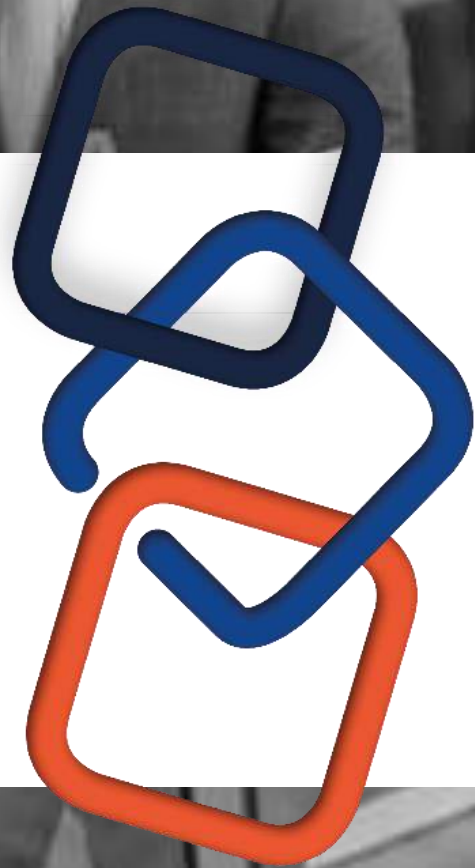




BELRIM

Belgian Risk Management Association



AI & Cyber Risk
10 / 10 / 2024



Cyber insurance

HOWDEN

Agenda

- 01** AI – impact on cyber risk, and what you can do as Risk Managers
- 02** The Risk Manager’s burden of explaining cyber risk
- 03** The CrowdStrike incident – how cyber insurance is growing up

- 04** Cyber for SMEs – watch the connections
- 05** Cyber insurance market update

AI and cyber risk



Mikko Peltonen
Cyber
Consultancy
Lead, Northern
Europe & UK

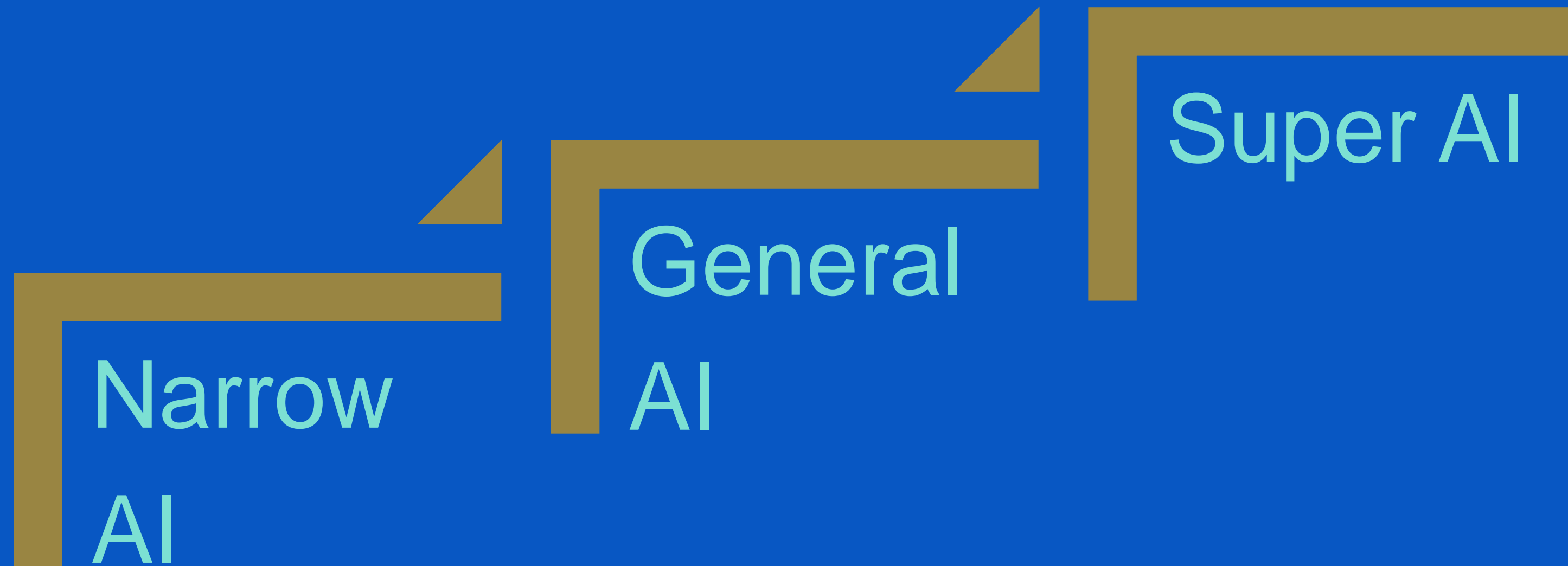
HOWDEN



AI and Cyber Risk: What Risk Managers Need to Know and Do

Mikko Peltonen
Cyber Consultancy Lead, Northern Europe &
UK

Classes of AI



A game changer in Cyber Risk?

- **AI has dual impact**
 - Accelerator of cyber risks
 - But also a powerful tool for risk mitigation
- **Already current AI has some real damage potential:**
 - Automating time consuming tasks in crafting cyber attacks
 - Generative AI already used to craft more realistic and credible phishing messages
- **Most troublesome for SMEs with no dedicated IT staff, struggling the most with patching the systems**

THE STRAITSTIMES

13% of phishing scams analysed likely to be AI-generated: CSA



Adversary Use Cases

Gen AI for phishing scams

Deepfake generation

AI assisted targeting

AI-powered cyber attacks

Defense Use Cases

Intelligent detection

AI Detection of deepfakes

AI assisted threat hunting

Adversary simulation

“The combination of increased automation, easy-to-use attack frameworks, and trained AI that assists threat actors will not necessarily make threat actors more advanced but more efficient. “

Source: Truesec Threat Intelligence Report 2024, Truesec AB

Upsides of AI for Cyber Defenders May Outweigh the Downsides

- Generative AI can be a great sparring partner and source of inspiration
 - E.g. play devil's advocate with an artificial adversary, helping to pinpoint attack vectors
 - Predict weaknesses in security posture before they become a risk
 - **Example:** security monitoring and threat hunting
 - Security analysts regularly scans large amounts of data in attempt to find needles in haystacks (e.g. abnormal login patterns etc.)
 - AI can do this in or almost real time
-

Practical Tips to Risk Managers

- Low tech solutions to protect against AI assisted attacks
 - Call back processes, eye to eye verification, 4 eyes principle
 - Be mindful that even caller ID can be spoofed
 - Monitor the use of AI:
 - encourage the benevolent
 - discourage harmful types of use
 - Understand and manage both your risk and your opportunities
 - Implementation of policies across your organisation
 - Stay up to date with the latest developments in AI as well as the new regulations i.e. EU AI Act
 - Include AI in risk assessments - e.g. what the adversaries might be able to accomplish or figure out with a clever use of AI
-

Summary

- 99% of all cyber risk is still traditional – non-AI based, but this may change very fast
 - Embrace proactive approach:- To predict is better than to prevent
 - Finally: Current form of AI is just a tool – an evolution, not a revolution – in computer science, and benefits both offensive and defensive sides of the equation
-

The Risk Manager's burden

Kristoffer
Haleen

HOWDEN



Choose your battles

“He who defends everything, defends nothing.”

– Frederick the Great





CrowdStrike Cyber insurance is growing up

Kristoffer
Haleen

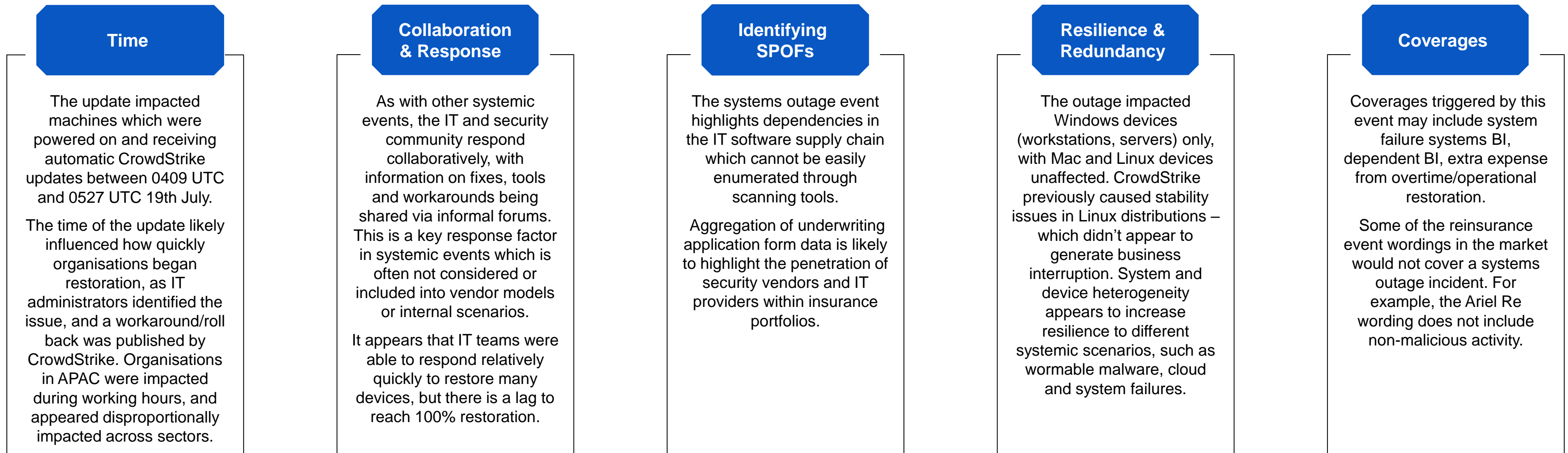
HOWDEN

CrowdStrike IT Systems Failure

Preliminary observations from the CrowdStrike mass IT outage

Within a 90-minute period on 19th July, a flawed CrowdStrike endpoint detection and response (EDR) software update was pushed to approximately 8.5 Million virtual & on-prem Windows servers and workstations globally. The flawed update produced a BSOD loop (Blue Screen of Death), which in many cases required manual restoration/recovery, impeding recovery times. This incident may increase regulatory focus on security products, including transparency, validation and dependencies.

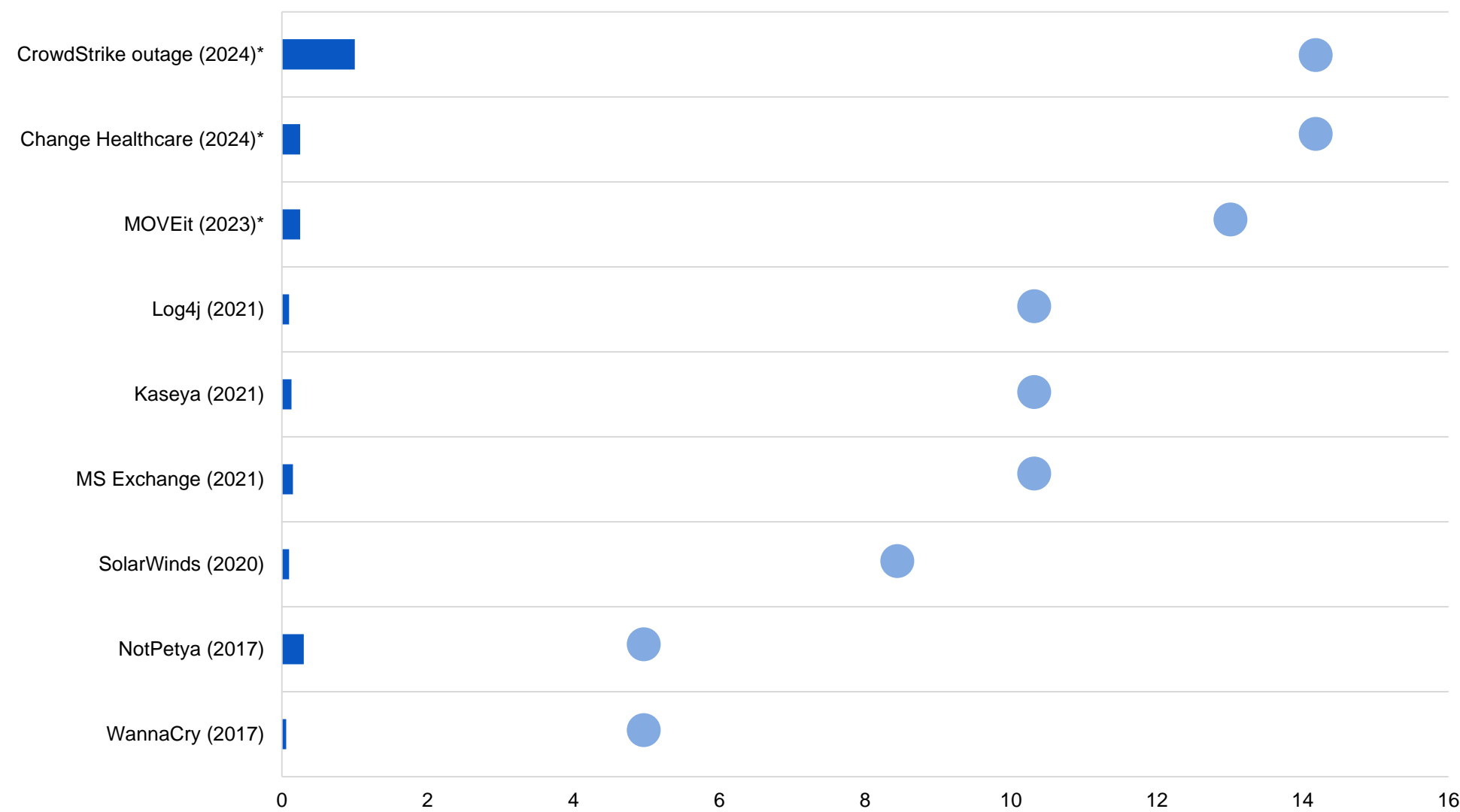
The incident coincided with a separate, unrelated outage impacting multiple services using Microsoft Azure's Central US region.



CrowdStrike loss analysis

Cyber insurance market well placed to absorb its biggest loss ever following CrowdStrike

Affirmative cyber insured loss estimates for high-profile cyber events vs GWP for global cyber market, USD billion (original value)

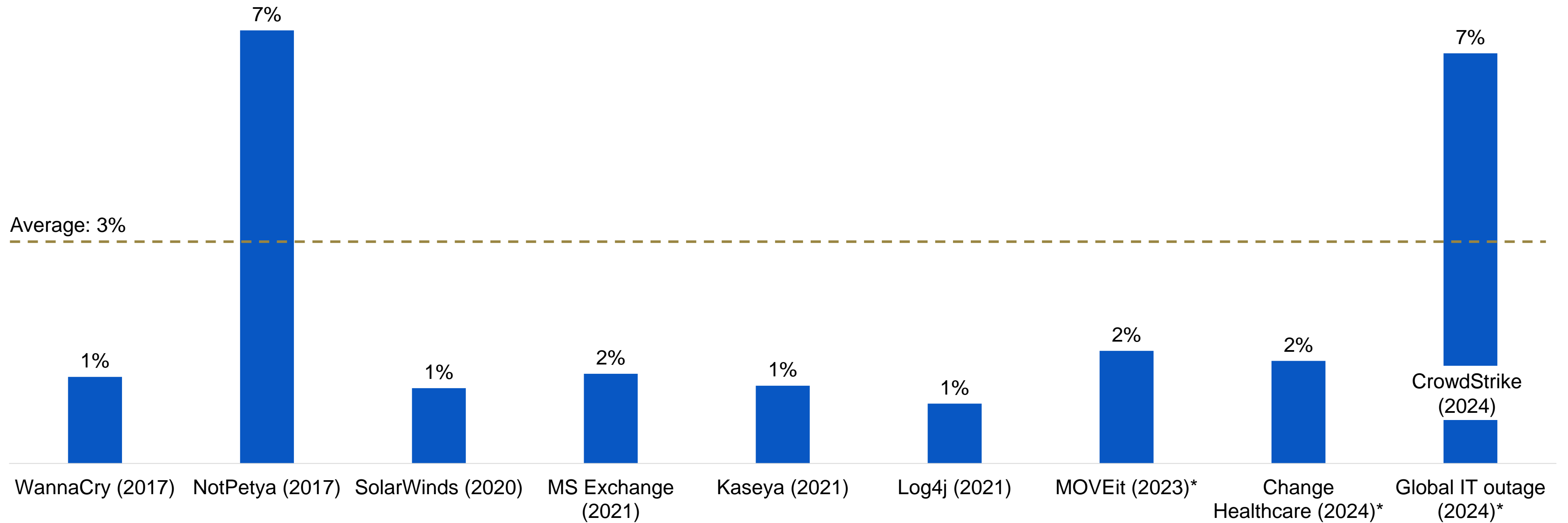


■ Affirmative cyber (excludes non-affirmative property losses for NotPetya)

Note: Loss development based on a range of early market estimates subject to revision. Source: Howden, PCS, Barclays, Parametrix, CyberCube

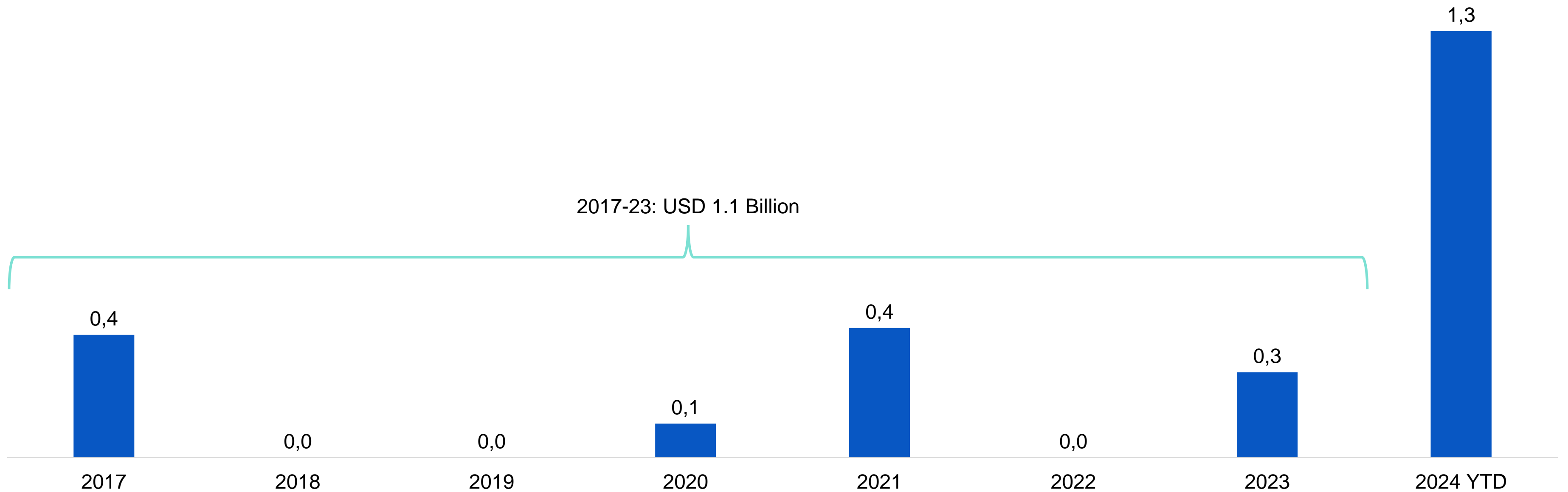
- Losses from the CrowdStrike are likely to be mitigated by the short duration of the incident and its non-malicious nature
- The 'systemic' potential of the incident mitigated by rapid patch delivery, enabling companies to resume operations quickly
- It is the latest in a series of incidents to highlight how the market's overall premium base can absorb insured losses from high-profile, systemic events
- There has been an increase in the frequency of these types of incidents in recent years
- In the case of the CrowdStrike, the (albeit early estimate of) loss is expected to be in the range of USD 1 billion relative to total cyber premiums of USD 14.5 billion
- All company demographics were impacted, with SME clients (typically lacking internal IT resources) contacting us first for advice
- As more information comes to light, data shows that indirect claims from third parties have been lower on average relative to direct claims, meaning the scale of events (or frequency of loss) would need to be multiples of what has been experienced to date to generate losses that threatens the premium base of the market

The estimated insured loss from the CrowdStrike are on a par with NotPetya



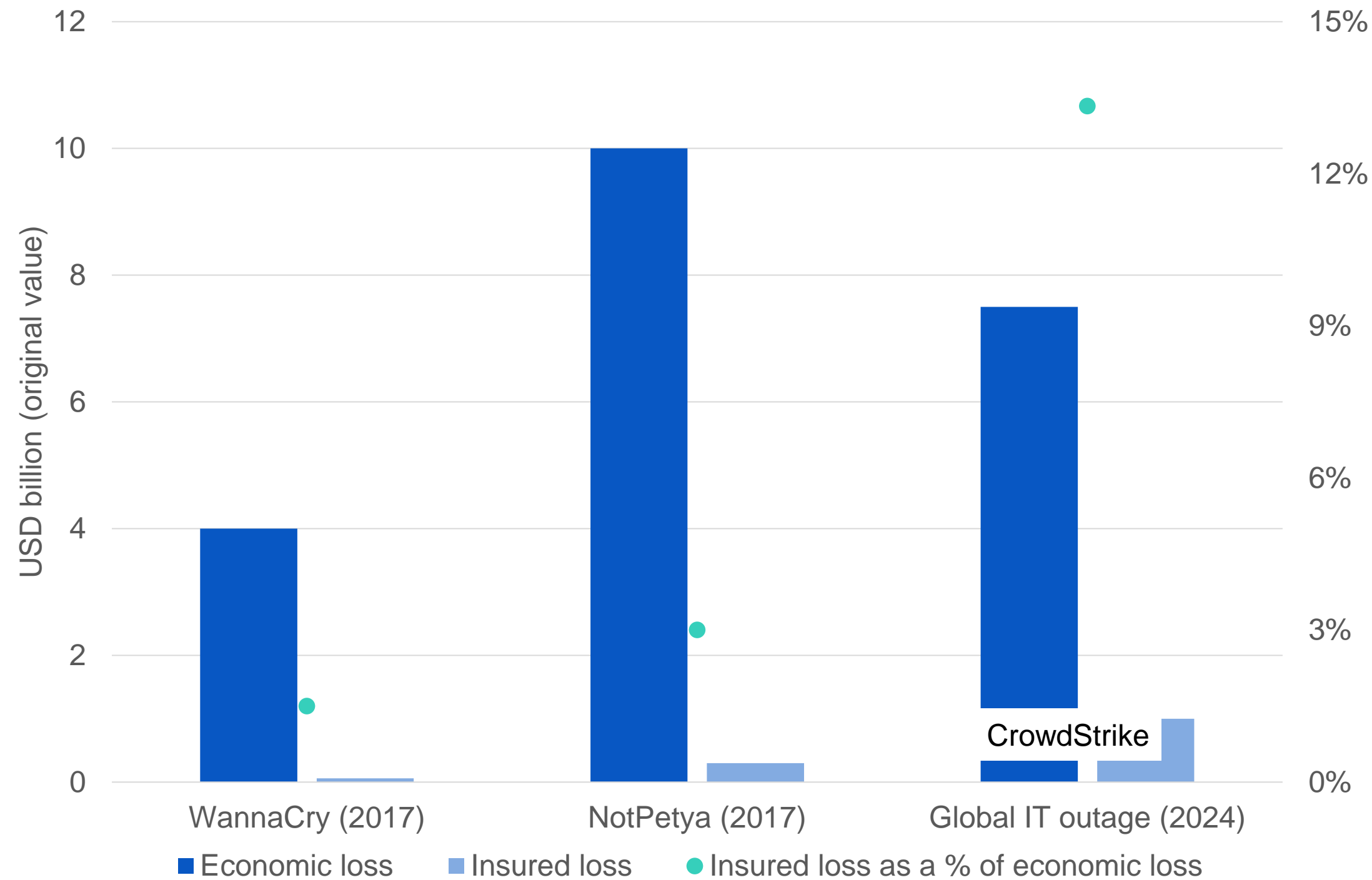
Note: Loss development based on a range of early market estimates subject to revision. Source: Howden, PCS, Barclays, Parametrix, CyberCube

Estimated Change Healthcare and CrowdStrike insured losses put 2024 significantly above recent years



Note: Loss development for 2023 and 2024 based on a range of early market estimates subject to revision. Source: Howden, PCS, Barclays, Parametrix, CyberCube

Insurance set to absorb a higher proportion of economic loss for the 2024 IT outage compared to WannaCry and NotPetya

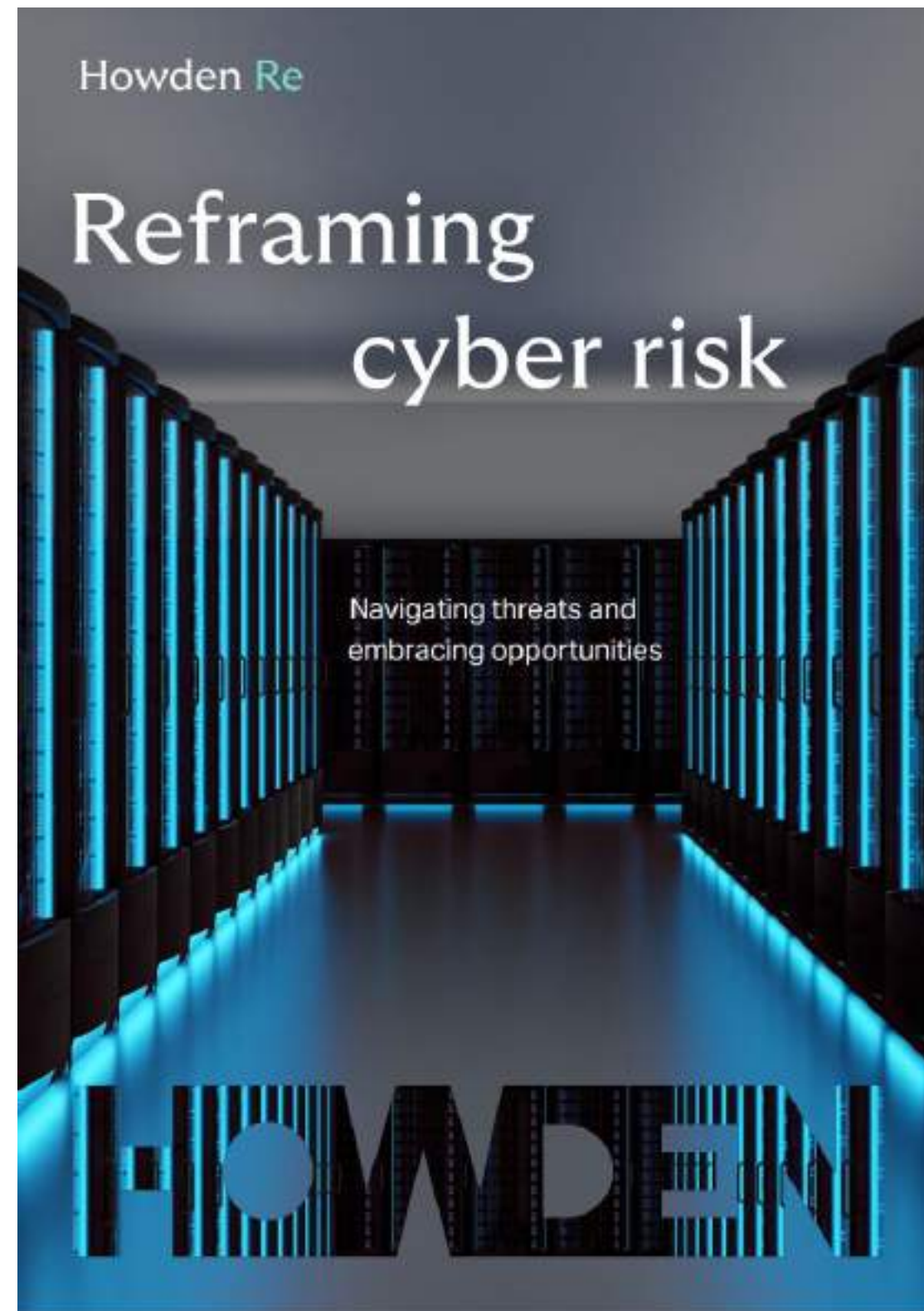
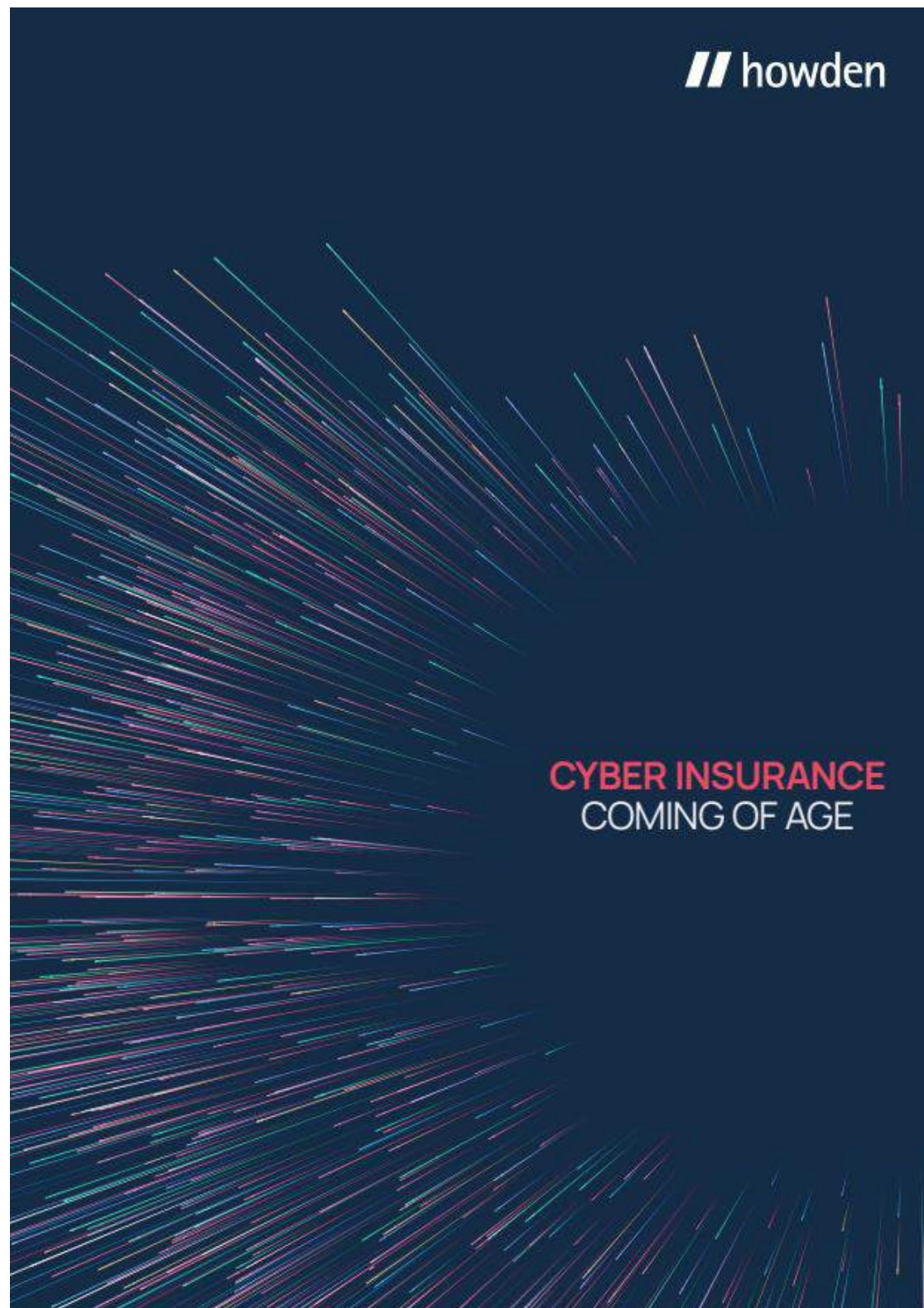


Source: Howden, PCS, U.S. government, Barclays, Parametrix, CyberCube

Key takeaways

- Cyber insurance market at USD ~14.5 billion of premium well placed to absorb its biggest loss ever following the CrowdStrike in Jul-24 at USD ~1 billion
- The estimated insured loss from the outage represents approximately 7% of global cyber premiums, which puts the incident on a par with 2017's NotPetya malware-driven loss
- Estimated insured losses from the Change Healthcare and global outage incidents put 2024 significantly above the total for comparable events in recent years, with 2024's YTD insured losses of USD ~1.3 billion already above those of 2017-23 combined at USD ~1.1 billion
- Insurance set to absorb a higher proportion of the economic loss (~13%) for the global outage compared to major losses of WannaCry and NotPetya in 2017 (~1-3%)
- New demand for cyber insurance from raised risk awareness (following the outage and other, lower-level events), deepening SME penetration and international expansion will help to propel the market above USD 40 billion in premiums by 2030
- Don't let your insurer point to the CrowdStrike incident as a reason to raise your premium!

Howden Cyber Research



Themes covered in this deck around systemic risk and the future of the market have been articulated by Howden in a series of in-depth reports (click on images to download)



Cyber risk for SMEs

HOWDEN

— watch the connections!

Kristoffer
Haleen

HOWDEN

Heightened cyber threat landscape in 2024

85%

Increase in # of global ransomware attacks in 2023

35%

CAGR 2021-23 in U.S. critical infrastructure ransomware attacks

17ppt

Decrease in % of victims paying ransom in 1Q24 vs 1Q23

>\$1bn

Ransomware revenue for the first time in 2023

100m

People affected by data leak in major SPoF attack in 2024

22%

Of CISOs using AI for threat hunting in 2024

■ Ransomware ■ Systemic ■ Gen AI

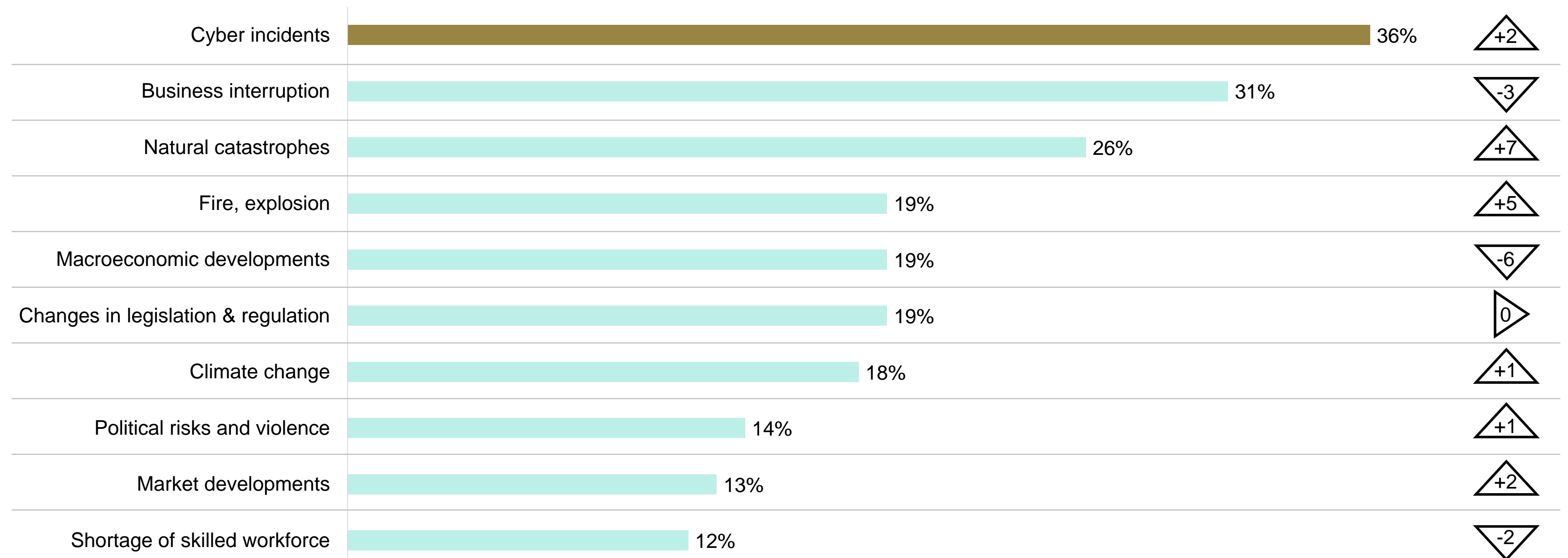
Heightened cyber threat landscape in 2024



Cyber increased lead as top global risk in Allianz Risk Barometer

Allianz Risk Barometer 2024

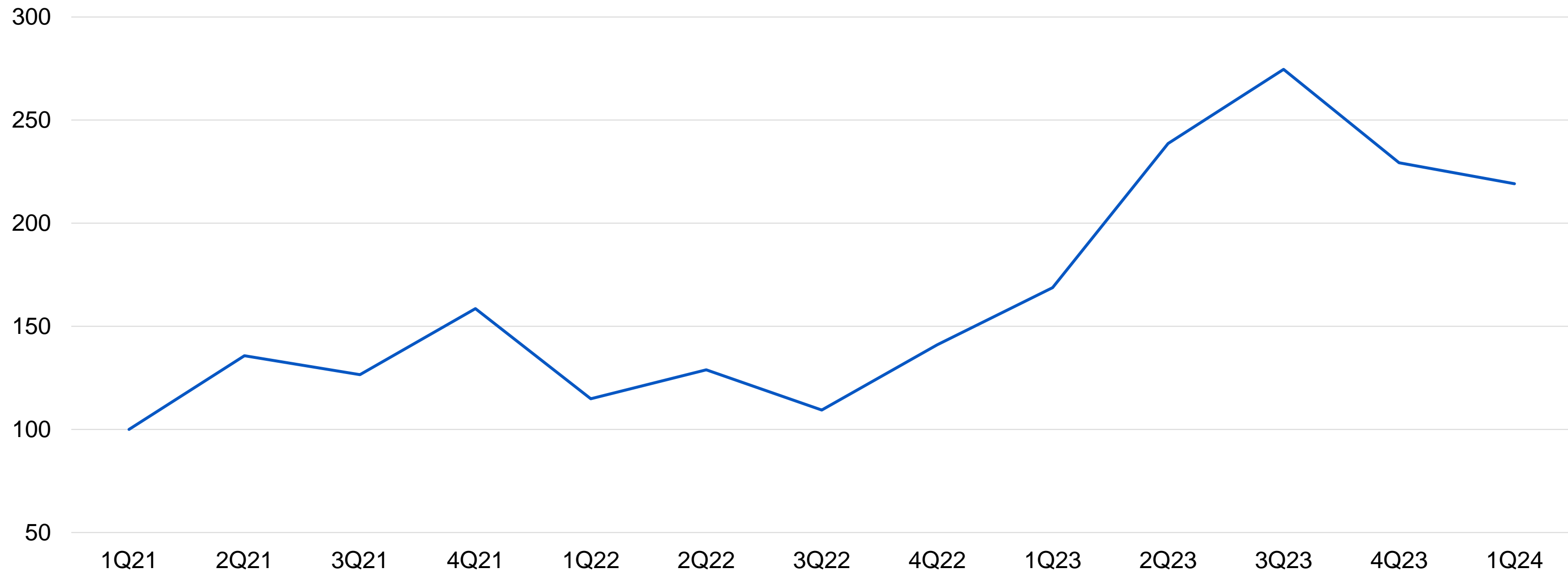
2022-23
change, pts



Note: Figures represent how often a risk was selected as a percentage of all survey responses from respondents. Figures do not add up to 100%, as respondents were asked to name up to three risks they saw as most important. Source: Allianz Commercial

Frequency index for global ransomware – 1Q21 to 1Q24

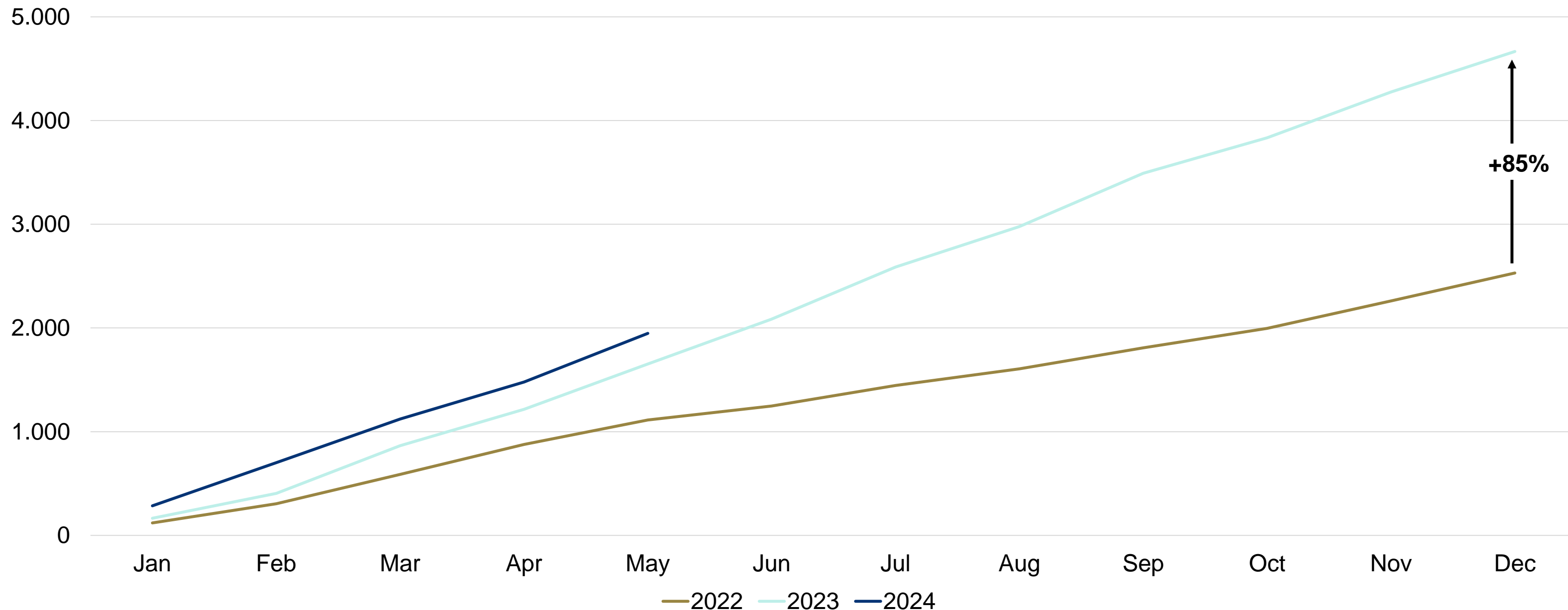
Frequency of global ransomware attacks has trended upwards since 2021, driven by ransomware-as-a-service and profitability of attacks



Note: NCC Group tracks ransomware groups operating the hack and leak double extortion tactic by monitoring leak sites and scraping victims' details as they are released. Source: Howden analysis based on data from NCC Group

Cumulative global ransomware activity by month – 2022 to 2Q24

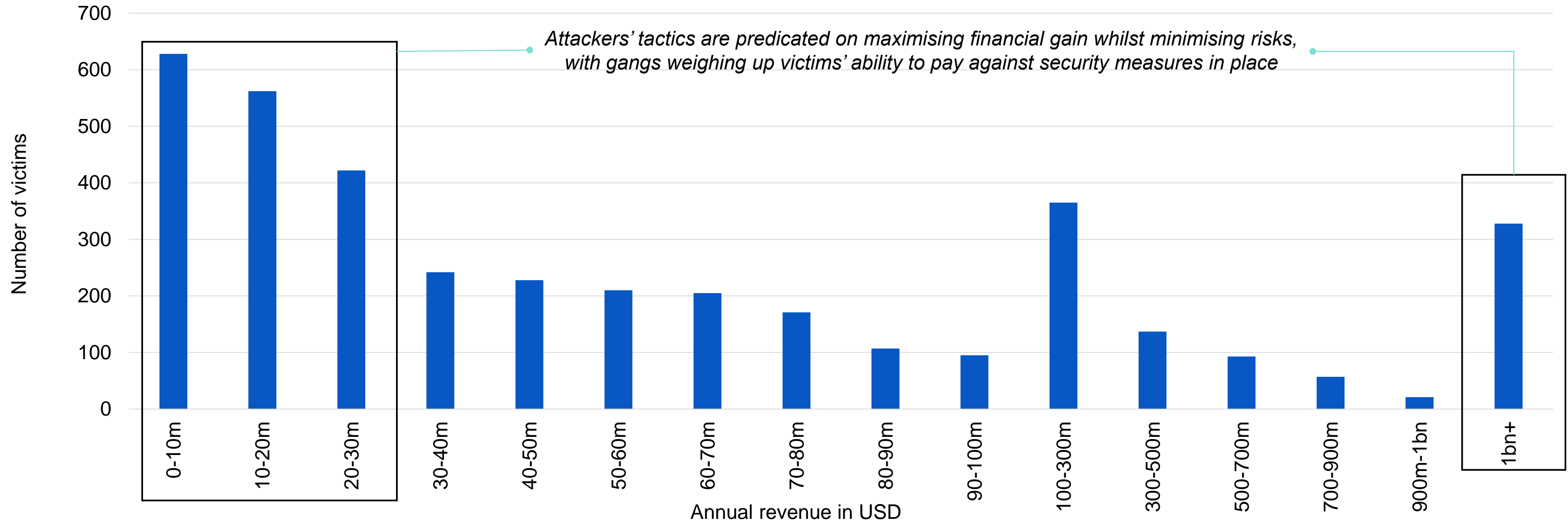
Acceleration in ransomware frequency in 2023, with established gangs attempting to recover from 2022 drop in revenue (Russia-Ukraine war) and emergence of new groups



Note: NCC Group tracks ransomware groups operating the hack and leak double extortion tactic by monitoring leak sites and scraping victims' details as they are released. Source: Howden analysis based on data from NCC Group

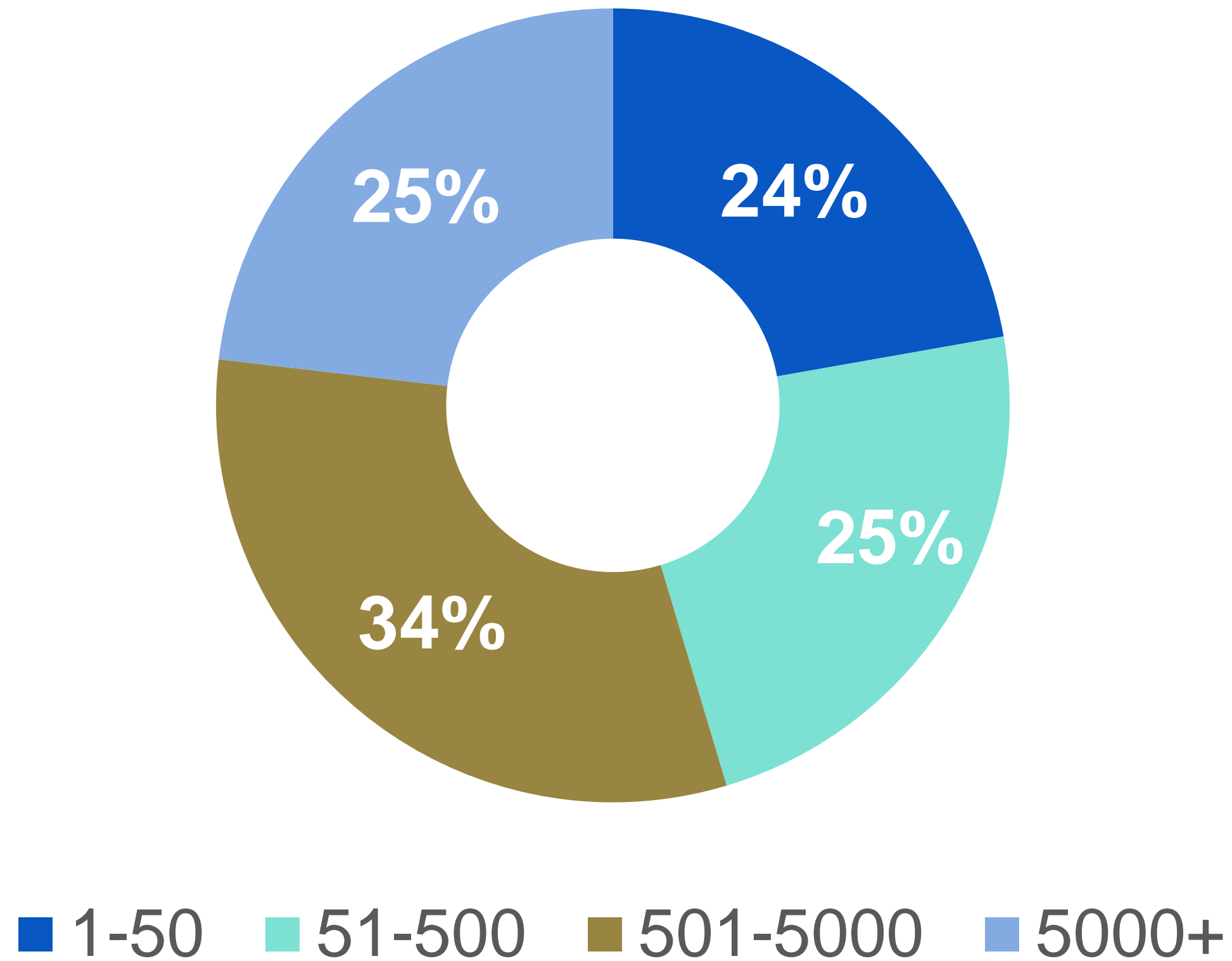
Distribution of ransomware attacks by companies' annual revenue in 2023/24

Companies of all sizes continue to be targeted by ransomware, with a noticeable bias towards the upper and lower bands of the revenue range



Source: Howden analysis based on Black Kite data

Lessons from the frontlines

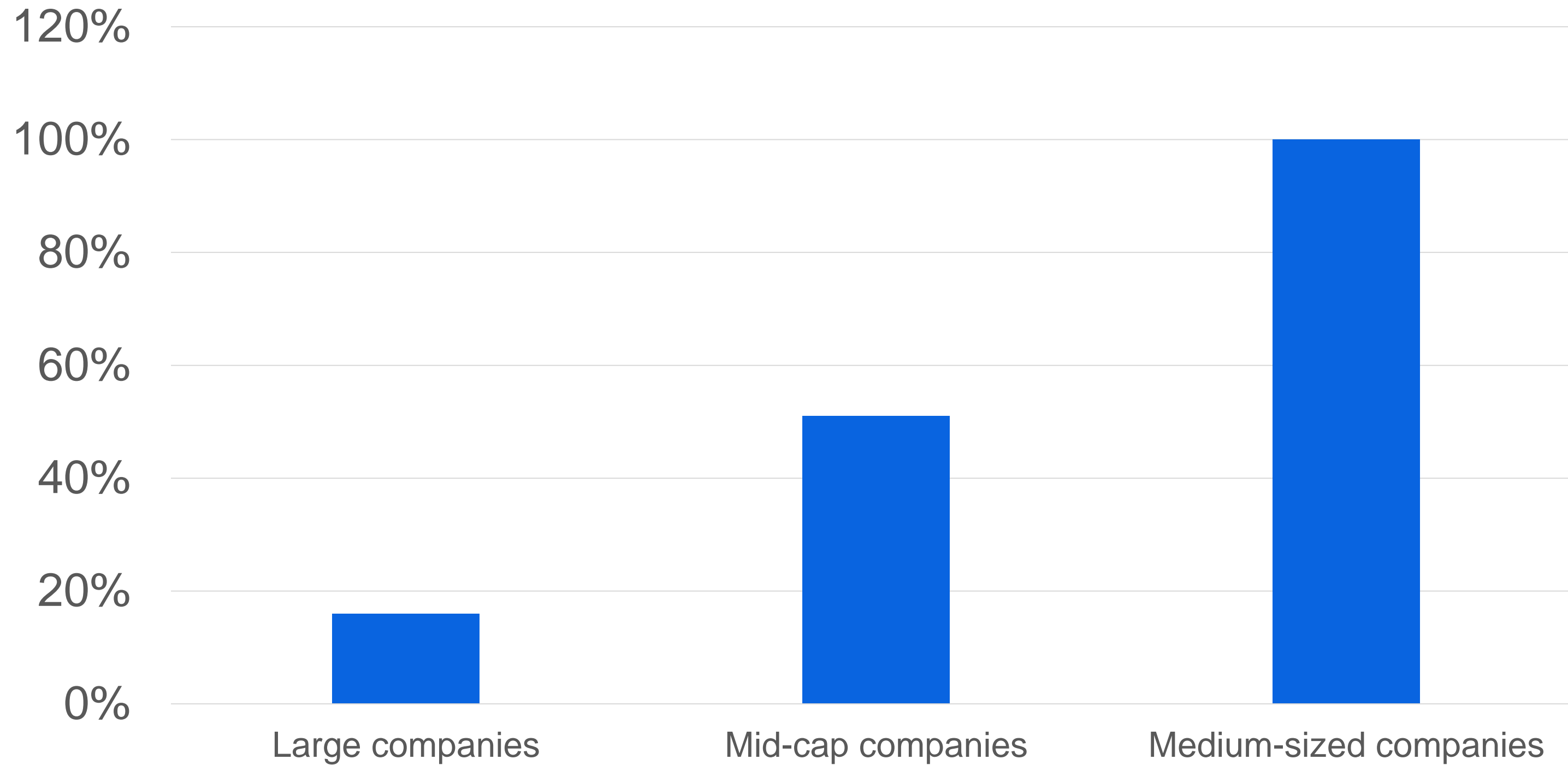


“ As more large businesses and corporations invest in cybersecurity tools, hackers are increasingly targeting small and medium-sized businesses and using them as supply chains.

Truesec Threat Intelligence Report
2023

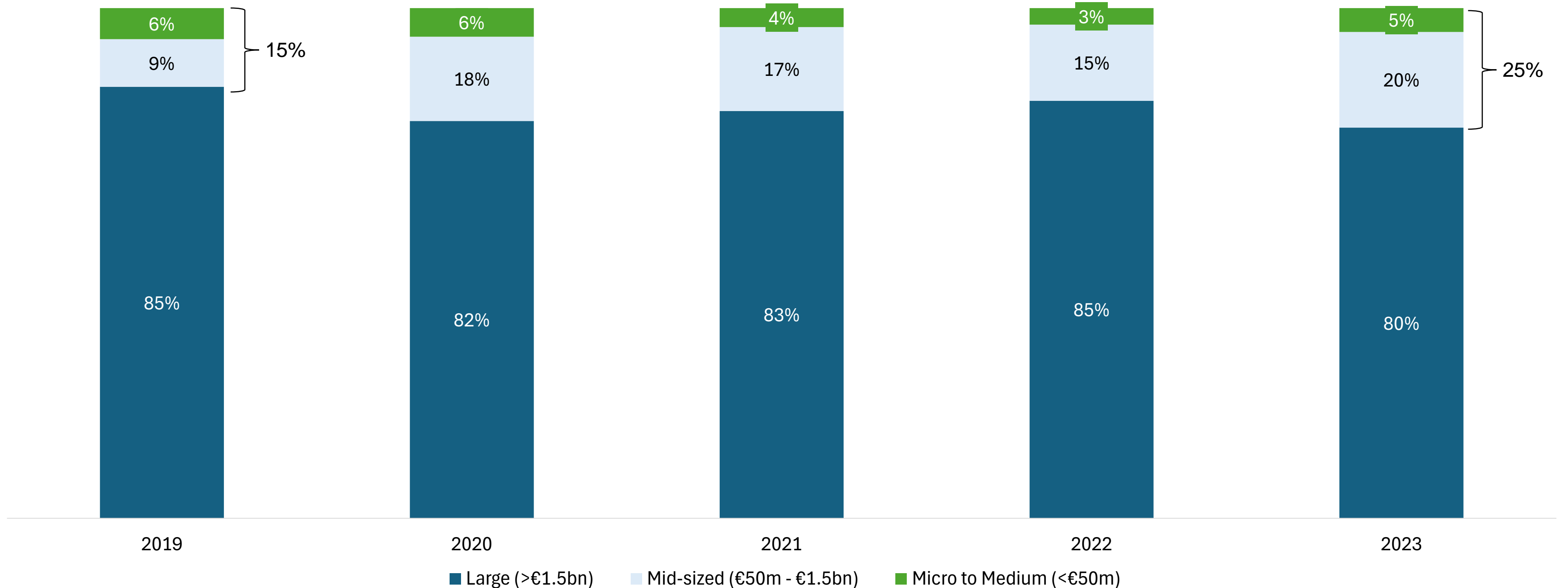
Lessons from the insurance markets

Loss ratios per revenue segment



Progress in the SME space is being made in markets such as France

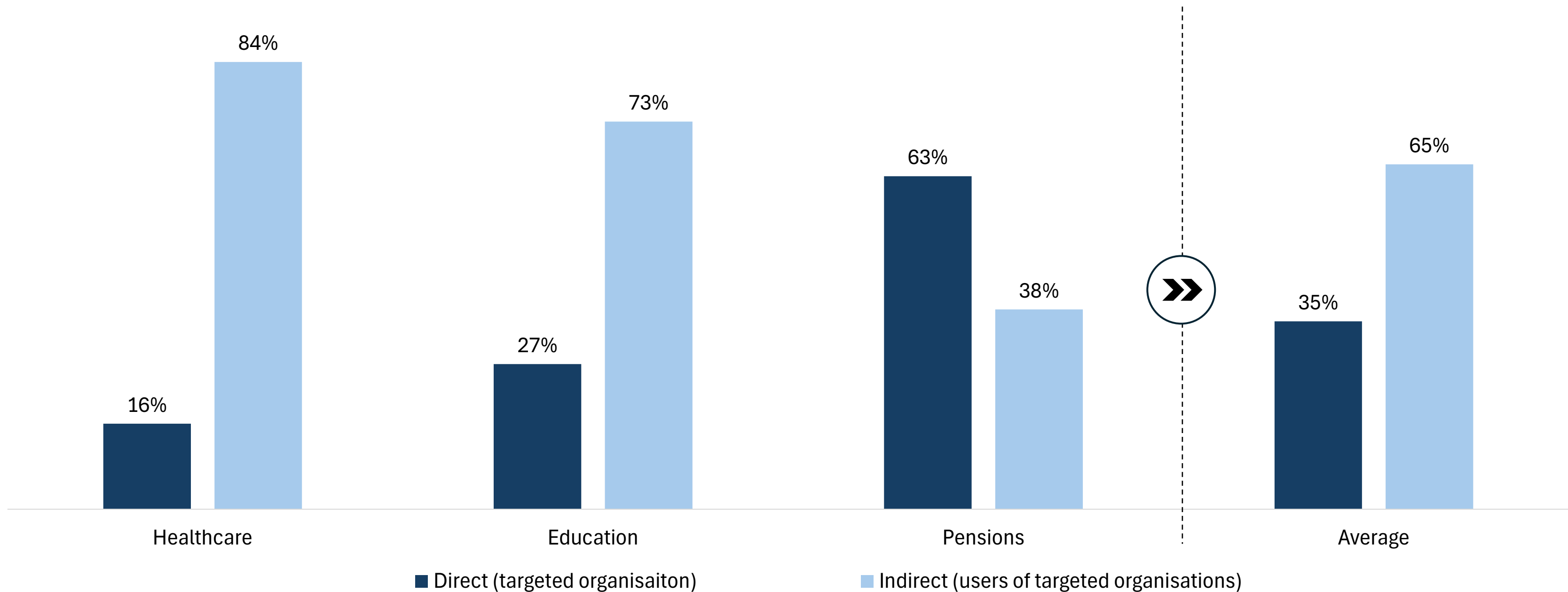
French cyber insurance premium distribution by company revenue band



Source: AMRAE

Indirect costs exceed the direct costs

Indirect costs sustained by third party companies can make up the lion's share of economic losses in systemic ransomware attacks



Note: Analysis is based on reported numbers of entities affected and average costs for first- and third-party ransomware attacks. Source: Change Healthcare, Coalition, At Bay, Pension Benefit Information and National Student Clearinghouse.

Basic Security – frameworks for SMEs

UK Cyber Essentials

1. Firewalls
2. Secure configuration
3. Security update management
4. User Access control
5. Malware protection

Insurance requirements

1. MFA for all remote access
2. *Anti Virus / Endpoint Detection & Response*
3. Backup procedures
4. Patching routines
5. Segmentation
6. *Access management*
7. *Monitoring of the environment*

Key takeaways

- Ransomware is as active as ever, but is now a greater threat to SMEs than large corporates
- The financial impact on large corporates has been manageable in the last 18 months – whether temporary or permanent
- Lessons from Ukraine teach us that threat actors use SMEs as segways into large corporates
- SMEs need to raise their security posture, there are several useful public standards to lean against
- A company's cyber risk extends to any company to which there are technical connections

References

- [Stop Ransomware | CISA](#)
- [Cyber Essentials Requirements for IT Infrastructure v3.1 April 2023 \(published January 2023\) \(ncsc.gov.uk\)](#)
- [Download the Truesec Threat Intelligence Report 2024](#)
- <https://cip.gov.ua/services/cm/api/attachment/download?id=53466>
- https://cert.gov.ua/files/pdf/SOC_Annual_Report_2022.pdf

State of the market

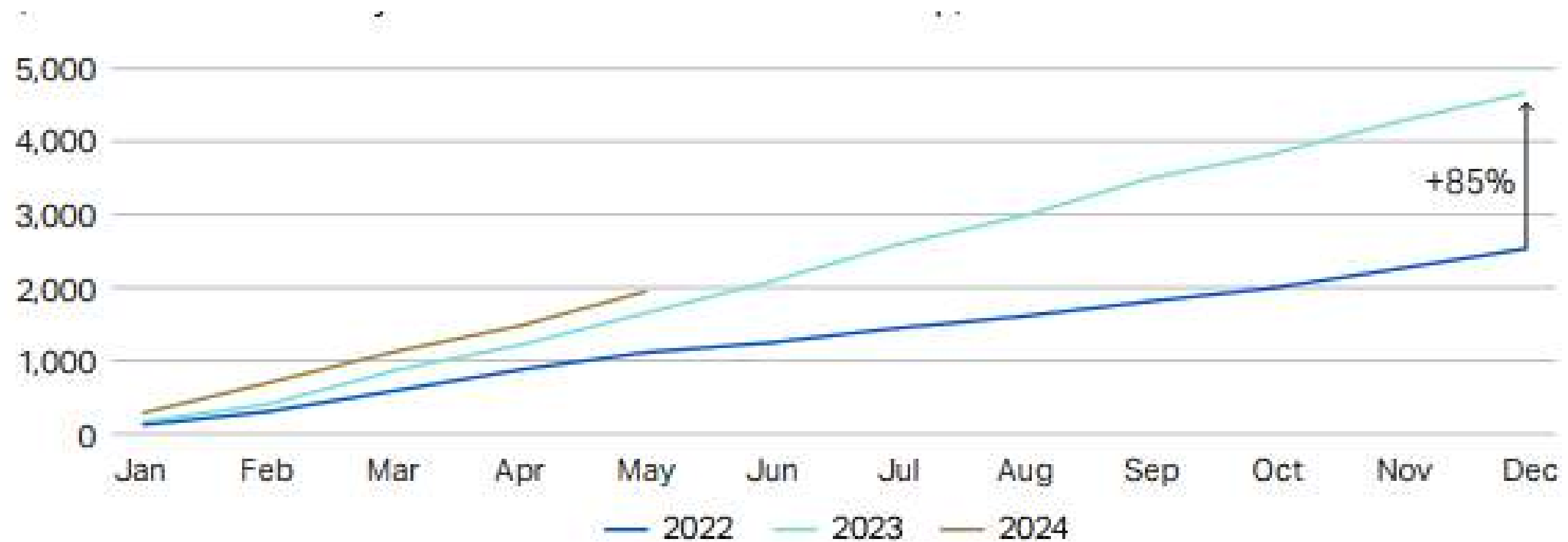
HOWDEN

Christophe
Liekens

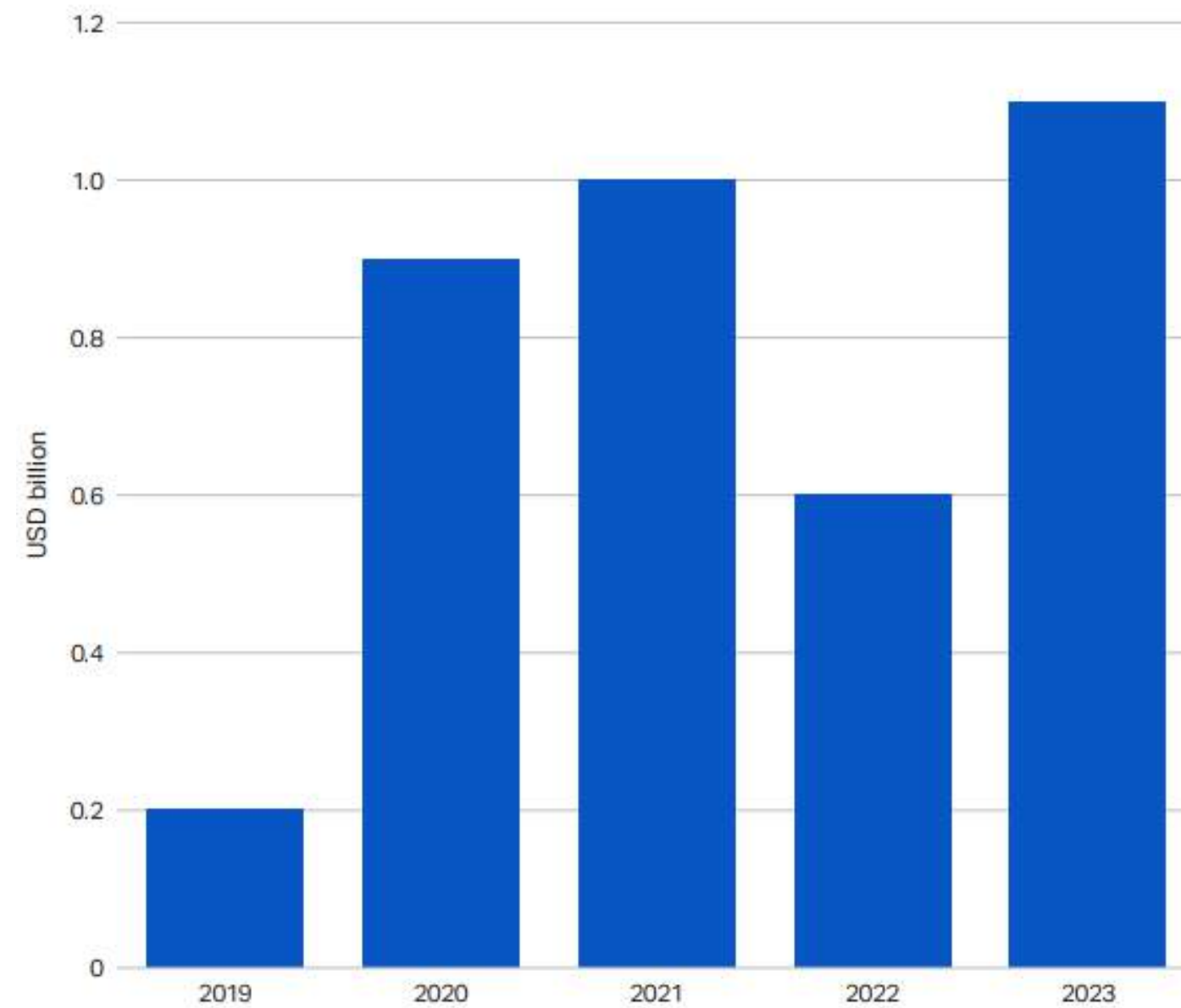


HOWDEN

Cumulative global ransomware activity by month – 2022 to 2Q24

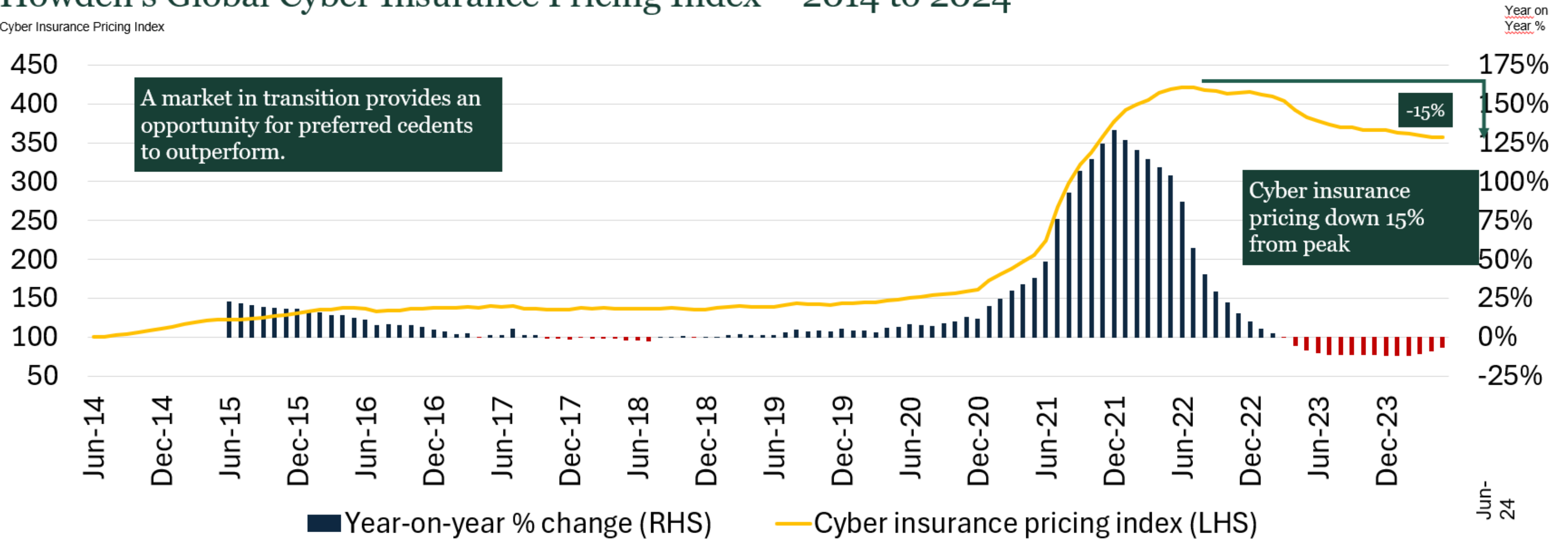


Ransom monies received by ransomware attacks – 2019 to 2023



Howden's Global Cyber Insurance Pricing Index – 2014 to 2024

Cyber Insurance Pricing Index

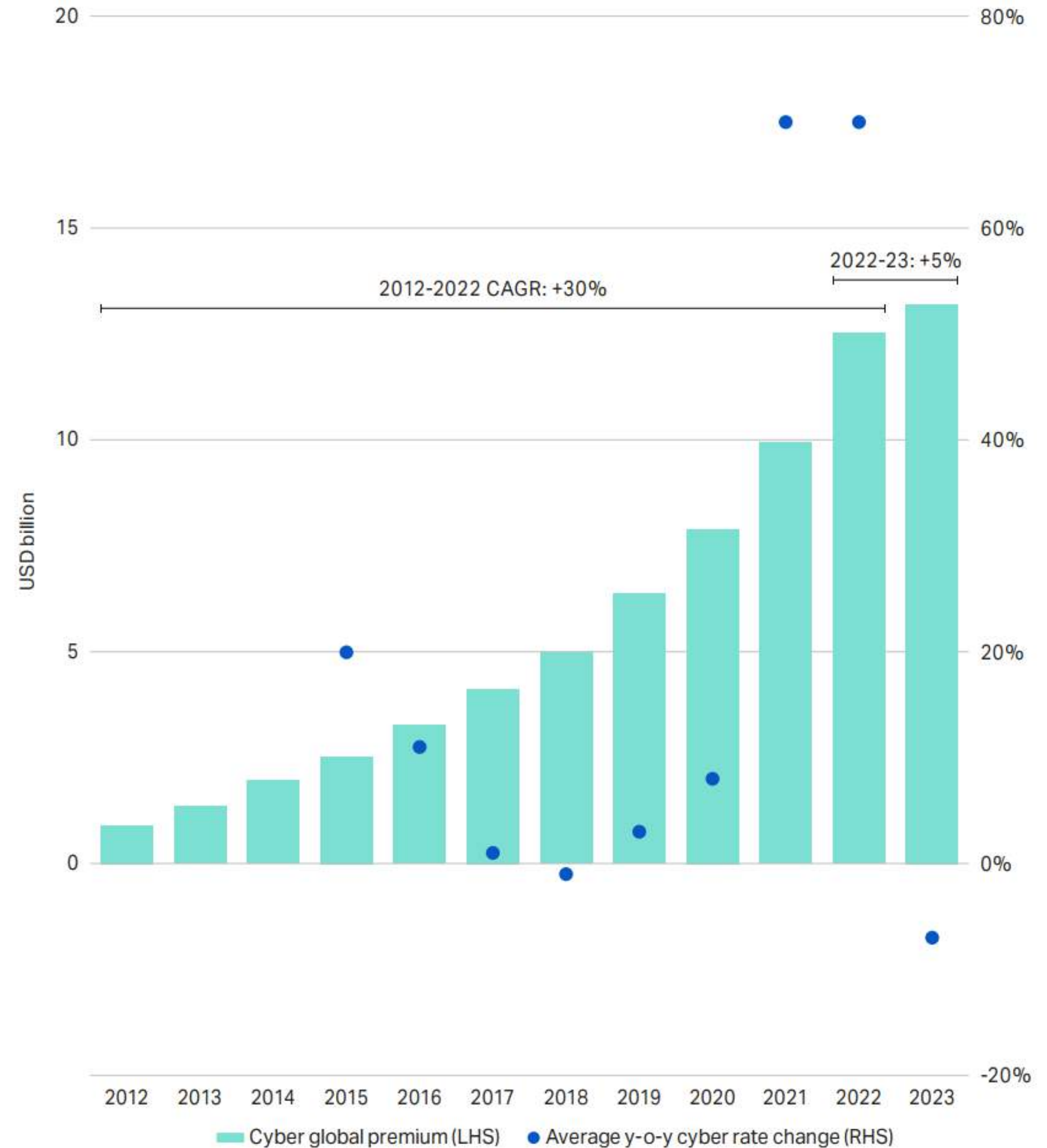


2012 to 2023

Cyber global gross written premium

Average y-o-y cyber rate change

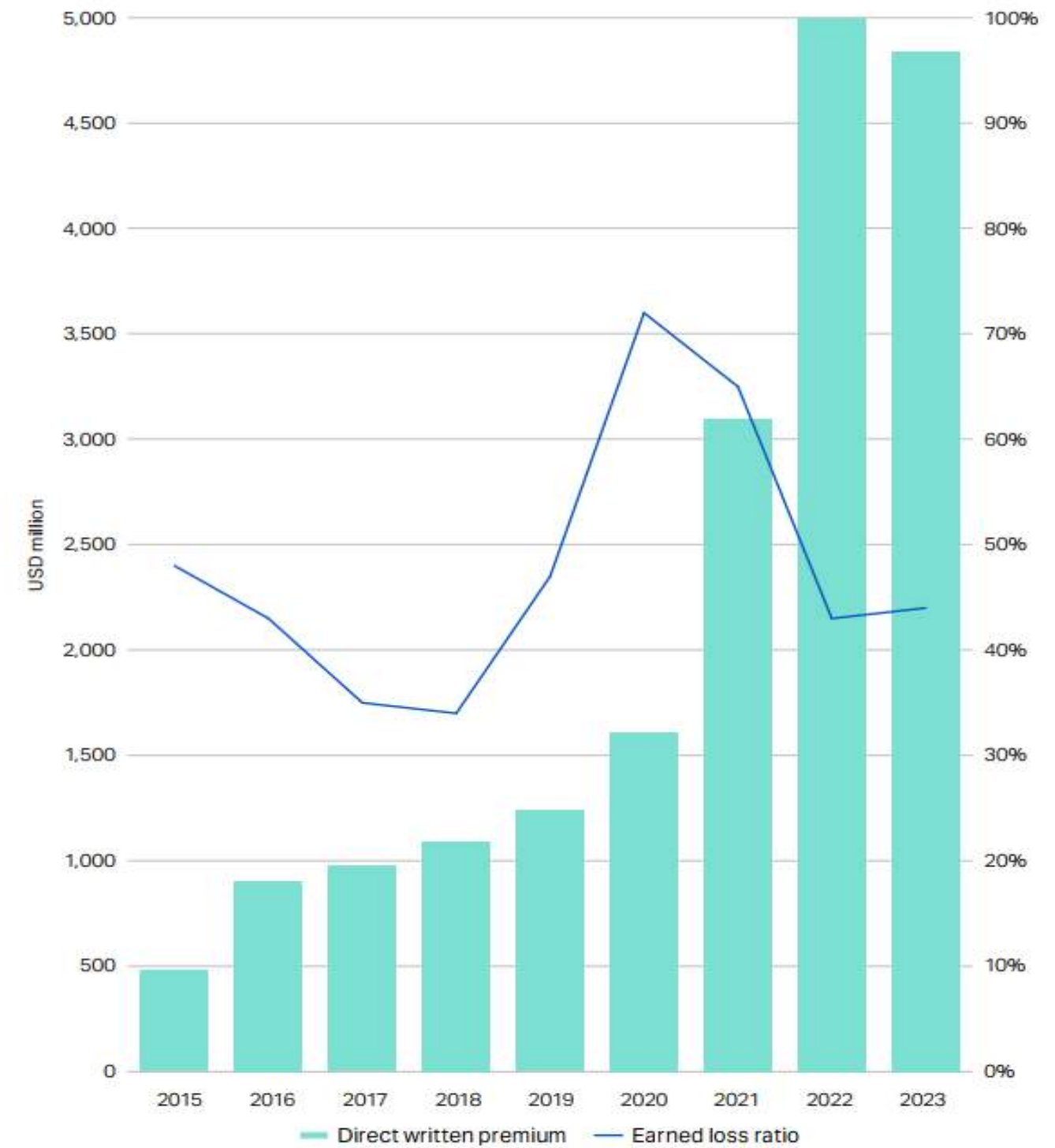
(Source Howden)



2015 to 2023

Loss ratio and direct written premium for U.S. standalone cyber policies

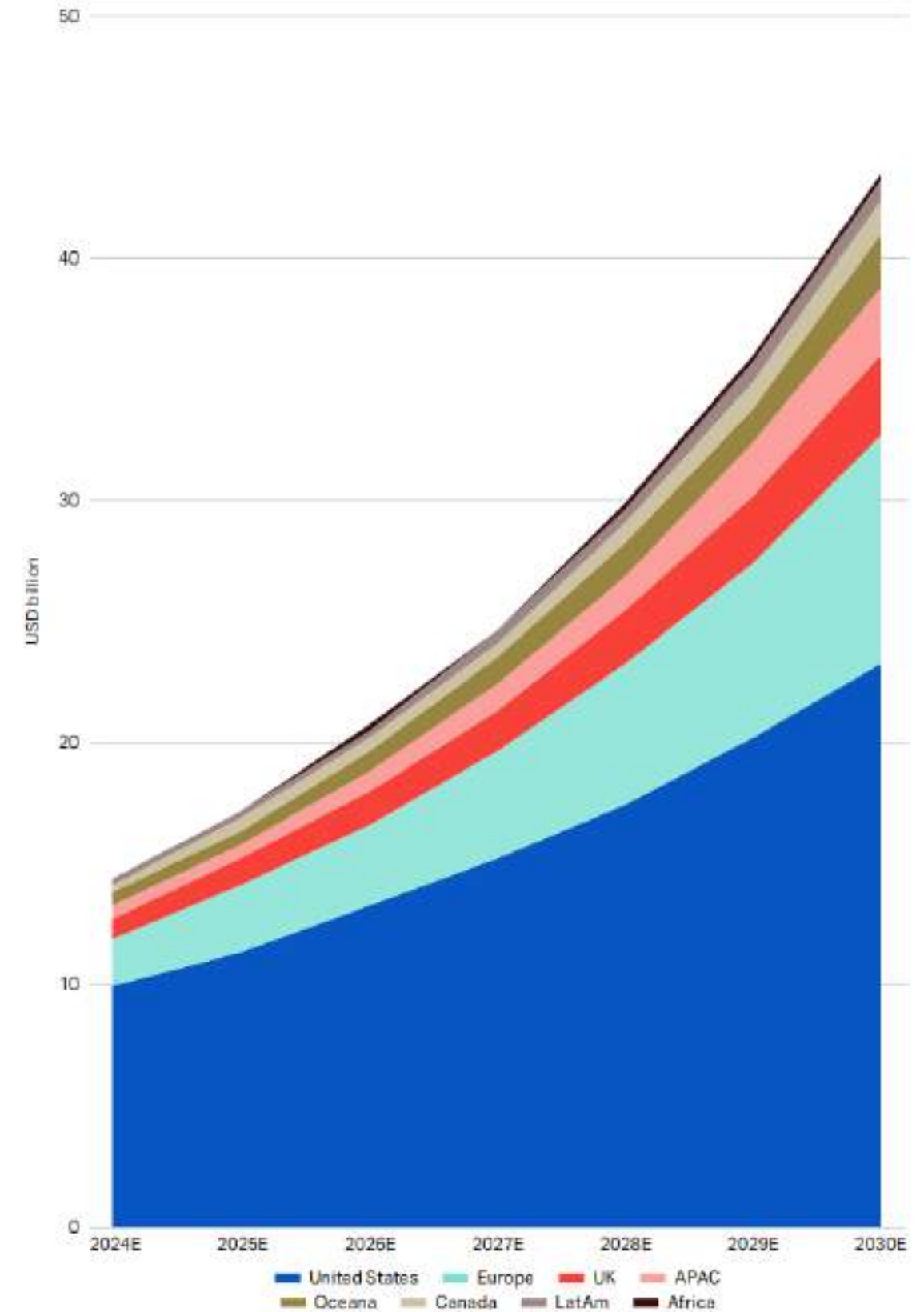
(Source: Howden, NOVA, NAIC)



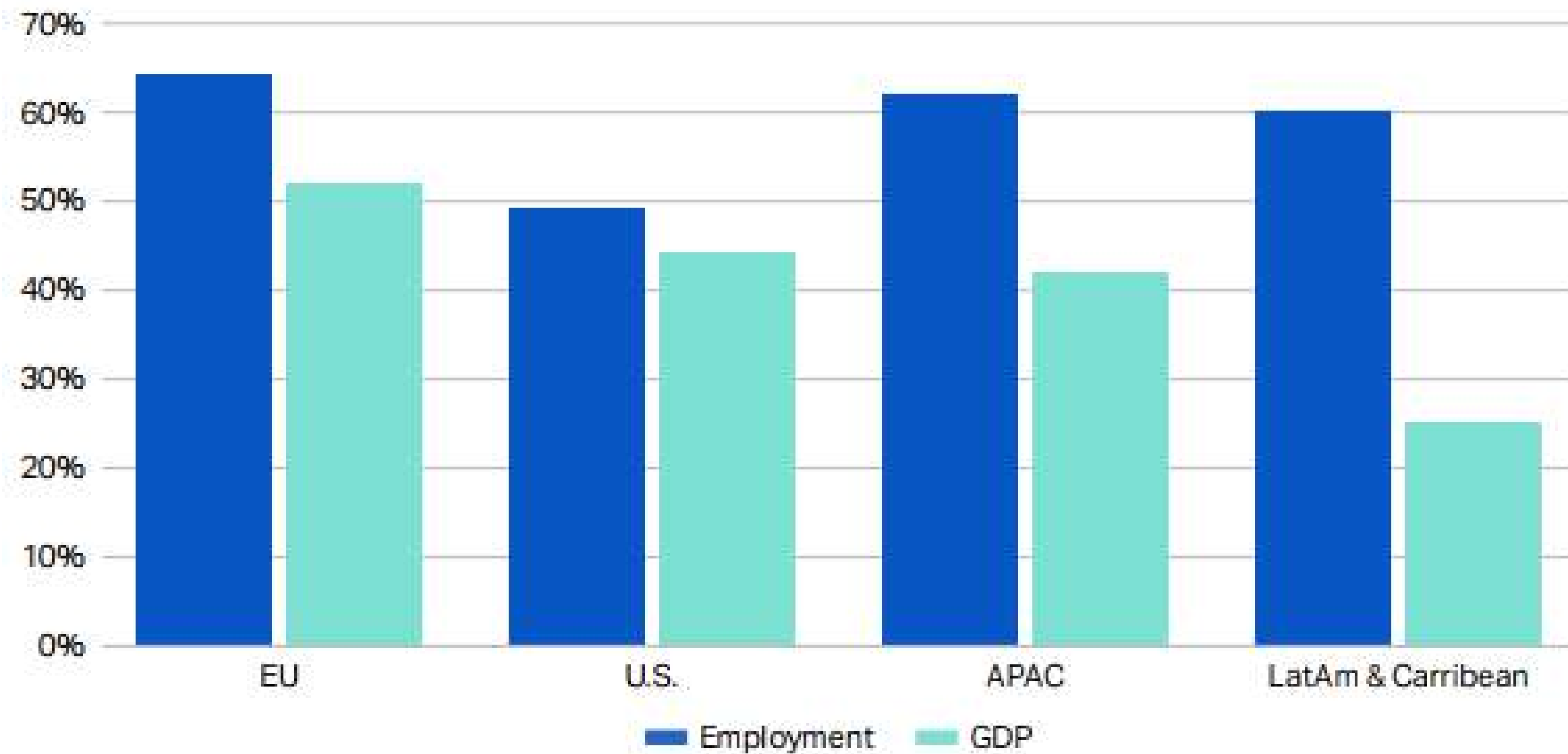
2024 - 2030

Estimated cyber gross written premiums by region – 2024 to 2030

(Source: Howden)

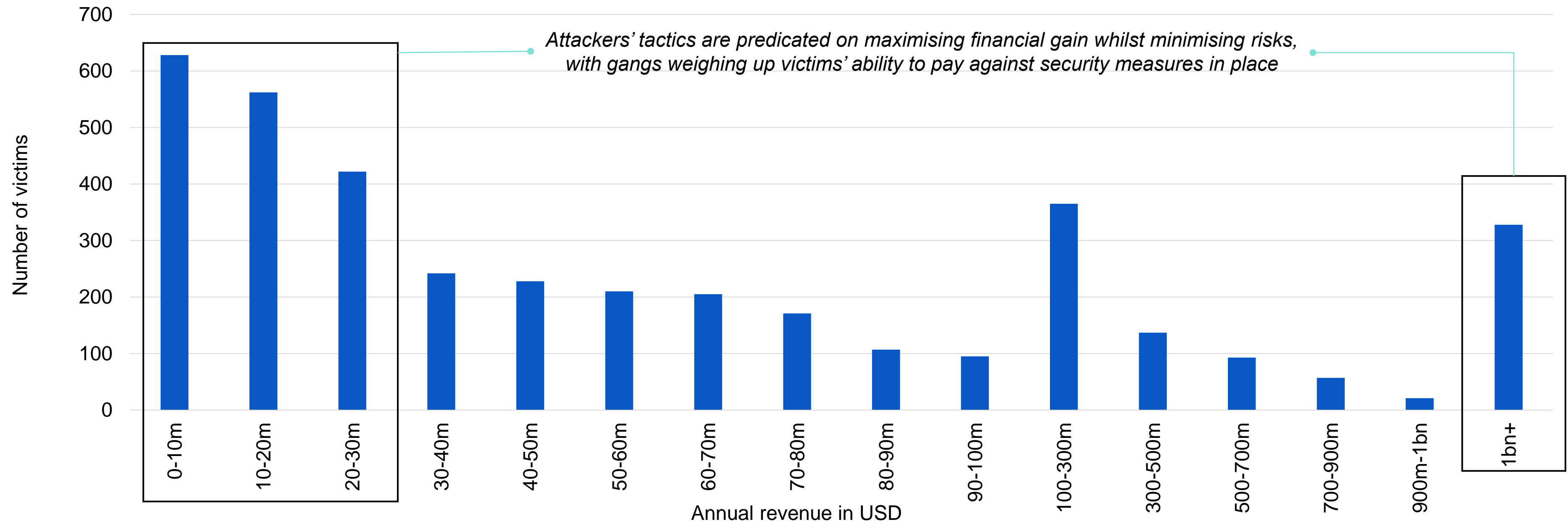


SME share of economy by region



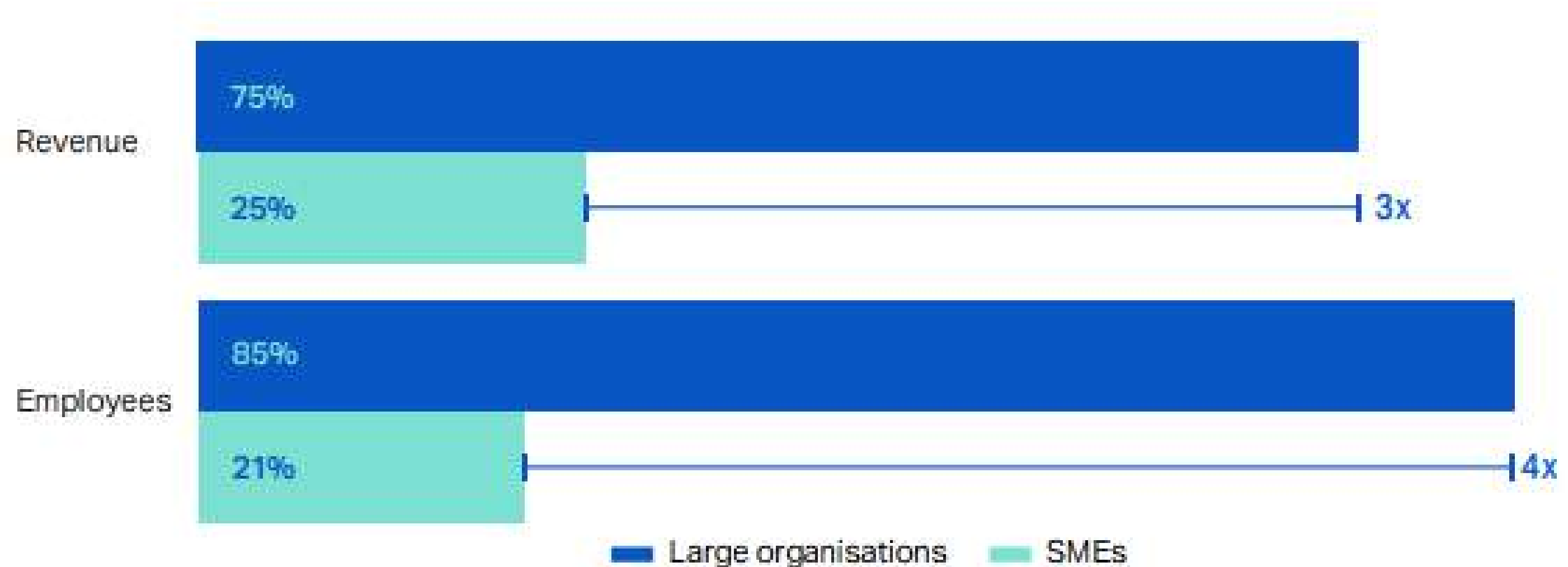
Distribution of ransomware attacks by companies' annual revenue in 2023/24

Companies of all sizes continue to be targeted by ransomware, with a noticeable bias towards the upper and lower bands of the revenue range



Source: Howden analysis based on Black Kite data

Share of organisations with cyber insurance globally in 2023



Note: SMEs defined as business with <250 employees or <\$250m in revenue, Large organisations defined as business with >100,000 employees or >\$5.5bn in revenue

Key Take Aways

- Cyber Insurance is maturing. Insurers seem to have found a way to cope with the evolving threat landscape for now helped by the more robust profile of the medium and larger companies around the world
- The premiums which were very and perhaps too low when the product entered the market stabilized after a dazzling steep climb in 2021 – 2022
- The cybermarket will continue to grow with an expected gross written premium exceeding USD 43 bn by the end of the decade
- The growth will for a large proportion take place in the SME market



Don't miss out on our next events



- | | |
|----------|---|
| 20/10 | Belgian Evening Madrid |
| 21-22/10 | FERMA Forum |
| 14/11 | BELRIM/LLOYDS Exchange: Insurance Protection Gaps in Europe |
| 18/12 | Cocktail & Jo Willaert Award Ceremony |



Jo Willaert Award

Jo Willaert was an inspiring member of the BELRIM Board and Scientific Committee as well as President of FERMA when he passed away during the corona pandemic in 2020. In his memory, BELRIM has decided to create the Jo Willaert Award. This award will be given to the Risk and/or Insurance Professional who has “gone the extra mile for risk management”.


All risk professionals are invited to nominate someone for this Award.

A CV, photo and maximum 1-page motivation letter should be sent to info@belrim.com.
The Award Ceremony will take place during the annual cocktail of December.



BELRIM

Belgian Risk Management Association



*Thank You
Very Much*