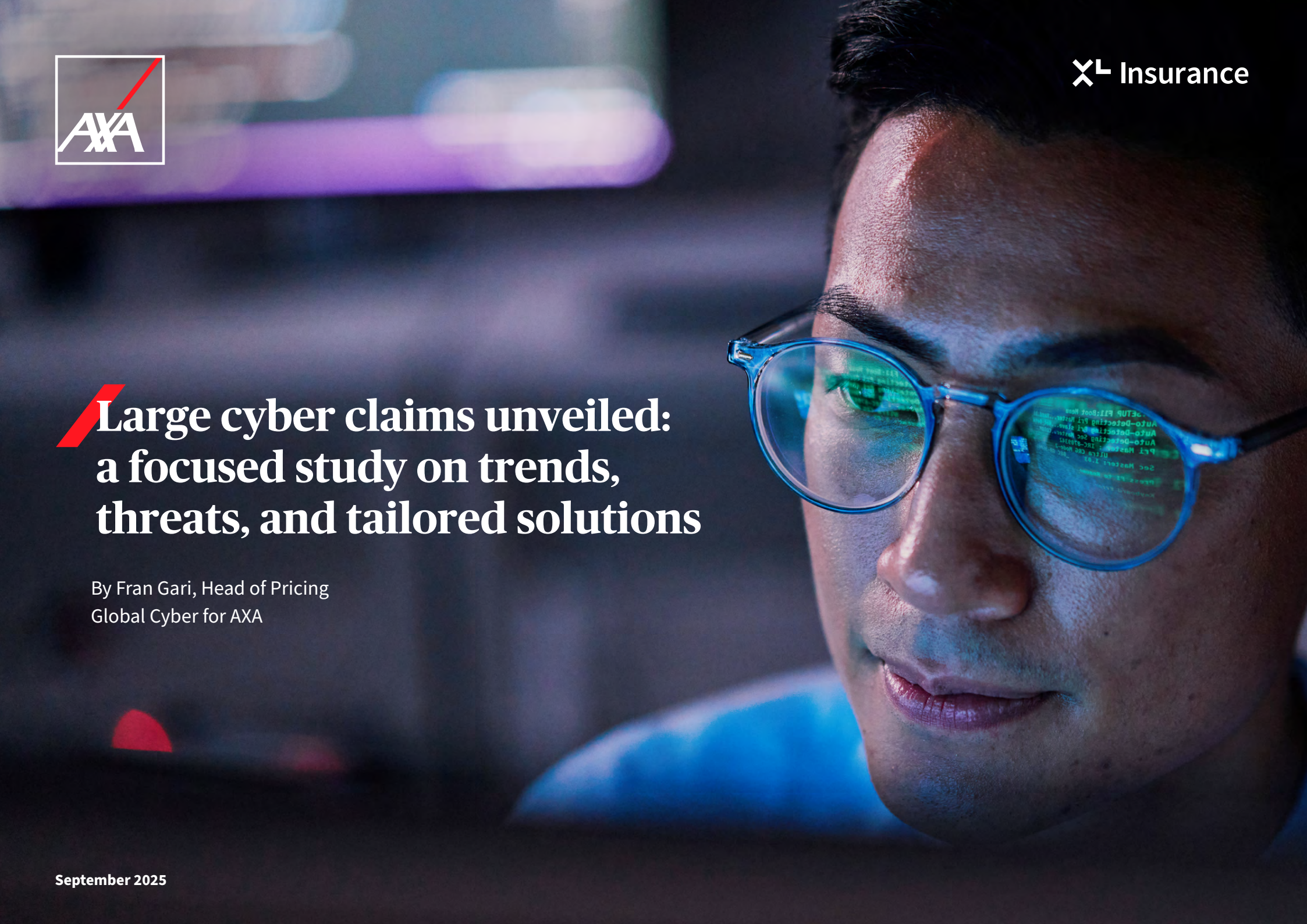


Large cyber claims unveiled: a focused study on trends, threats, and tailored solutions

By Fran Gari, Head of Pricing
Global Cyber for AXA

September 2025

Contents

Introduction

In an age marked by digital transformation, the surge in cyber incidents has become a significant challenge for businesses worldwide, and for valid reasons.

Cybersecurity threats are escalating. Fueled by the growing sophistication of threat actors, the expansive adoption of digital technologies, and the increasing value of sensitive data, cybersecurity threats are escalating.

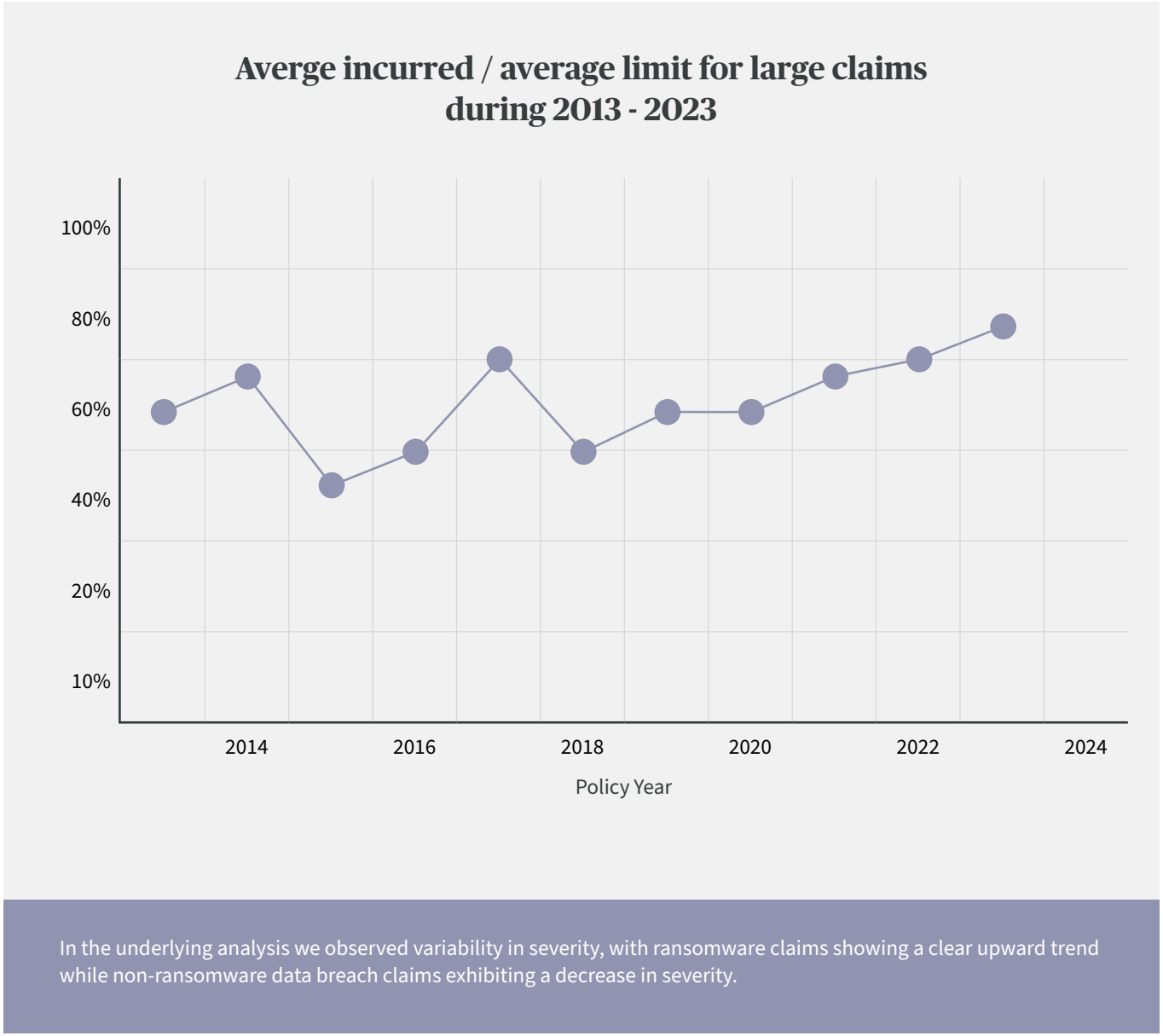
A comprehensive analysis of AXA XL's Global Cyber insurance portfolio reveals that 88.1% of total incurred losses arise from the claims that exceed $1 million. Studying these losses in depth not only enhances our understanding of the claims landscape but also provides underwriters, actuaries, brokers, and clients with essential insights to effectively navigate the evolving risk environment and build tailored solutions to help anticipate and manage these threats.

Examining claims over an extended period, particularly over the past several years, is vital for uncovering evolving trends and patterns in cyber incidents. Our longitudinal analysis sheds light on the frequency and severity of claims while also identifying emerging threats, such as the increasing prevalence of ransomware and shifts in the types of data breaches. By analyzing these narratives, insurers can refine their underwriting practices, adjust pricing strategies, and enhance risk management solutions, ultimately fostering more informed decision-making and improving protection for clients against future cyber risks.

Severity of large losses

Recent trends indicate an increasing severity of large losses, as evidenced by the rising proportion of high-value claims and the average incurred loss relative to limit size.

This trend, however, is partially influenced by underwriting actions in line with the market - such as changes to self-insured retentions and distribution of limit sizes.



In the underlying analysis we observed variability in severity, with ransomware claims showing a clear upward trend while non-ransomware data breach claims exhibiting a decrease in severity.

Insuring agreements in cyber claims

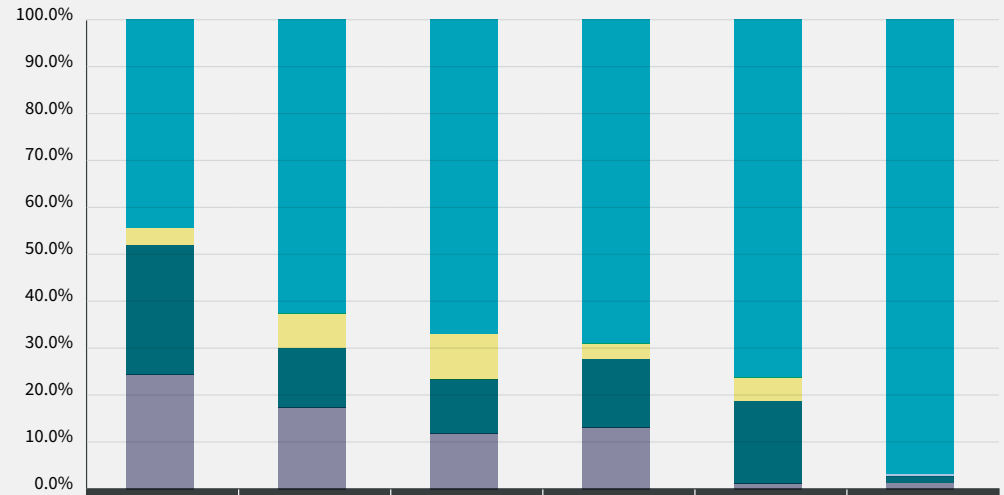
Most large cyber claims involve multiple insuring agreements being triggered simultaneously. The most frequently triggered agreements include:

- **Data breach response/crisis management:** Marginally more dominant in excess claims, this coverage often encompasses costs associated with notifying affected parties, legal fees, and public relations efforts to mitigate reputational damage.
- **Business Interruption:** More prevalent in excess claims, this coverage addresses losses incurred due to temporary shutdowns of operations resulting from cyber incidents, highlighting the financial impact of disruptions.
- **Extortion:** More common in primary claims, extortion coverage is particularly relevant in ransomware scenarios, where threat actors demand payment to restore access to data or systems.
- **Privacy and cyber security:** This coverage provides protection against losses resulting from various privacy and security wrongful acts, including unauthorized access and non-compliance with relevant laws and regulations. It is more common in excess claims, highlighting the potential for large severity where this is triggered.

The prominence of these insuring agreements has notably increased in recent years, driven largely by the surge in ransomware incidents, which account for a significant portion of claims. The evolution of these claims necessitates a proactive approach to policy design that anticipates emerging threats.

Top 5 insuring agreements triggered

Proportion of claims where each insuring agreement is triggered - and distribution of impact

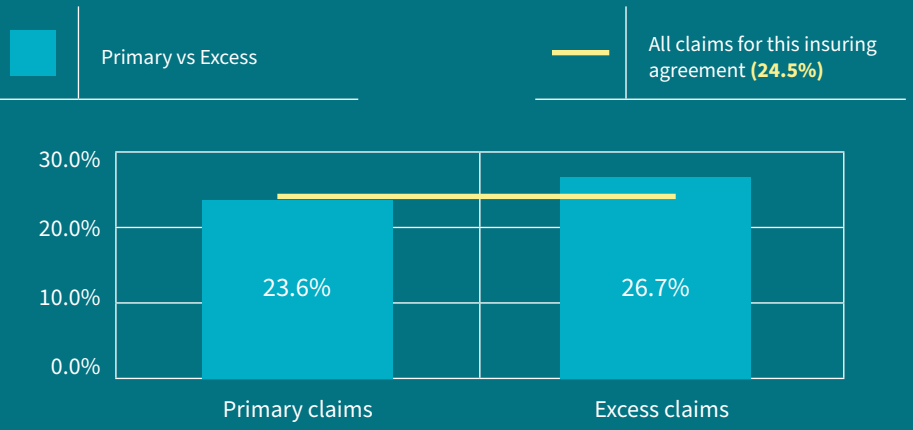


	Data breach response / crisis	Business interrruption	Extortion	Privacy and cyber security	Data recovery	Average across other insuring agreements
Not Triggered	44.4%	62.6%	66.9%	68.9%	76.2%	96.6%
Triggered (no loss impact known)	3.6%	7.3%	9.6%	3.3%	5.0%	0.5%
Triggered (some loss impact)	27.5%	12.6%	11.6%	14.6%	17.5%	1.4%
Triggered (main driver of loss)	24.5%	17.5%	11.9%	13.2%	1.3%	1.6%

Insuring agreements in cyber claims

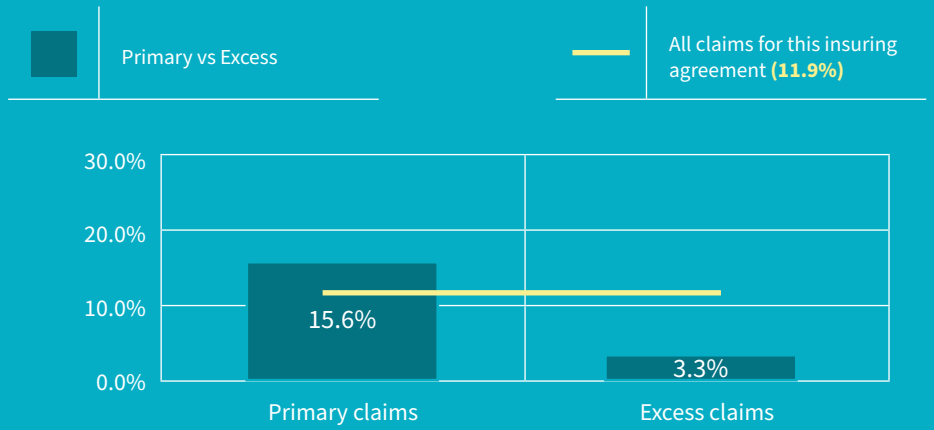
Data breach response / crisis management

Proportion of instances within the sample (by claim count, across all year) where this insuring agreement is identified as main driver of loss.



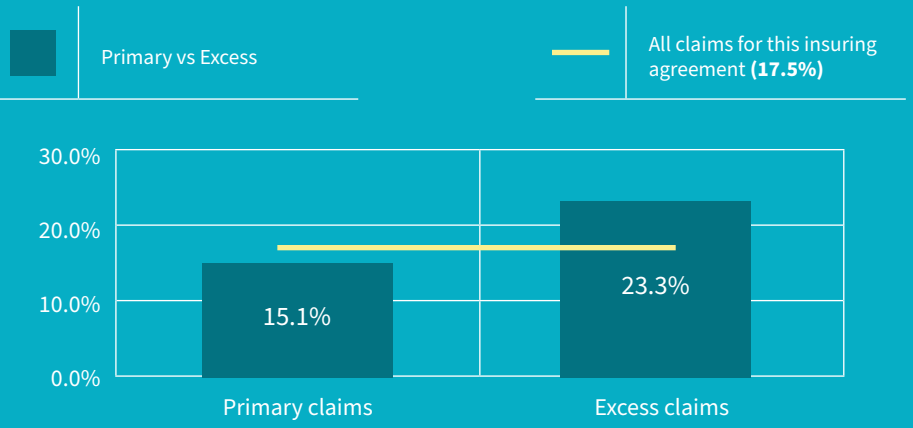
Extortion

Proportion of instances within the sample (by claim count, across all year) where this insuring agreement is identified as main driver of loss.



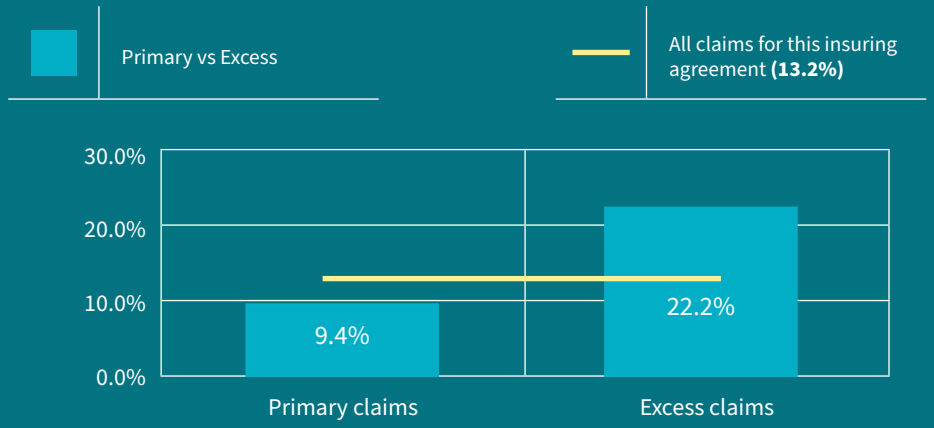
Business interuption

Proportion of instances within the sample (by claim count, across all year) where this insuring agreement is identified as main driver of loss.



Privacy and cyber security

Proportion of instances within the sample (by claim count, across all year) where this insuring agreement is identified as main driver of loss.

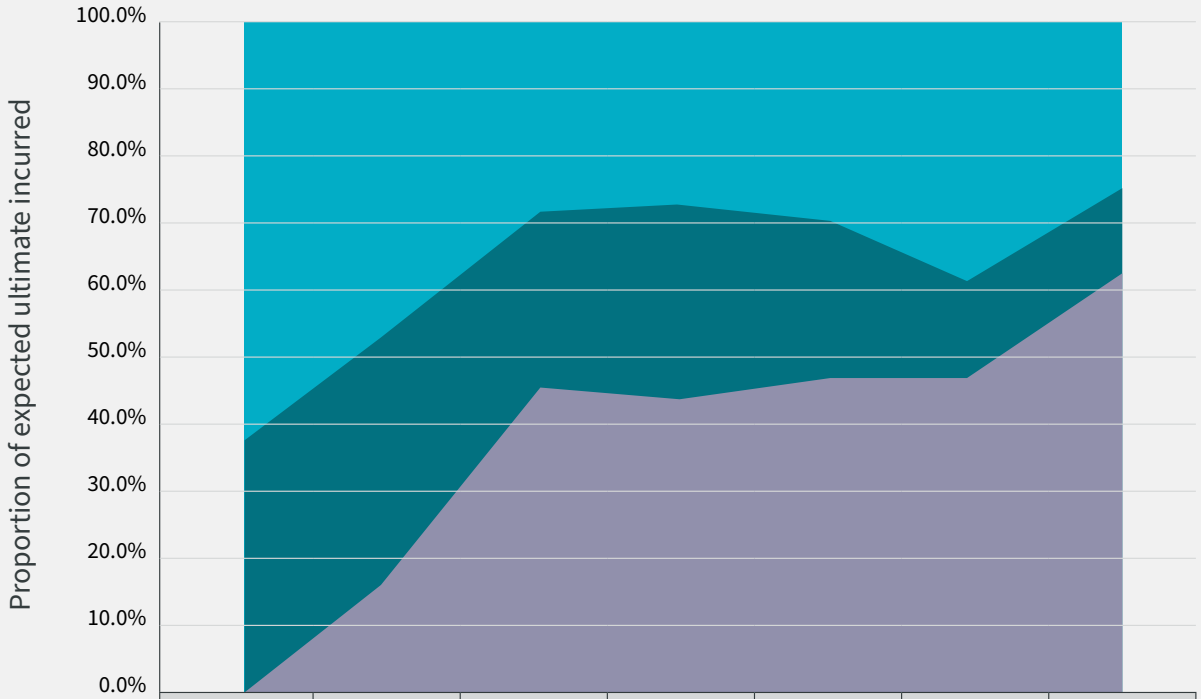


Causes of loss

Ransomware claims became noticeable in our portfolio since around 2018, and quickly emerged as a leading cause of large claims. It impacted 54.3% of claims in the sample for the period 2019 and onwards.

Ransomware claims tend to develop more rapidly compared to other types of claims, highlighting the need for actuaries to segment projections based on cause type. Even adjusting for this, the prominence of ransomware as a dominant cause of large insurance losses in recent years is very significant.

Split of ultimate large losses (year by year) between most dominate causes

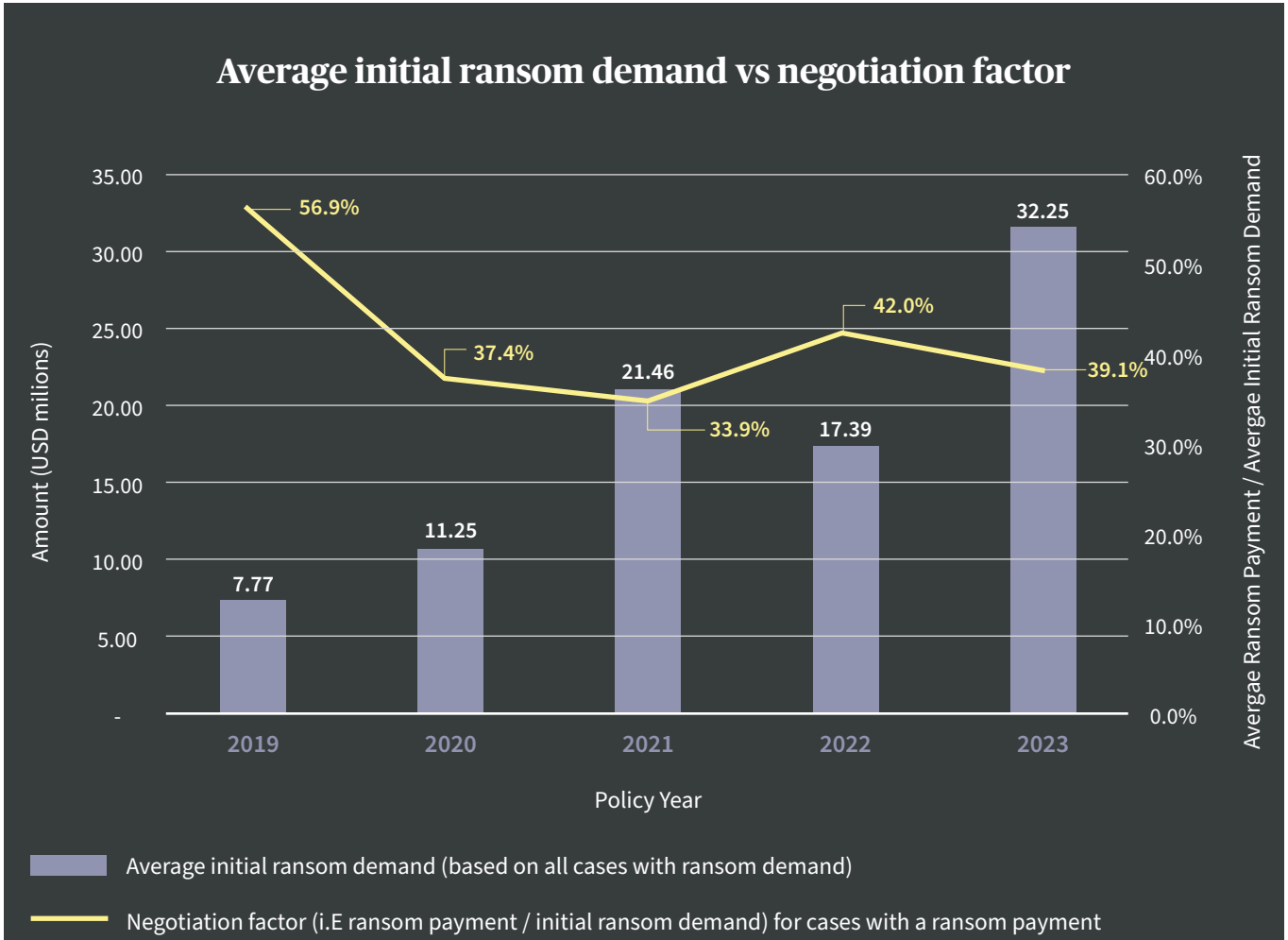


	2010/2017	2018	2019	2020	2021	2022	2023
Other	62.3%	46.2%	28.1%	27.3%	29.7%	37.2%	24.0%
Data breach	37.7%	37.9%	29.2%	29.2%	23.7%	16.0%	13.3%
Ransomware	0.0%	15.9%	45.1%	43.4%	46.6%	46.6%	62.8%

Policy Year

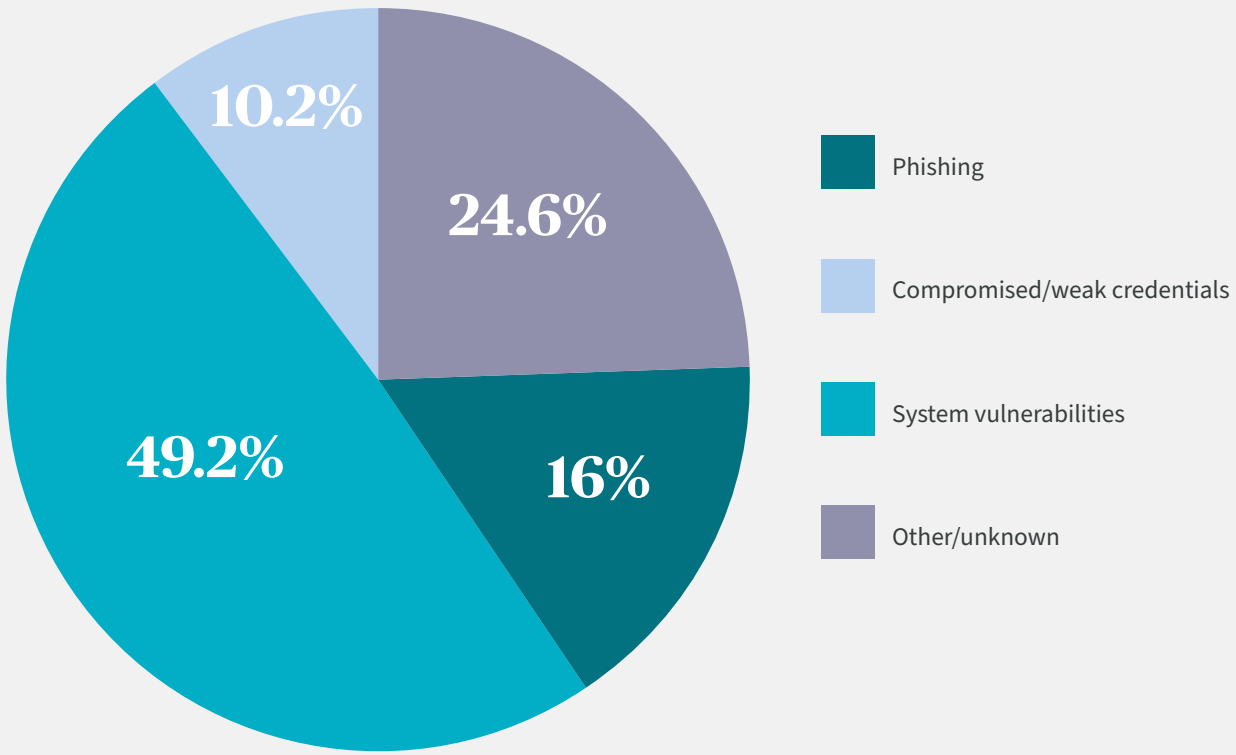
Trends in ransomware

Our report identifies several critical trends surrounding ransomware claims. For one, insureds are experiencing higher ransom demands, leading to a more discerning approach in deciding whether to pay. The increase in demands raises questions about the cost-effectiveness of paying versus investing in cybersecurity.



Negotiation dynamics are changing too. The effectiveness of ransom negotiations has evolved, with various ransom negotiators now involved in the process, which may influence outcomes. The presence of experienced negotiators can potentially reduce ransom amounts and improve recovery outcomes.

Actions taken by attackers



Analysis of attack vectors reveals that exploiting system vulnerabilities remains the most common method for threat actors to gain access in a ransomware attack.

Our claims analysis uncovered some interesting observations.

First, attackers often exploit admin credentials to move laterally within networks, resulting in higher average severities. This lateral movement can amplify the impact of an attack, as it allows the threat actor to compromise additional systems and data.

Also, threat actors increasingly employ various tactics, such as data exfiltration followed by encryption, to maximize leverage during ransom negotiations. This multifaceted approach complicates recovery efforts and increases the overall cost of incidents.

Business impact of ransomware

The analysis indicates that ransomware incidents often lead to significant business interruptions, with some level of systems shutdowns occurring in approximately 92% of these cases.

The analysis found that businesses typically required around two full months to restore operations following a ransomware attack. The lengthy restoration periods emphasize the need for robust business continuity planning.

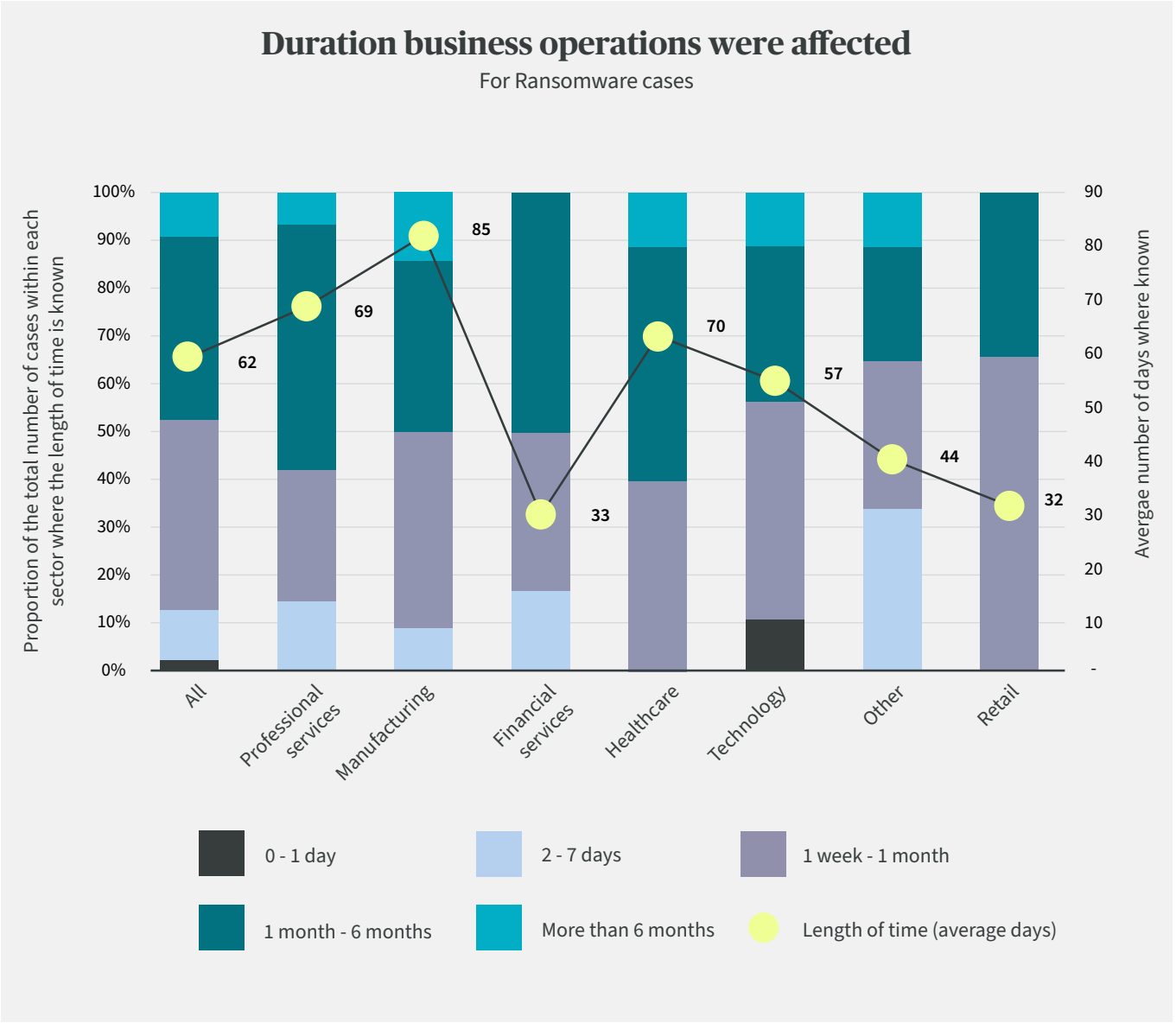
Different sectors appear to experience varying impacts from ransomware, with manufacturing firms typically taking longer to recover compared to retail companies, for example. Understanding these sector-specific dynamics is crucial for tailoring risk management strategies.

It was encouraging to notice some positive trends which suggest that organizations are becoming better at managing ransomware threats, such as:

a) **A decrease in "claims frequency where backups were affected**

b) **A reduction in the number of days for ransomware victims being able to restore operations**

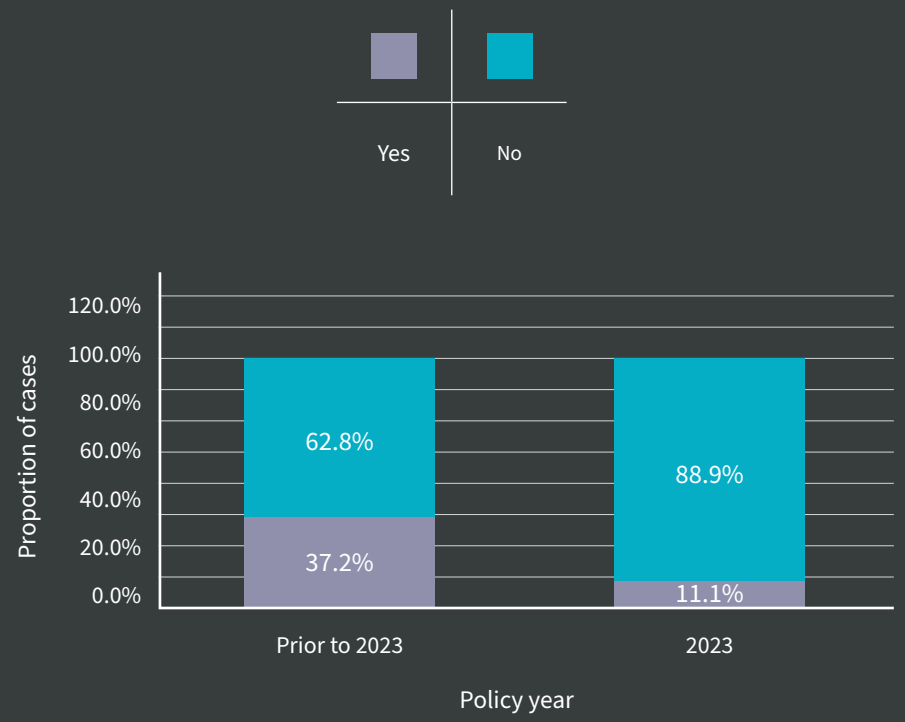
These improvements might be indicative of shifts in risk management practices, where companies are investing more in cybersecurity measures.



Business impact of ransomware

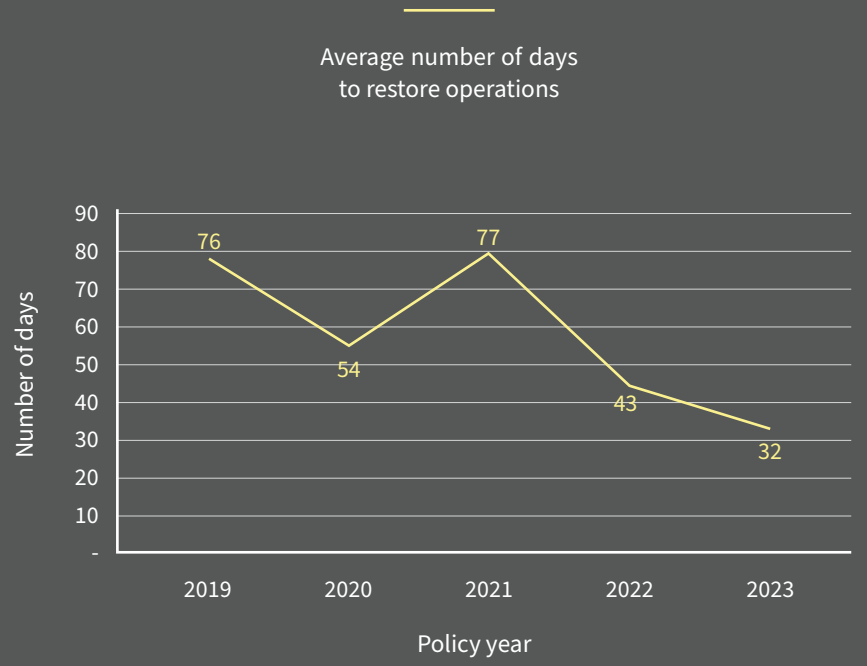
Backups affected?

For Ransomware claims where this is known



Average number of days to restore operations

Ransomware cases involving disruptions, where the number of days is known

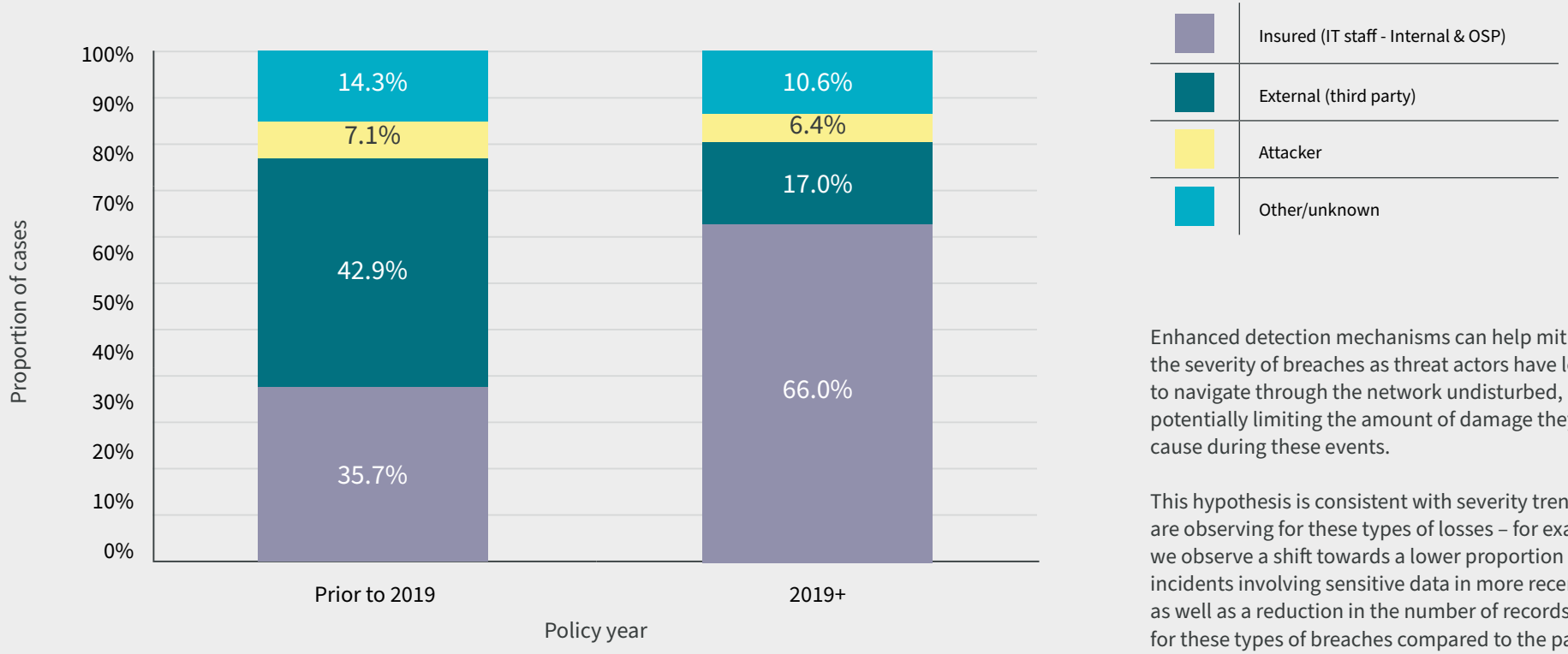


Data breaches and third-party claims

While ransomware claims dominate the landscape, non-ransomware data breaches continue to be significant. A growing proportion of data breach incidents are being identified by insureds rather than external parties, suggesting improved monitoring capabilities.

Who was the attack flagged by?

For data breach cases



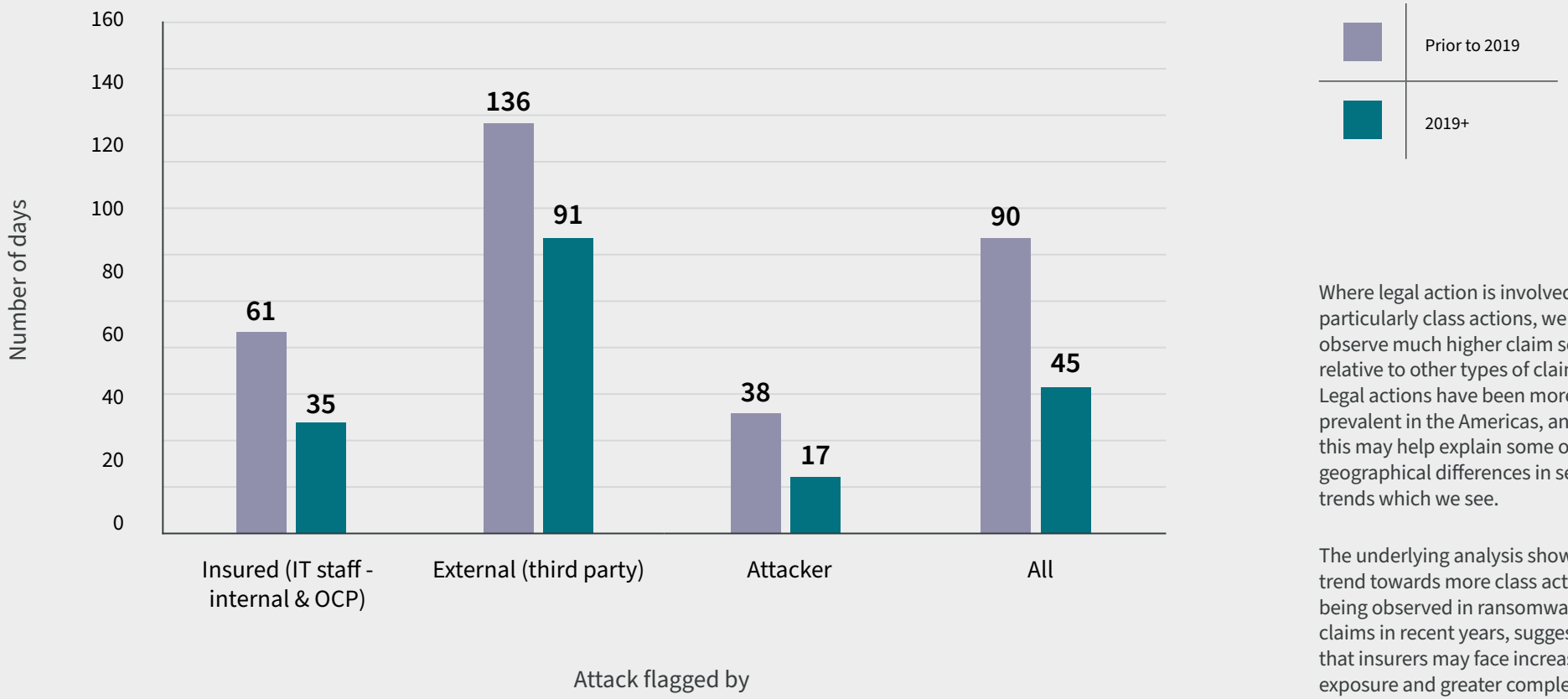
Enhanced detection mechanisms can help mitigate the severity of breaches as threat actors have less time to navigate through the network undisturbed, hence potentially limiting the amount of damage they can cause during these events.

This hypothesis is consistent with severity trends we are observing for these types of losses – for example, we observe a shift towards a lower proportion of incidents involving sensitive data in more recent years, as well as a reduction in the number of records involved for these types of breaches compared to the past.

Data breaches and third-party claims

Average number of days before attacker was noticed

Data breach cases where this is known



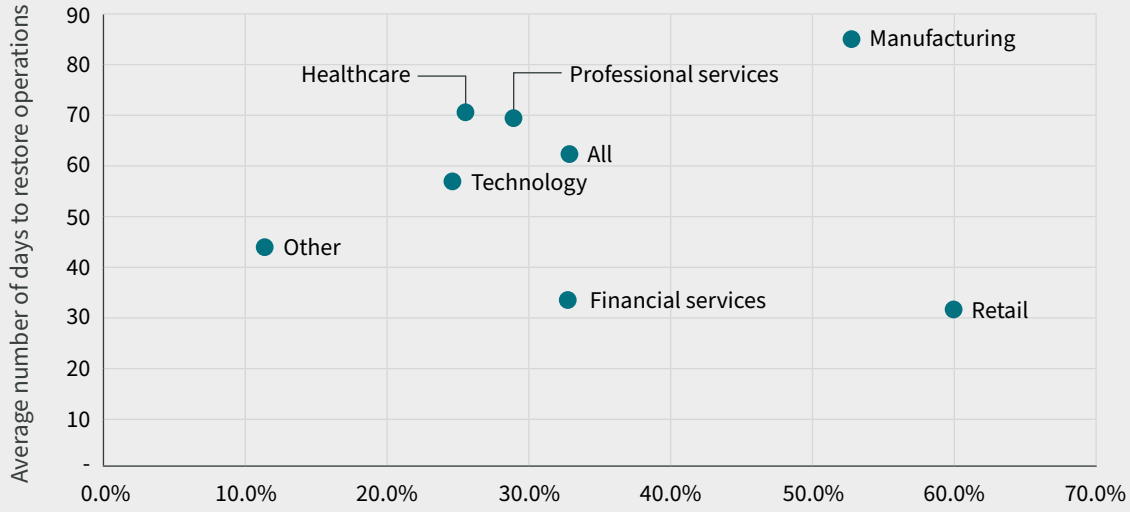
Where legal action is involved, particularly class actions, we observe much higher claim severity relative to other types of claims. Legal actions have been more prevalent in the Americas, and this may help explain some of the geographical differences in severity trends which we see.

The underlying analysis showed a trend towards more class actions being observed in ransomware claims in recent years, suggesting that insurers may face increased exposure and greater complexity in these claims.

Industry and size matters

The analysis emphasizes the importance of industry and size in understanding cyber claims frequency and severity.

For example, we observe that Ransomware claims in certain industry sectors (such as manufacturing or retail) have a greater propensity to trigger business interruption compared to others. In the case of retail companies, this is despite the number of days to restore operations being relatively low compared to other industries. This suggests that one day of business interruption for a retail company is significantly more disruptive than it may be for companies in other industries – hence efforts to improve business continuity in a Ransomware event will have a differing level of ultimate impact depending on the business activity of the victim.



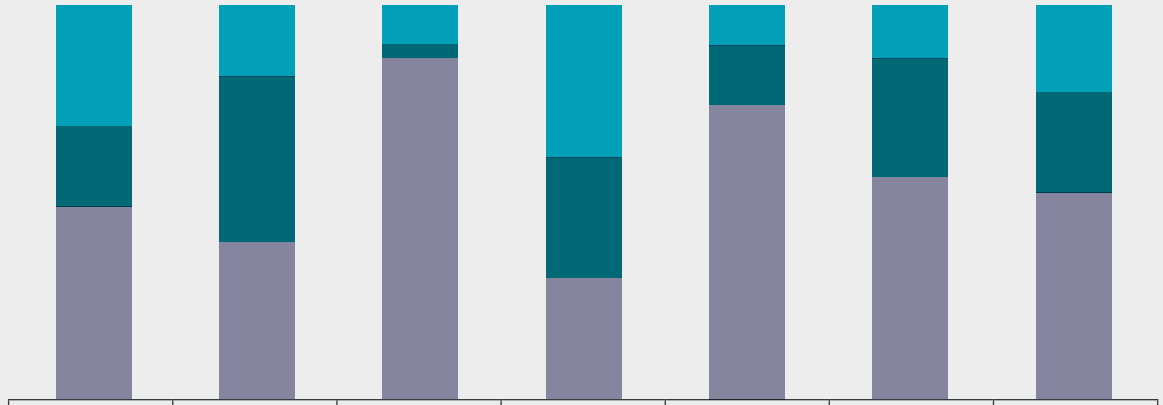
In addition – certain sectors, such as healthcare and financial services, are experiencing higher relative frequencies of large claims compared to others. Healthcare organizations manage vast amounts of sensitive personal data, including patient records and financial information. The breach of this data can lead to severe legal and financial repercussions, driving up claim sizes. The healthcare sector is heavily regulated, with laws like HIPAA in the U.S. mandating stringent data protection measures. Breaches can lead to not only financial losses but also significant fines, further increasing the claims.

Financial institutions hold valuable financial data that is a prime target for cybercriminals. Sectors such as retail and manufacturing also face cyber risks, but the nature and impact of breaches may differ. For instance, while retail may see claims related to payment data theft, manufacturing might face disruptions in supply chains or intellectual property theft. Moreover, the mix of causes of loss that impact companies varies depending on the industry sector – with ransomware being highly prevalent in the manufacturing sector, but much less so amongst technology companies.

Industry and size matters

Split of large loss frequency by main cause of loss

By industry sector 2019 - 2023



	Retail	Financial services	Manufacturing	Technology	Professional services	Healthcare	Other
Other	30.0%	18.2%	10.0%	38.0%	10.7%	14.3%	21.9%
Data breach	20.0%	40.9%	3.3%	30.0%	14.3%	28.6%	25.0%
Ransomware	50.0%	40.9%	86.7%	32.0%	75.0%	57.1%	53.1%

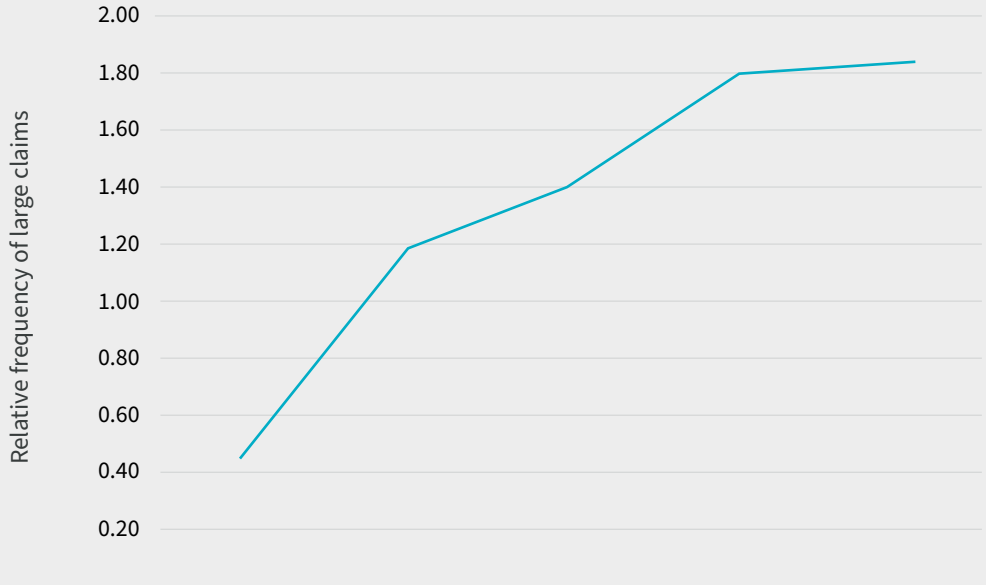
Understanding these nuances can help insurers tailor their approaches.

Size of company is also a key factor. Larger companies tend to have higher frequencies of claims, reflecting their greater exposure to cyber risks. In addition, larger companies often have more extensive networks and a larger number of endpoints, making them more attractive targets for cybercriminals. This increased complexity can lead to higher claim frequency.

Industry and size matters

Average Relative frequency of large claims

Primary policies 2019 - 2023



	0-250m	250m-500m	500m-750m	750m-2bn	2bn+
Average relative frequency of large claims (primary policies)	0.45	1.19	1.40	1.80	1.86

While larger firms may have more resources to invest in cybersecurity, these resources must protect a broader and more complex attack surface. Increased Personal Identifiable Information (PII), regulatory scrutiny and reputation risk among others can lead to larger financial implications when breaches occur. The larger the organization, the more media attention breaches garner, often leading to greater severity and therefore, larger claims.

While SMEs may experience fewer claims, they are often less equipped to effictively defend against cyber threats. This can lead to significant financial impact when breaches do occur, signaling a need for tailored insurance solutions and relevant services that reflect their unique vulnerabilities and risk profiles.

Insurers can benefit from analyzing segment-specific data (e.g. size and industry sectors) as we do at AXA to create tailored underwriting approaches and to develop effective risk management solutions that reflects the unique cyber risk profile of each organization.

Helpful insights

Our analysis underscores the need for a nuanced understanding of the evolving cyber risk landscape. As cyber threats continue to evolve, it is imperative all experts in the field remain agile and informed, leveraging insights from data to navigate the complex landscape of cyber insurance effectively.

Analysis of claims data by technical experts can reveal underlying narratives about cyber incidents, highlighting patterns and vulnerabilities that often go unnoticed.

Combining our experience with proprietary data insights enables us to help clients prioritize their cybersecurity investments and implement targeted strategies which mitigate future risks - creating the solutions that matter most to our clients.