches?

- A >EUR 500m
- B >EUR 2BN
- C >EUR 4BN
- D >EUR 10BN

Please go to slido.com and use code #azc-cyber

GDPR: 5 years on

Allianz

Largest fines issued

€1.2 Bn
against Meta in Ireland

€746 M
against Amazon in Luxembourg

€405 M
against Meta in Ireland

€390 M
against Meta in Ireland

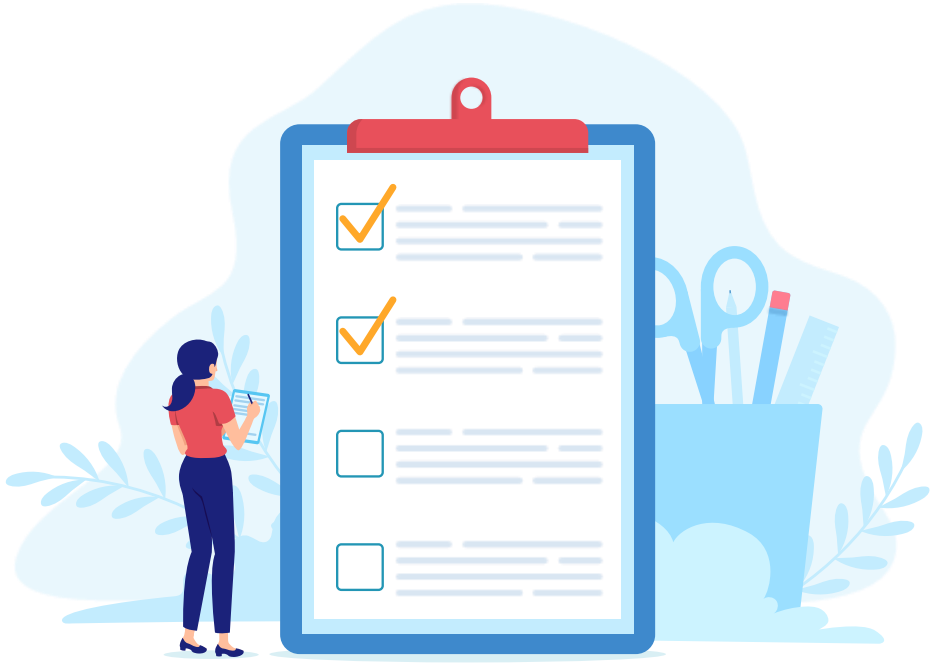
Data exfiltration and court decisions

In Armstrong Watson LLP v Persons Unknown [2023] EWHC 1761 (KB) the English High Court has granted a final injunction in default of defence to a claim for breach of confidence in a case involving ransomware and financial blackmail i.e. the threat actor cannot publish or disclose any of the information they got their hands on in the data breach

What is the value of an injunction against unknown persons? To show that you are doing everything you can.

Horizon scanning

- Evolution of data privacy laws
  - AI is a key topic for new legislation
  - EU Digital Operational Resilience Act (DORA) entered into force earlier this year (to apply from 17 January 2025), applying to financial entitles regulated at EU level
  - Biometric data is a hot topic at the moment
- Social inflation and the value of claims



Your participation: Please share your views

How relevant have Cyber liability claims been so far?

- A Low
- B Medium
- C High

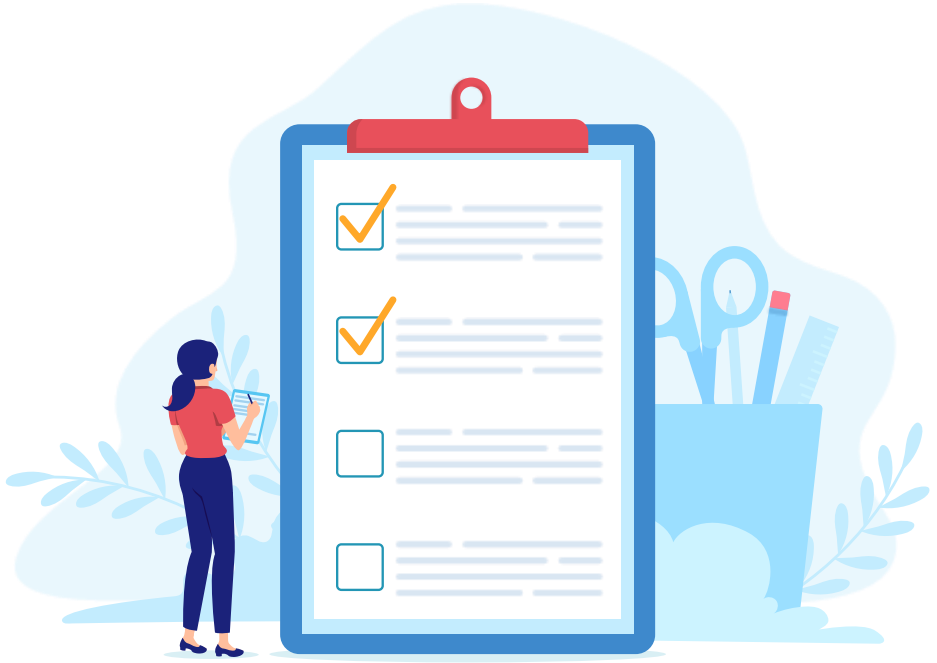
Please go to slido.com and use a code #azc-cyber

EUR 2.500

Art. 82 GDPR –
Right to compensation and liability

- Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

- (...)

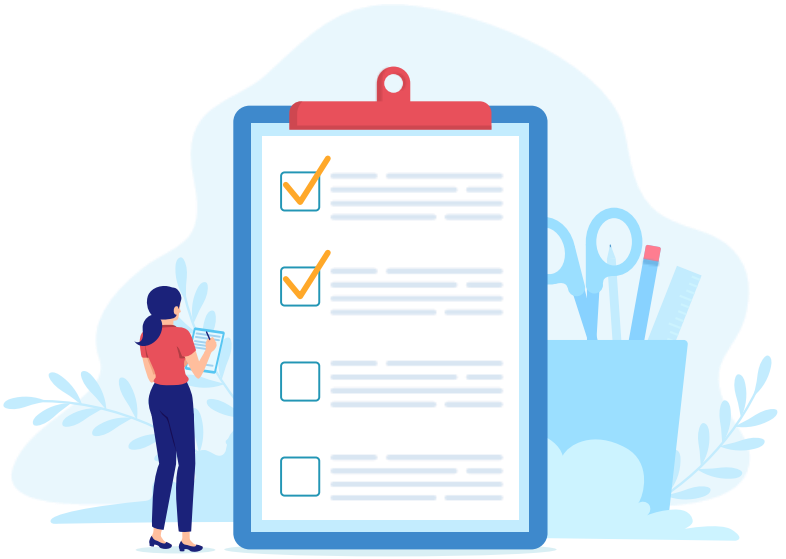



Allianz

Litigation for wrongful data collection is here to stay – The EU ECJ rulings on Art 82 GDPR

ECJ, judgment of 4 May 2023, C-300/21 – Österreichische Post AG

- Österreichische Post AG used an algorithm to determine political preferences of customers. The plaintiff claimed non-material damages in the amount of EUR 1,000.
- The national courts refused to award damages, but referred the question to the ECJ.
- The ECJ ruled that the mere infringement of the provisions of that regulation is sufficient to confer a right to compensation.
- The damage is not subject to a 'threshold of seriousness', but the plaintiff must show and, if necessary, prove a non-material damage.
- National courts must apply the domestic rules relating to the extent of financial compensation, based a compensatory function on not of a punitive nature.



Litigation for wrongful data collection is here to stay – The UK

01 The Data Protection and Digital Information (No. 2) Bill is working its way through the Parliamentary processes.

02 Data collection – Cookies

03 Gormsen v Meta Platforms Inc, a claim in the Competition Appeals Tribunal

Litigation for wrongful data collection is here to stay – US class actions

Allianz

01 Illinois Biometric Information Privacy Act (BIPA)

02 Meta Pixel litigation

03 Video Privacy Protection Act (VPPA)

Your participation: Please share your views

How relevant will cyber liability claims be in the future?

- A Low
- B Medium
- C High

Please go to slido.com and use code #azc-cyber

I

(Legislative acts)

DIRECTIVES

DIRECTIVE (EU) 2020/1828 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 25 November 2020

on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC

(Text with EEA relevance)

EUR 2.500 x 33.200

= EUR 83m

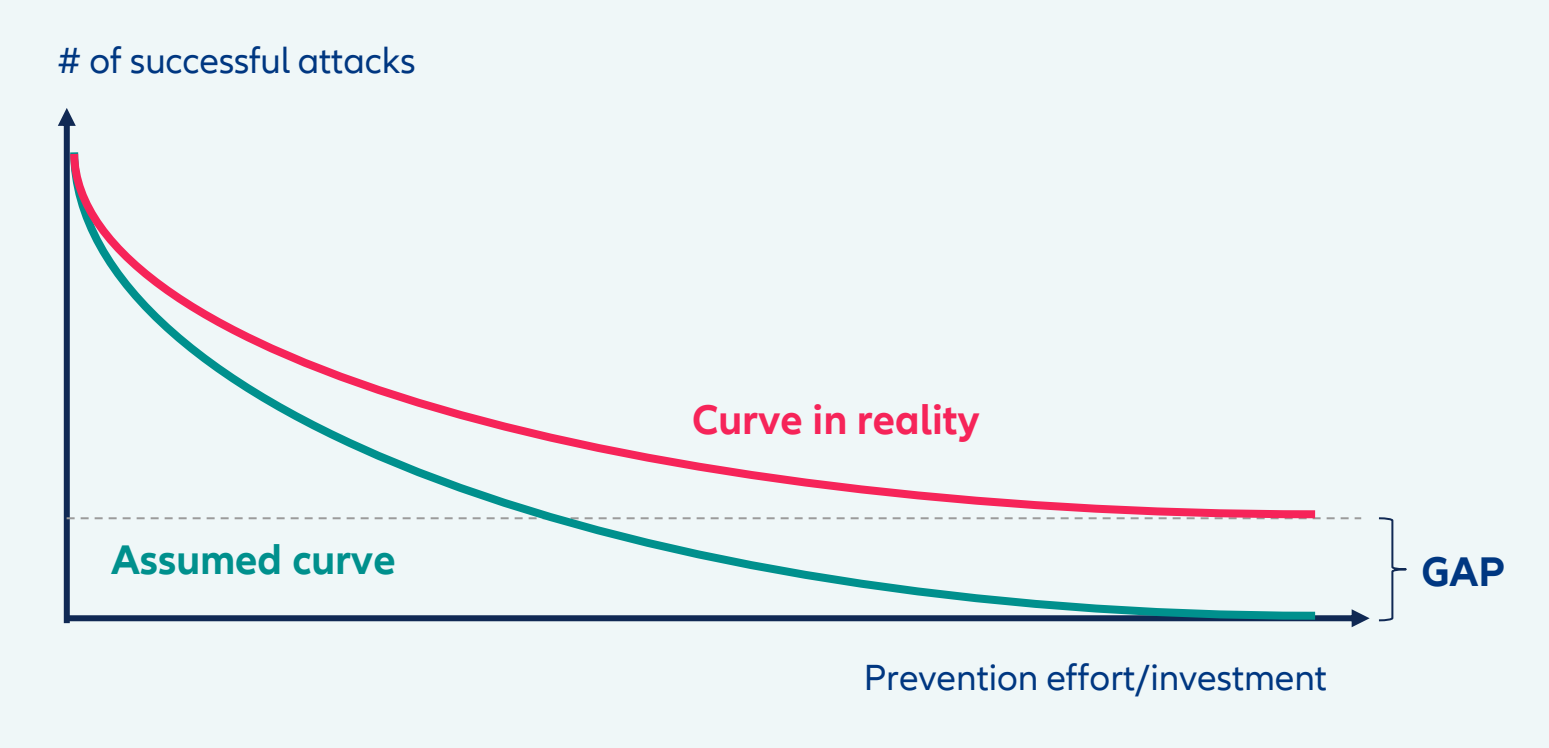
Agenda & Team

1. Cyber Claims trends 2023 – the attackers are back
2. The toxic cocktail of data exfiltration and tightening data privacy regulation
3. **The new key to Cyber defense: Detection and Response capabilities**
4. Detection & Response at Allianz Group – our key learnings and insights
5. Success factors of handling and mitigating Cyber Claims
6. Managing a Cyber Crisis as a team!
7. Closing the loop – using Cyber Claims intelligence for enhanced client benefit

Rishi Baviskar
Global Head of Cyber Risk Consulting
Allianz Commercial

Michael Daum
Global Head of Cyber Claims
Allianz Commercial

How to edge out the attackers? Just adding more of classic prevention mechanism will not suffice!



Key reasons for GAP

01 Attackers improve

02 Human factor

03 Comfort & cost

04 Lack of full overview

- Accept to be breached every once in a while
- Prevention drives frequency, Detection & Response capabilities will determine severity

Many of our claims examples confirm limitations of Prevention focused defense

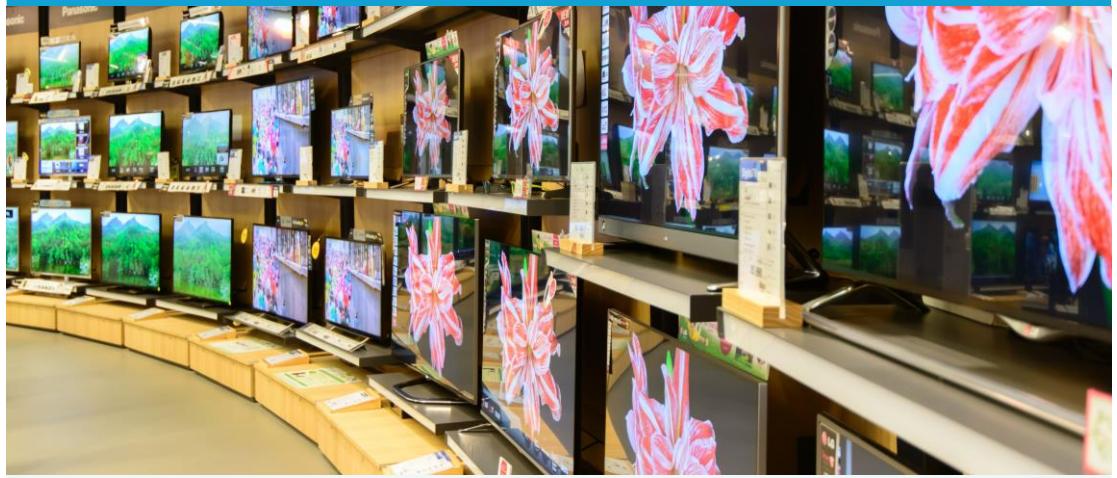
Allianz

Lack of full overview

Target: Strong security in place across all countries & subsidiaries

Reality: Weak security in foreign subsidiary not monitored by Headquarter

Comfort & cost

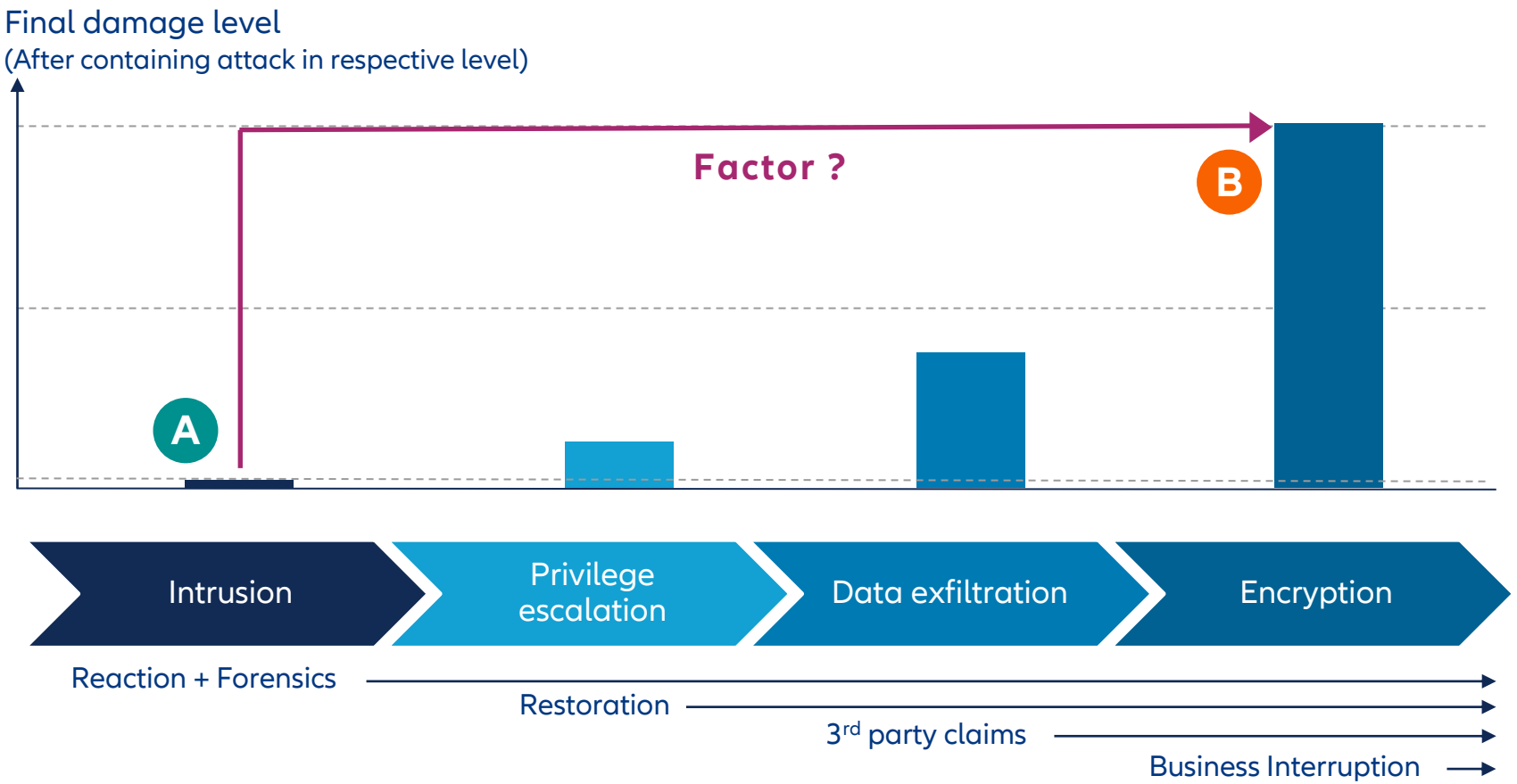


Target: Use of corporate devices only and MFA enabled for all external access

Reality: Granted use of private devices with MFA disabled to enable remote work during Covid crisis

Value of loss mitigation delivered by Detection and Response is tremendous

Allianz



2 Scenarios

A Attacker manages to bypass prevention mechanisms and infect a PC

B Attacker successfully gains admin rights, exfiltrates data and encrypts large parts of the computer system

Mindset limits investments in Detection & Response capabilities, particularly in smaller companies

Allianz

Elements many clients are missing today

- Understanding of how adversaries work
- “Assume breach" mindset
- Proactive instead of reactive threat detection
- You can’t do everything

Detection & Response capabilities fall behind Prevention

	Ranking	
	Your view	Our clients
Prevention	Slido poll	1 (~90%)
Detection		2 (~75%)
Response		3 (~65%)

SME View

- SME companies generally care and invest less, yet can’t treat cyber security as an afterthought
- **Only 4% of small business owners say cybersecurity is the biggest risk to their business**
  – CNBC Small Business Index Q4 2022

Allianz Cyber Risk Consultants helps Clients understand and implement our Claims learnings

What we look for in terms of Detection and Response

- Real time vulnerabilities and attacks detection
- Remediation workflow to protect the company
- Defence-in-depth model
- Faster and more accurate response

How we as Risk Consultants support our Insureds

- Provide global insights and benchmarking
- Run independent, risk-focused assessments
- Support improving clients' IT security year on year

We see constantly improving prevention, detection and response mechanisms for our clients

> "You can't fight what you can't see."

Agenda & Team

1. Cyber Claims trends 2023 – the attackers are back
2. The toxic cocktail of data exfiltration and tightening data privacy regulation
3. The new key to Cyber defense: Detection and Response capabilities
4. **Detection & Response at Allianz Group – our key learnings and insights**
5. Success factors of handling and mitigating Cyber Claims
6. Managing a Cyber Crisis as a team!
7. Closing the loop – using Cyber Claims intelligence for enhanced client benefit

Alexander Pabst
Deputy Chief Information Security Officer
Allianz Group

Robert Feser
Head of Allianz Cyber Defense Center
Allianz Technology

Michael Sauermann
Partner, Head of Forensic Technology Germany & EMA
KPMG

Agenda & Team

1. Cyber Claims trends 2023 – the attackers are back
2. The toxic cocktail of data exfiltration and tightening data privacy regulation
3. The new key to Cyber defense: Detection and Response capabilities
4. Detection & Response at Allianz Group – our key learnings and insights
5. **Success factors of handling and mitigating Cyber Claims**
6. Managing a Cyber Crisis as a team!
7. Closing the loop – using Cyber Claims intelligence for enhanced client benefit

Tilmann Ohlinger
Senior Cyber Claims Expert
Allianz Versicherungs AG

Roberta Morrell
Senior Cyber Claims Expert
Allianz Commercial

Dominik Geistanger
Senior Cyber Claims Expert
Allianz Commercial

Not only an IT incident – Rather a severe crisis of the organization

Client was hit by a ransomware attack. Before external support was called in, the affected system was restored from the latest backup. After the attackers had broken into the system a while before, the backup was also affected and the network was reinfected. Through the autonomous recovery process new complications arose.

1

Important forensic traces were lost

2

The forensic analysis subsequently commissioned and conducted was also compromised

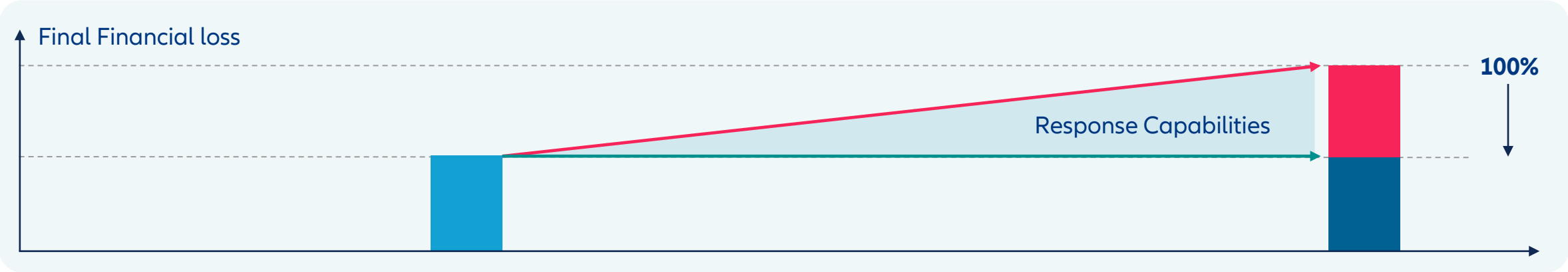
3

Recovery effort was significantly higher

Responding to such a severe crisis requires timely involvement of many parties

1	• PR & Crisis Management	• Sales • Communications
2	• System Recovery • Business interruption • Ransom	• IT • Finance • Legal
3	• Awareness of exposure • Monitor Security Standards • Continuous Insurance Cover	• Insurer

Response capabilities have a significant effect on the financial loss originating from a cyber event



- Response capabilities can manage claim in a certain bandwidth (Indemnity, Ransom, Fine,...)
- Partner network is key and Insurers can meaningfully assist

Enhancing "Cyber Incident Readiness" of an Organisation (1/2)

Allianz

General rule

We as an insurer can offer support in order for you to better handle the crisis, but we cannot handle the crisis for you

Aim

Ensure short response times and decision making processes where possible throughout the whole cyber incident handling

Enhancing "Cyber Incident Readiness" of an Organisation (2/2)

Selection of important topics to consider

Proper understanding of your cyber exposure

- Sound crisis management – and business continuity plans
- PR strategy with focus on cyber incidents
- Involvement of public authorities
- Prepare engagement of external service providers in advance
- Obtain "prior written approval" from Allianz where necessary

Involving insurers early

Allianz

Ensures the insurance recovery process runs smoothly

- Notification obligations and prior consent provisions within the policy
- Early understanding of supporting document requirements (vendor invoices & BI losses)

Allows you to leverage insurers and vendors expertise to minimise the incident impact

- Data/intel on threat actors and similar incidents (ransom payment reductions etc.)
- Access to pre-negotiated rates
- Insured's existing IT vendor vs. independent vendor
- Internal Allianz IT expertise
- Vendors beyond IT expert – legal advice on notification obligations (customer & regulators)/ PR advice etc.

Enables you to ensure you are compliant with sanctions requirements

- Advice from experts on ransom payments so you can avoid the risks of non-compliance with rules on sanctions

Case Study – leveraging insurers expertise to minimize the incident impact

1. Client discovered suspicious activity in their network and initiated incident response measures
2. Confirmed unauthorized access and large amount of data exfiltrated
3. Spread of ransomware could be contained and extortion demands from the attackers were not met
4. Client needed to evaluate and assess the compromised data – their usual vendor offered an investigation of the whole data package for a €10M fee
5. Client approached Allianz in order to verify whether the offer as reasonable
6. With the assistance of our colleagues from Allianz Technology, we were able to convince the client to conduct a public tender
7. Alternative service provider who offered to examine the data package for **30% of the original offer**

Agenda & Team

1. Cyber Claims trends 2023 – the attackers are back
2. The toxic cocktail of data exfiltration and tightening data privacy regulation
3. The new key to Cyber defense: Detection and Response capabilities
4. Detection & Response at Allianz Group – our key learnings and insights
5. Success factors of handling and mitigating Cyber Claims
6. **Managing a Cyber Crisis as a team!**
7. Closing the loop – using Cyber Claims intelligence for enhanced client benefit

Robin Kroha
Head of Global Protection and Resilience
Allianz Services

Alexander Fink
Partner, specialized in Crisis Management & Communications
Kekst CNC

Proper preparation prevents poor performance

Reduce complexity

- Not a complicated IT issue
- Instead, a complex top management challenge
- Many agents (IT, legal, forensics, risk management, finance, communications, sales, marketing), very little time: minutes, not hours or days

Maximise speed

- Decisions taken in the first minutes decide success or failure
- Plans, training, coaching, and exercises are the only way to increase speed

Leverage agility and creativity

- Crisis management is an agile process requiring creativity
- Crisis management generates knowledge based on incomplete data an information
- Crisis management can, however, be influenced by outside parties

Your participation: Please share your views

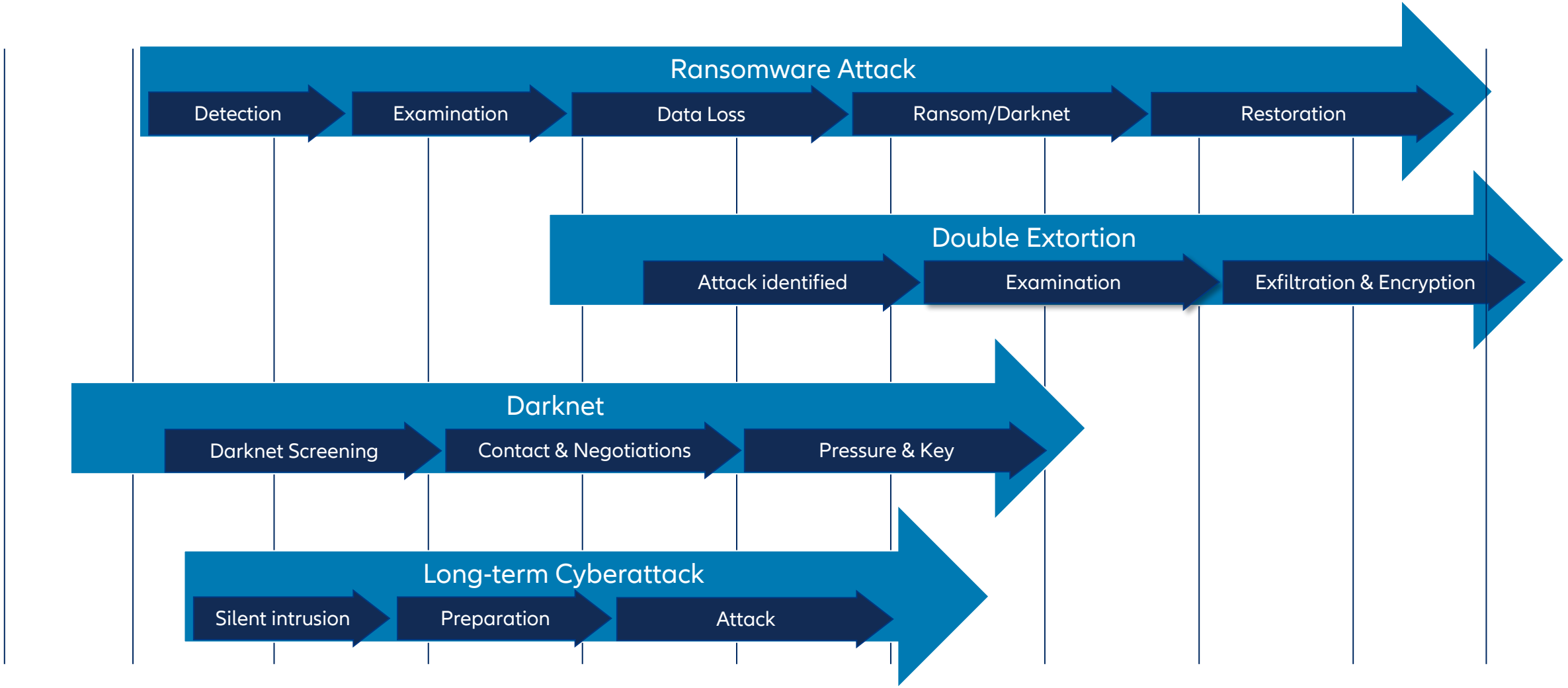
1. **When was your company last hit by a cyberattack?**
   - In the last year
   - More than a year ago
   - It was not hit

2. **Do/Did you work with external partners to master a cyber crisis?**
   - Yes
   - No

3. **When did you last perform a cyber crisis management exercise?**
   - In the last 12 months
   - In the last 24 months
   - No exercise performed

Please go to slido.com and use code #azc-cyber

Key challenges in various scenarios



Agenda & Team

1. Cyber Claims trends 2023 – the attackers are back
2. The toxic cocktail of data exfiltration and tightening data privacy regulation
3. The new key to Cyber defense: Detection and Response capabilities
4. Detection & Response at Allianz Group – our key learnings and insights
5. Success factors of handling and mitigating Cyber Claims
6. Managing a Cyber Crisis as a team!
7. **Closing the loop – using Cyber Claims intelligence for enhanced client benefit**

Joerg Ahrens
Global Head of Key Case Management (LT)
Allianz Commercial

Sabrina Sexton
Head of SME & MidCorp
Cyber Center of Competence
Allianz Commercial

Rishi Baviskar
Global Head of Cyber Risk Consulting
Allianz Commercial

Michael Daum
Global Head of Cyber Claims
Allianz Commercial

Thank you!

commercial.allianz.com
Allianz Commercial
az.commercial.communications@allianz.com