wtw | Willis

Getting value from cyber insurance

Cyber Claims in Focus 2026

How to use this report

Willis Cyber is dedicated to helping organizations get more value and greater assurance from cyber insurance. To help you do this, this report uncovers the trends, causes and costs of the main cyber loss events most likely to hit your business.

Our analysis draws on our dataset from 2013 to January 2026, representing around 5,500 claims from more than 95 countries, and around $1 billion in insurer payments. It shows cyber insurance is covering claims, with more than 95% of the average data breach loss and 90% of the average first-party loss being covered. However, we believe by analyzing how cyber losses are really happening, you can pinpoint how to get even more value from your cyber insurance and support more effective cyber risk management.

> **"Cyber insurance is covering claims, with more than 95% of the average data breach loss and 90% of the average first-party loss being covered..."**

Key themes, insight and next steps for your business

Our numbers show data breaches as the most frequently reported event, with malicious data breaches being the most frequently occurring type. Ransomware losses have the highest financial severity, largely driven by disrupted productivity and prolonged downtime. Third-party vendors are responsible for an increasing proportion of losses, while exposure to single third-party vendor incidents impacting multiple organizations continues to affect exposures.

AI isn't yet appearing as a stand-alone driver of cyber insurance claims, but is fueling risk volatility by materially amplifying existing threats such as social engineering and ransomware attacks.

This report includes practical ideas on how your business can get ahead of these major drivers of cyber insurance losses, as well as mitigate the impacts of regulation and AI on your cyber risk exposures.

Each core section gives you:

- Key claims data insight
- What this means for your business
- Steps to better prepare, respond and recover from the cyber risks in focus.

To bring issues to life and share lessons learned, we also feature real-business case studies and industry-specific spotlights.

“AI isn't yet appearing as a stand-alone driver of cyber insurance claims, but is fueling risk volatility”

What does this report cover?

What do **ransomware** losses look like now and how is cyber insurance responding?
Read now

How can you assess and protect your business from **third-party cyber risks** now?
Read now

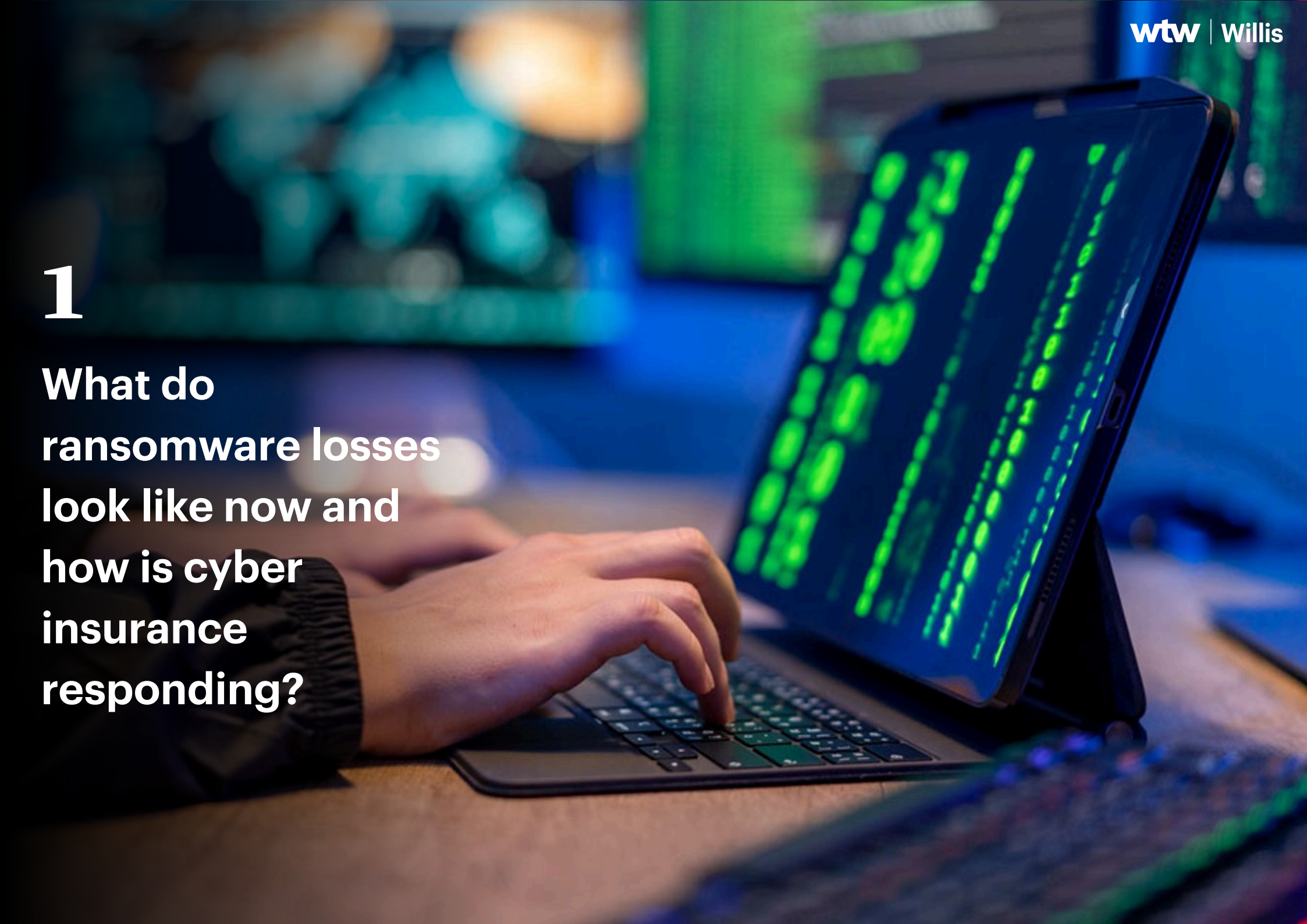
How is **AI** driving claims and how is cyber insurance responding?
Read now

Why is **cyber regulation** driving costs and how can you manage them?
Read now

How can you get **more value from cyber insurance** in 2026?
Read now

Five **priority steps** to get more value from cyber insurance
Read now

How Willis Cyber helps you better assess, quantify, protect and recover from cyber risks
Read now



1

What do ransomware losses look like now and how is cyber insurance responding?

Key claims data insight

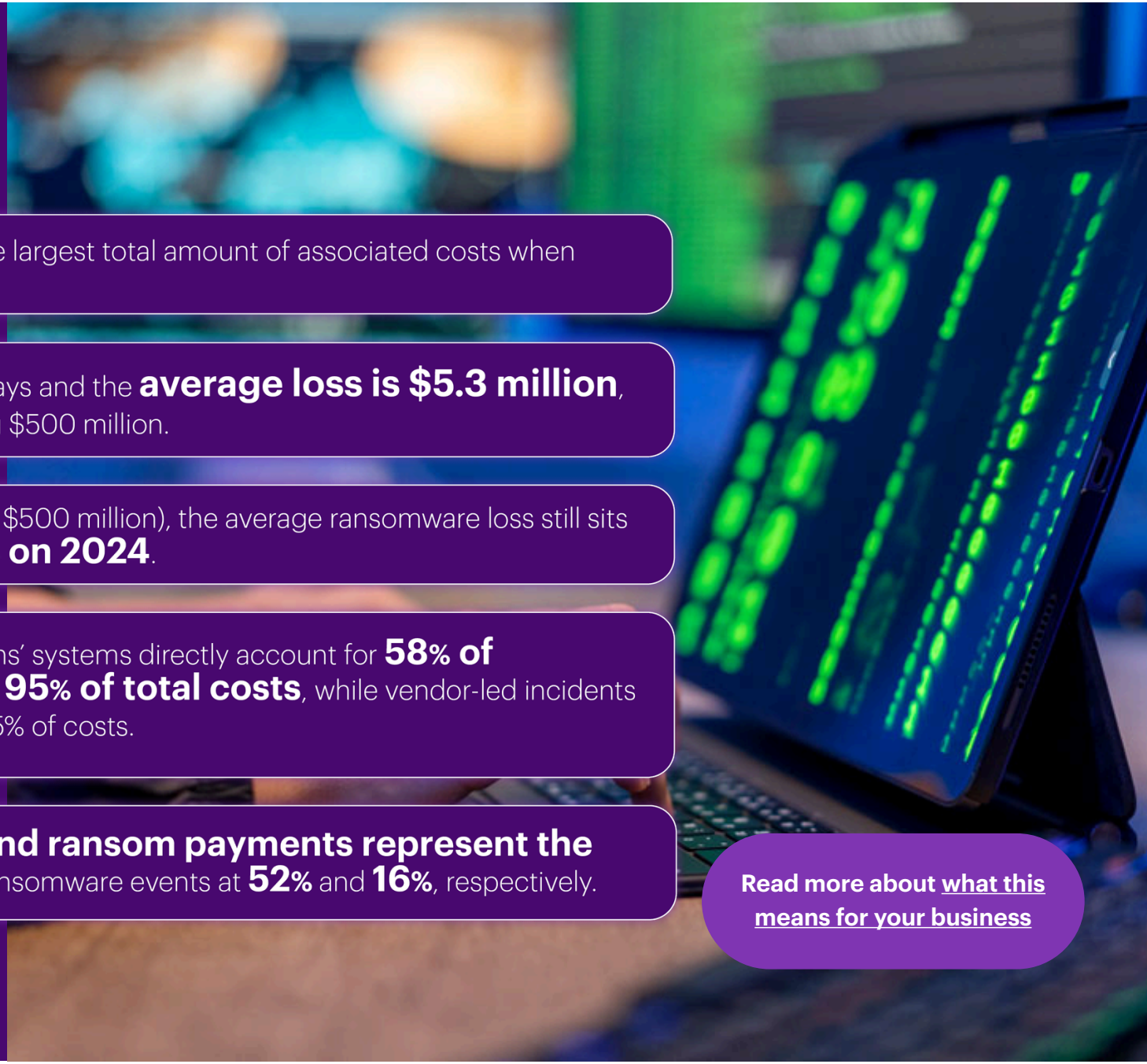
Ransomware incidents have the largest total amount of associated costs when compared to other cyber incidents.

The average ransomware event lasts 25 days and the **average loss is $5.3 million**, with the largest single loss now exceeding $500 million.

Even when we exclude the largest loss (of $500 million), the average ransomware loss still sits at **$2.9 million in 2025, up 7.5% on 2024**.

Events where attackers target organizations' systems directly account for **58% of ransomware notifications and 95% of total costs**, while vendor-led incidents account for 42% of notifications but only 5% of costs.

Business interruption losses and ransom payments represent the two largest cost elements for ransomware events at **52%** and **16%**, respectively.



Read more about what this means for your business

What this means for your business

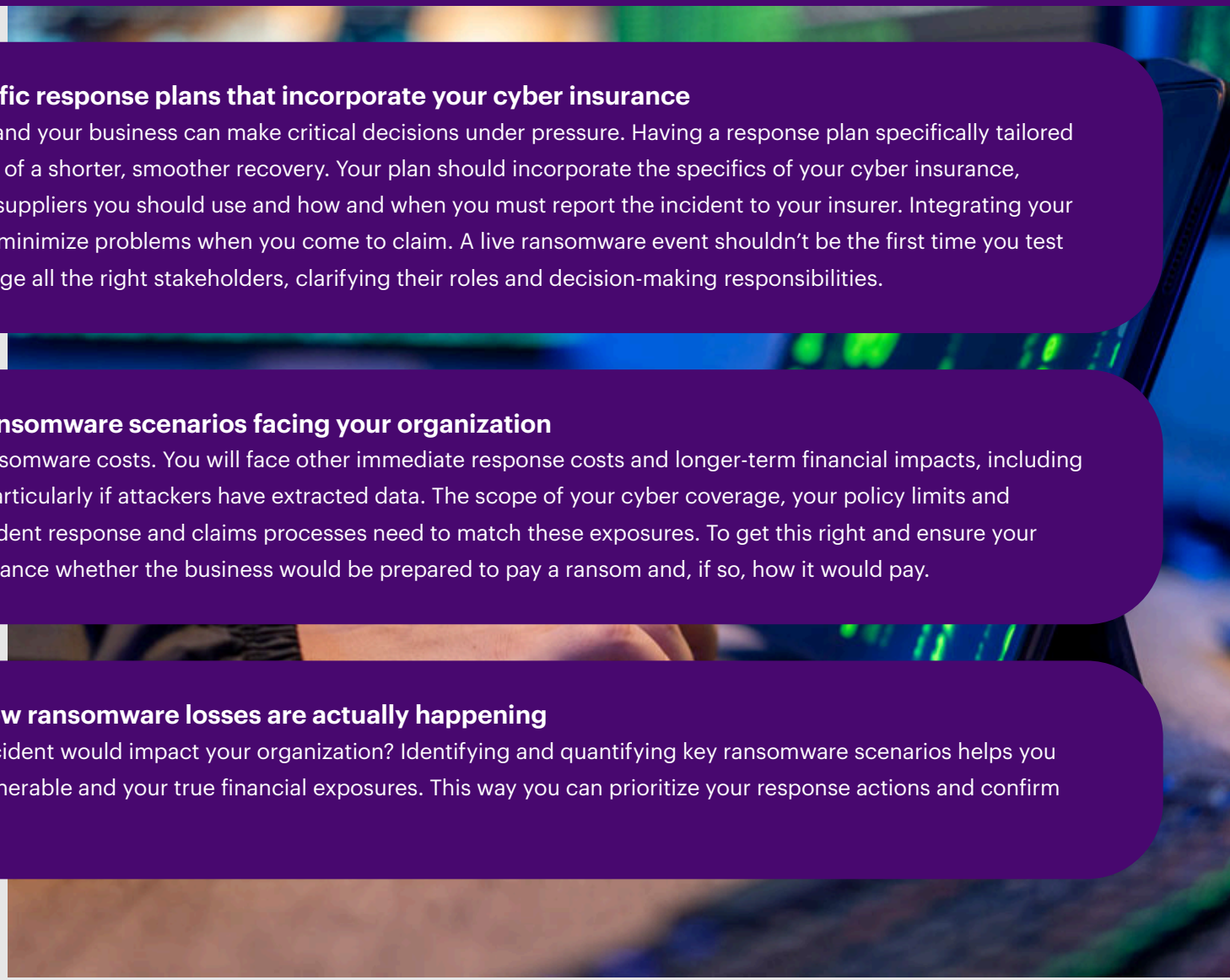
Ransomware is the highest-severity risk in our dataset and one of the most expensive categories of all cyber events. It's also impacting organizations large and small.

Organizational disruption from ransomware is often greater than expected, which can lead to underinsurance. If your business relies on time-sensitive systems, ransomware is the threat most likely to generate significant losses as a result of downtime, lost productivity, interrupted customer services and the cost of rebuilding systems. Every hour you can cut from ransomware discovery and recovery timelines can reduce total costs.

If attackers hit you directly, it's usually more costly than if they hit your vendors. However, direct attacks tend to be discovered faster than vendor-originating events. This means third-party vendor incidents can add days to the total duration of incidents, making recovery more complicated and expensive than it may have otherwise been.

"
"Every hour you can cut from ransomware discovery and recovery timelines can reduce total costs."

Priority steps to better prepare, respond and recover from ransomware attacks



1

Develop and test ransomware-specific response plans that incorporate your cyber insurance

Ransomware incidents move fast and demand your business can make critical decisions under pressure. Having a response plan specifically tailored to ransomware will maximize your chances of a shorter, smoother recovery. Your plan should incorporate the specifics of your cyber insurance, including the approved incident-response suppliers you should use and how and when you must report the incident to your insurer. Integrating your cyber insurance into response plans helps minimize problems when you come to claim. A live ransomware event shouldn't be the first time you test your plan. Test your plans regularly to engage all the right stakeholders, clarifying their roles and decision-making responsibilities.

2

Identify and quantify the specific ransomware scenarios facing your organization

Paying a ransom is only one element of ransomware costs. You will face other immediate response costs and longer-term financial impacts, including damage to your reputation and revenue, particularly if attackers have extracted data. The scope of your cyber coverage, your policy limits and retentions and the foundations of your incident response and claims processes need to match these exposures. To get this right and ensure your insurance aligns, you should discuss in advance whether the business would be prepared to pay a ransom and, if so, how it would pay.

3

Align your insurance coverage to how ransomware losses are actually happening

Do you know how a 25-day ransomware incident would impact your organization? Identifying and quantifying key ransomware scenarios helps you understand where the business is most vulnerable and your true financial exposures. This way you can prioritize your response actions and confirm you have the right cyber insurance limits.

Industry spotlight: Manufacturing

Manufacturing is among the industries persistently reporting cyber incidents more than others.

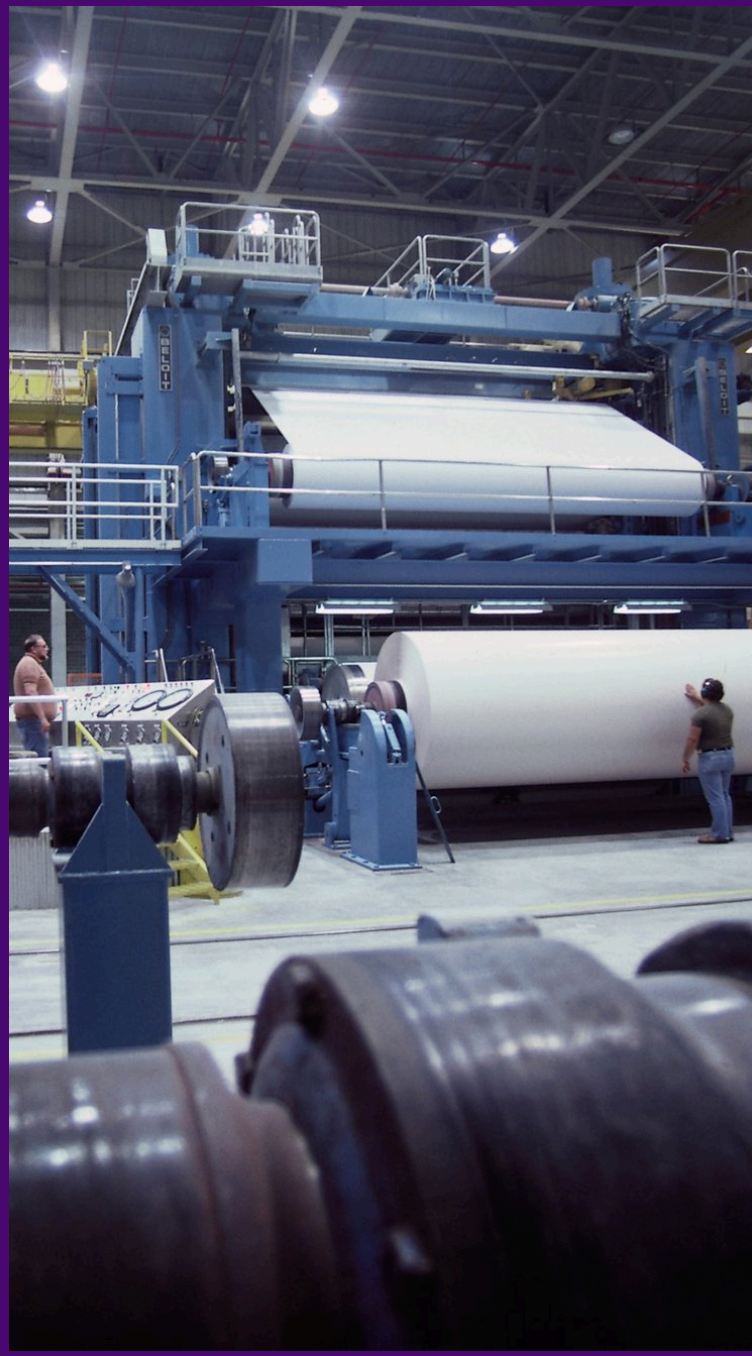
The sector accounts for around **13% of all cyber notifications** in our dataset, with ransomware as the top driver of the most costly and damaging events for the industry.

Case study: Ransomware attack on critical systems

Attackers accessed a global manufacturing company's network and encrypted critical systems across multiple production sites. While the business identified the breach quickly and disconnected plants within two hours, operations were disrupted for several weeks while systems were restored.

Costs exceeded $80 million, with the business interruption costs alone hitting the maximum amount the manufacturer's cyber insurance policy could pay out.

The business has since strengthened its cyber security controls and runs regular recovery exercises to better protect against and recover from ongoing cyber threats.



2

How can you assess and protect your business from third-party cyber risks?

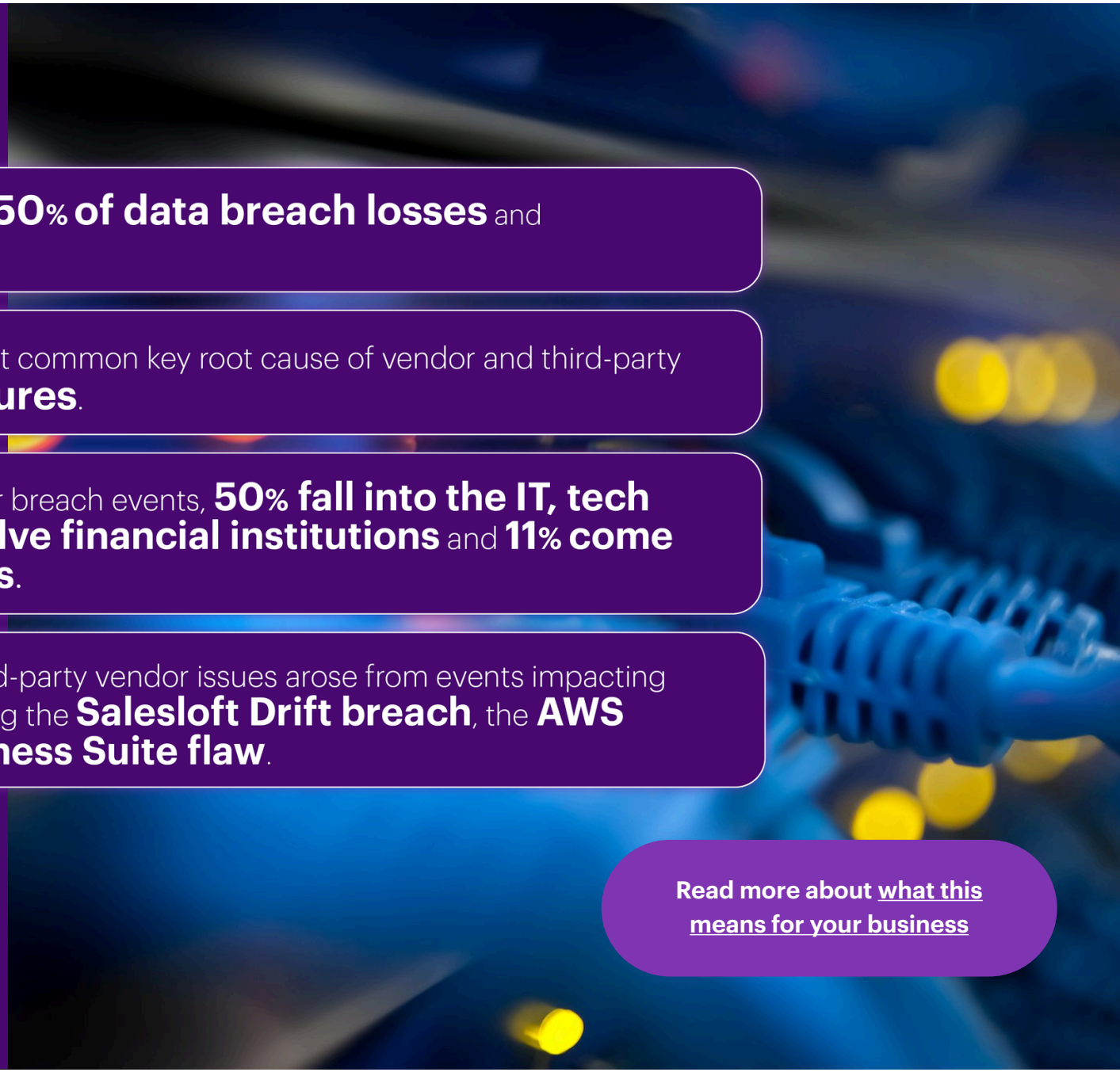
Key claims data insight

Third parties are responsible for nearly **50% of data breach losses** and **29% of first-party losses**.

Security breaches are the most common key root cause of vendor and third-party issues, followed by **IT system failures**.

Among the third parties responsible for breach events, **50% fall into the IT, tech or telecom** categories, **17% involve financial institutions** and **11% come from administrative services**.

11% of notified claims from third-party vendor issues arose from events impacting multiple organizations in 2025, including the **Salesloft Drift breach**, the **AWS Outage** and the **Oracle E-Business Suite flaw**.



Read more about what this means for your business

What this means for your business

Don’t underestimate your potential exposure to third-party vendor breaches and failures. Your exposures aren’t confined to technology vendors, but extend to administration and support services. Major third-party system outages can impact your revenues and create longer-term liabilities and financial and reputational damage, even if it isn’t your fault.

Given the increasing interconnectivity between businesses, tightening your oversight and monitoring of third-party vendors, including understanding your IT vendors’ vendors, could be one of the most financially impactful elements of your cyber risk and insurance strategy.

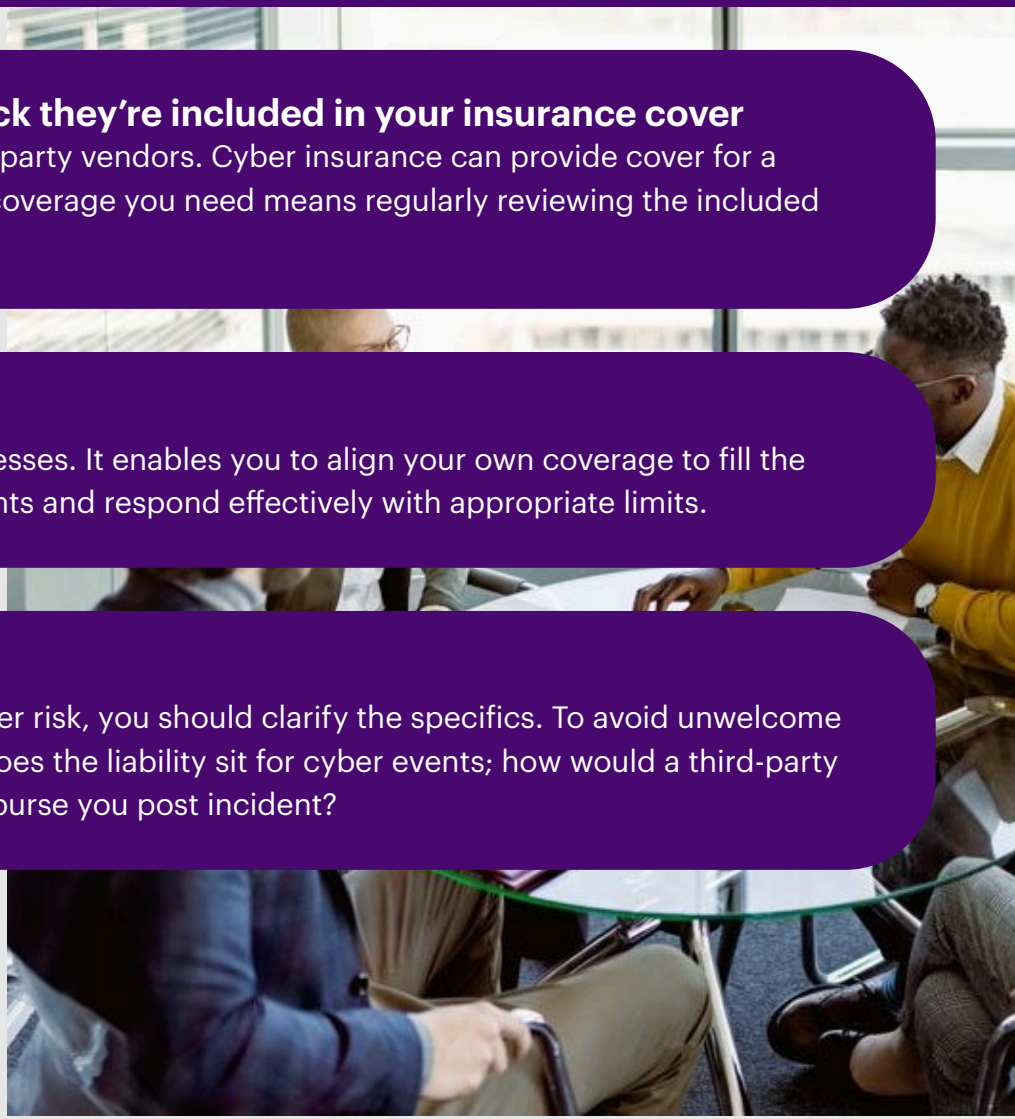
“Major third-party system outages can impact your revenues and create longer-term liabilities and financial and reputational damage, even if it isn’t your fault."

Priority actions to better prepare, respond and recover from third-party vendor risks

1 **Identify your most critical third-party vendors and check they're included in your insurance cover**
You should regularly identify and monitor any business-critical third-party vendors. Cyber insurance can provide cover for a range of third-party vendor issues, but to ensure you're getting the coverage you need means regularly reviewing the included parties and checking the extent of the cover provided.

2 **Don't assume your contract will protect you**
This should be a routine part of your selection and contracting processes. It enables you to align your own coverage to fill the gaps and offers assurance your vendors are ready to manage incidents and respond effectively with appropriate limits.

3 **Check your third-party vendors' cyber insurance**
While contractual terms normally provide some protection from cyber risk, you should clarify the specifics. To avoid unwelcome surprises in the event of an incident, confirm the following: Where does the liability sit for cyber events; how would a third-party vendor respond to a cyber incident; to what extent would they reimburse you post incident?



Case study: Transportation provider used cyber insurance to close contractual gaps

A major international transportation provider was impacted by a cyber issue at a key third-party service provider. While the contract provided some protection, the loss exceeded the contractual indemnity provisions. Willis Cyber specialists worked to ensure the organization's cyber insurance cover wrapped around the contract so it picked up where the contract stopped, lowering the upfront costs and covering most of the damage.

> **"...the organization's cyber insurance cover wrapped around the contract so it picked up where the contract stopped, lowering the upfront costs and covering most of the damage.**

Industry spotlight: Healthcare

Our dataset shows the healthcare industry drives the highest number of cyber notifications to insurers (20%).

Data breaches are the most frequently reported losses for the healthcare sector, accounting for **45% of notifications**. The number of records compromised is often small, with **52% of data breach claims** impacting fewer than **1,500 records**. Such incidents still drive legal and defence costs around dealing with regulators and the settlement of claims.

The healthcare sector has also been impacted by ransomware with an increase in events in recent years. Ransomware incidents now account for **18% of healthcare notifications overall**, with costs being driven by business interruption and increased costs of working.

Case study: Ransomware impacts mitigated by cyber insurance

A company providing telecare remote monitoring was hit by a ransomware attack that saw its critical systems encrypted and panic buttons provided to elderly and vulnerable people deactivated. With the support of ransom negotiators provided through the organization's cyber insurance policy, once the threat actor understood the impact on vulnerable people, they released the decryption key without the need for any payment. The insurer covered the incident response costs.

3

Is AI driving claims and how is cyber insurance responding?

Key claims data insight

While AI isn't yet appearing as a stand-alone driver of cyber insurance claims, **it is materially amplifying existing cyber exposures. The technology is increasing the scale and sophistication of both malicious cyber events, such as ransomware attacks, and AI-driven social engineering and phishing incidents using deepfakes**. The nature of AI also introduces new operational, regulatory and liability challenges that don't always fully align with traditional policy coverage.

Read more about how can your cyber insurance policy respond to AI-related threats?

How can your cyber insurance policy respond to AI-related threats?

Whether an AI-related event triggers a cyber insurance policy depends on whether it creates a covered cyber incident. Current cyber policies don't tend to distinguish between AI-enabled and non-AI-enabled events and typically don't feature AI exclusions.

Where can AI-related threats fall outside of cyber insurance?

Several AI-related costs and scenarios are less likely to be covered because they don't fit common cyber insurance clauses, including:

- The costs of retraining or restoring a machine learning model after sabotage or malfunction
- Revenue loss caused by hallucination (where an AI system invents something) or data drift (where an AI system's performance worsens because it's not using up-to-date data) where there is no covered network outage
- Regulatory actions for non-compliance with AI legislation.

How can other insurance policies respond to AI-related losses?

Because AI losses can arise in the absence of a covered cyber incident, you should look beyond cyber to understand your overall protection, including:

- Professional liability and technology errors and omissions
- Directors' and officers' liability cover for governance or disclosure failures
- Crime for fraud, insurance and impersonation events.

"Current cyber policies don't tend to distinguish between AI-enabled and non-AI-enabled events and typically don't feature AI exclusions."

Priority actions to better prepare, respond and recover from AI cyber risks

1. Identify and quantify the impact of malicious and non-malicious AI loss scenarios and map them to your current policies.
2. Review your cyber and broader insurance policies for overlaps and gaps in the most damaging malicious and non-malicious AI-related loss scenarios.
3. Stay informed on emerging AI-specific coverage where you identify gaps that could lead to significant harm to your revenue and reputation.

“
Review your cyber and wider insurance policies for overlaps and gaps of the most damaging malicious and non-malicious AI-related loss scenarios.

4

How is regulation influencing cyber insurance claims and costs and how can you manage them?

Key claims data insight

When it comes to data protection, the regulatory focus from cyber incidents is often focused on **data breaches** rather than broader privacy non-compliance issues.

Pixel-tracking litigation is the 'hidden' cyber insurance risk. Pixel-tracking incidents involve tiny, invisible images being hidden in a webpage or email. Regulators treat incidents as wrongful data collection and privacy violations, with the invisibility of pixels meaning they may be embedded without users' knowledge or consent to collect, share and track data across sites.

Within our dataset, Pixel tracking litigation represents a disproportionately large share of notifications, **accounting for 38% of all major multi-insured events and 5% of notifications overall**. While in terms of costs, they account for very little in our data set, litigation remains open and we're aware of cases leading to substantial losses across wider cyber insurance markets.

Read more about what this means for your business

What this means for your business

Global cyber and data protection regulation continues to increase in volume and complexity, particularly in sectors either handling financial, health or personal information or interacting with critical infrastructure. Regulators are shifting their focus towards broader cyber resilience. The UK's new Cyber Security and Resilience Bill and the Digital Operational Resilience Act (DORA) in the EU represent a deliberate shift from reactive, incident-focused compliance to how well organizations can withstand, respond to and recover from cyber disruption. Regulators are also moving toward shorter reporting windows and broader notification obligations, meaning your business needs to be ready to act quickly.

"Regulators are also moving toward shorter reporting windows and broader notification obligations, meaning your business needs to be ready to act quickly."

Priority actions to better assess, quantify, protect against and recover from regulatory risks

1. Be clear on the regulations that could impact your organization and understand regulators' expectations, particularly where you operate across multiple jurisdictions, bearing in mind. regulations aren't static so you should keep this under ongoing review.

2. Document your decision-making process and ensure you include regulatory notifications in your incident response planning. The cyber insurance underwriting process is an opportunity to demonstrate your organization's approach to identifying and managing cyber risk.

3. Make sure your cyber insurance reflects your regulatory exposures, including regulatory investigations, legal defense, notification and credit monitoring and strengthen coverage for privacy violations, wrongful data collection and vendor-driven outages.

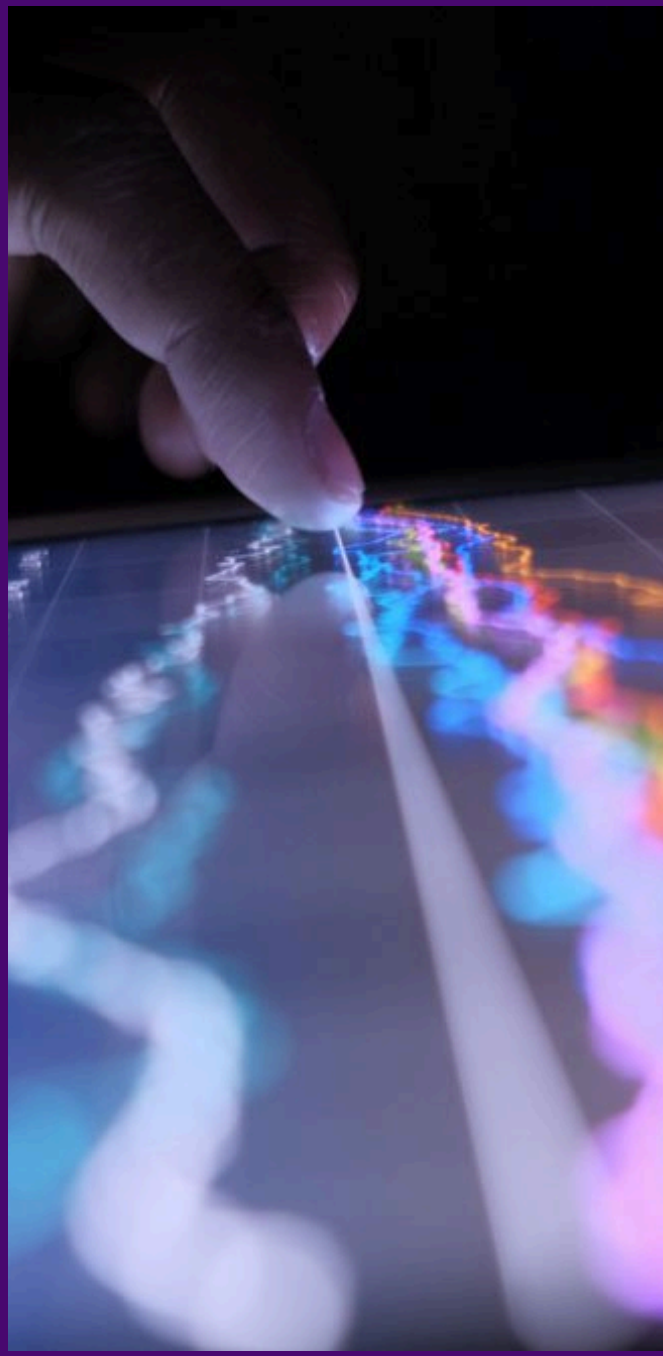
> **"Document your decision-making process and ensure you include regulatory notifications in your incident response planning"**

Industry spotlight: Financial institutions

Financial institutions account for **16% of all cyber notifications in our dataset**, with the insurance sector alone representing almost half (49%) of FI-related incidents. The sector exhibits the highest concentration of data breaches involving more than 100,000 compromised records.

The associated loss profile **shows financial institutions face both low-frequency, high-severity losses (exceeding $100m) and high-frequency, low-severity events (below $100k)**. The **average loss for the sector of $6.9m** is more than twice the average across all other claims in our data set.

Loss severity is largely driven by regulatory and settlement costs, alongside credit-monitoring obligations. **These account for nearly 70% of total losses incurred**. Financial institutions should consider these losses when determining the appropriate cyber insurance retentions, limits and overall program structure.



5

How can you get more value from cyber insurance in 2026?

Our data shows how cyber insurance is a vital component of cyber resilience for organizations globally. By proactively incorporating cyber insurance into strategic cyber risk management, your organization can maximize the value cyber insurance is already able to provide.

To get the strongest value from cyber insurance, your preparation needs to match the claims patterns seen across the market. The data shows organizations that act early, document decisions and engage with insurer-approved vendors capture the highest proportion of recoverable losses. In contrast, late notifications, unclear escalation routes, or calling on unapproved specialists almost always increase uninsured spending and make claims and recovery processes more challenging.

6

Five priority steps to get more value from cyber insurance

1 **Use the cyber insurance underwriting process to drive discipline and governance, rather than approaching as a tick-box exercise.**

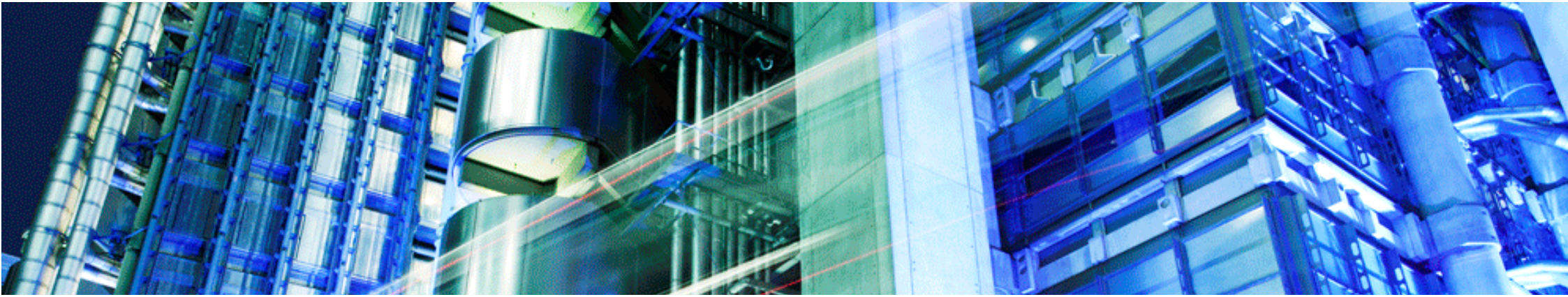
Why?

The cyber insurance underwriting process focuses on your key risks and controls and should complement your existing cyber risk management frameworks. It can provide independent validation of the maturity of your controls and demonstrate to regulators and stakeholders a strong commitment to cyber hygiene. Accurate and honest disclosure is essential to avoid coverage issues, with particular scrutiny currently on multi-factor authentication and how consistently it's deployed across your organization.

How?

Identify and engage the stakeholders best-placed to provide accurate input to the underwriting process.

If insurers' requests for information are unclear, challenge and clarify them with your broker early.



2 Align your policy coverage with your real risks, rather than assumptions.

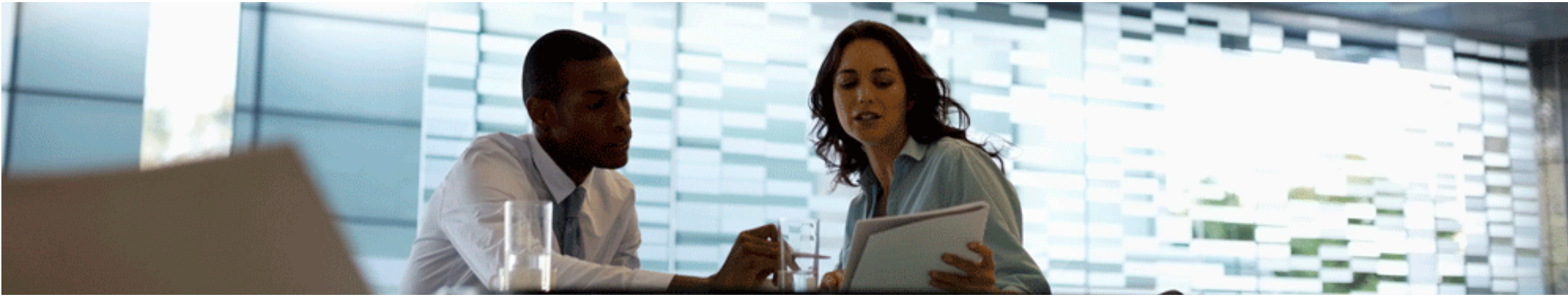
Why?

Cyber insurance cover varies widely. Understanding what you have and aligning this to your real risk exposures ensures your policy will respond as you expect and delivers value when it matters. When cover doesn't reflect reality, you risk both gaps in protection and paying for cover you may not need. Cyber risks can also extend beyond cyber insurance, so consider the impacts across your wider insurance portfolio, particularly around directors' and officers' liability.

How?

Use claims and loss data to understand how cyber losses really occur and what that means for your organization.

Prioritize your most material scenarios and design coverage around these realities instead of relying on generic assumptions.



3

Align your policy limits with your financial exposures.

Why?

Many organizations tend to base cyber insurance decisions on average breach sizes when your true exposures may be driven by low-frequency, high-severity scenarios characterized by long discovery times and extended business interruption. Aligning your limits and retention around your specific financial exposures will help prevent underinsurance, avoid overpaying for excessive limits you don't need and improve your risk transfer strategy.

How?

Use risk quantification modeling to ensure your insurance is structured to reflect the real cost of downtime, vendor failure, privacy claims and ransomware.

4

Integrate cyber insurance into your incident response and continuity planning and testing.

Why?

Your cyber insurance policy will be less effective if it isn't embedded in how you respond to an incident. Using non-approved vendors and late notification can cause issues around claims. If you're the buyer of cyber insurance and haven't yet been engaged in your organizations' cyber planning and testing, it's time to partner with colleagues. Your cyber cover is more likely to respond as the business expects when it's not seen as a stand-alone item.

How?

Review your insurer-approved vendors and hardwire them into your incident response plan so teams can act without delay.

Onboard partners early and include them in exercises.

If you rely on external providers outside the policy, agree these with your insurers in advance.

5

Maximize pre-loss risk management services to improve your cyber resilience.

Why?

Most cyber insurance provides access to a suite of pre-loss risk management services, from board-level response planning and tabletop exercises, to data services. These can complement your existing approach, fill gaps and improve your overall cyber resilience and insurance outcomes. These services are already included in the premium you pay and may enable you to eliminate spend on similar services you would otherwise pay for.

How?

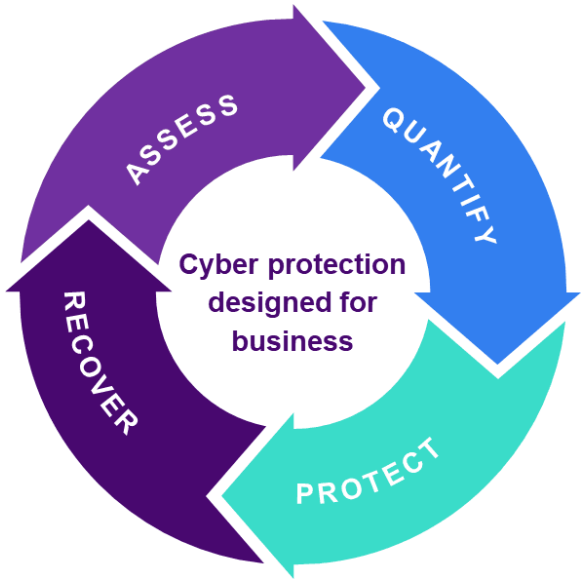
Engage with your broker and insurer to understand the full suite of what's included. Review what different insurers provide and engage with internal stakeholders to consider how these value-added services could best support you.

> **"...services are already included in the premium you pay and may enable you to eliminate spend on similar services you would otherwise pay for"**

7

How Willis Cyber helps you better assess, quantify, protect and recover from cyber risks

To protect your business revenues, stay compliant with regulation and ensure better recovery from cyber incidents, Willis Cyber specialists can help you:



Assess your cyber risks
We help identify blind spots, key vulnerabilities, regulatory exposures, third-party dependencies and uncover the cyber loss scenarios most likely to impact your industry and business.

Quantify your cyber risks
Better understand your financial exposures from cyber risks and the impact on your balance sheet, enabling business leaders to make more informed and effective cyber risk and insurance decisions

Protect against your cyber risks
We don't offer cyber insurance based on generic checklists; we build solutions around how your organization really operates and the new and emerging cyber threats most likely to hit and do damage.

Recover from your cyber risks
We support rapid and effective responses to incidents, reducing downtime and losses to strengthen your recovery.

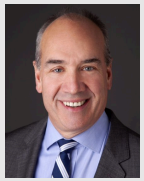
Cyber protection designed for business

How Willis Cyber helps you get more value from cyber insurance

- **Business first focus:** We start with your business priorities and what you need to protect most, recognizing how cyber risk is a wider business issue, rather than an isolated technical consideration.
- **End to end support across the cyber life cycle:** Our wide-ranging expertise that combines specialist insurance broking, cyber risk consultants, former CISOs, privacy lawyers and actuaries' means we can turn cyber complexity into clarity to enable better business decisions.
- **Aligning key stakeholders:** We help align your cyber risk stakeholders to maximize value from cyber underwriting, placement and claims.
- **Grounded in real claims:** We know what drives claims, what it costs and how you can stay ahead.
- **Global experience, local relevance:** We adapt our global insights into advice that works for where you do business.

Cyber protection designed for business

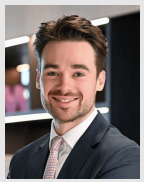
Key contacts



Peter Foster
Chairman, Global FINEX Cyber
peter.foster@wtwco.com

Glyn Thoms
Global FINEX Cyber Strategy Leader
glyn.thoms@wtwco.com

Asia



Conor Keating
Head of FINEX Cyber, Asia
conor.keating@wtwco.com

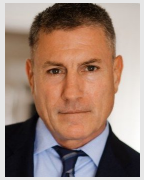
LatAm

Rodrigo Flores
Head of FINEX Cyber, LatAm
rodrigo.flores@wtwco.com

Pacific

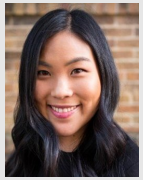
Ben Di Marco
Head of FINEX Cyber, Pacific
benjamin.dimarco@wtwco.com

EMEA

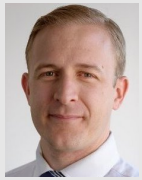


Brian Vosloh
Head of FINEX Cyber, EMEA
brian.vosloh@wtwco.com

North America



Annice Ma
Head of FINEX Cyber, North America
annice.ma@wtwco.com

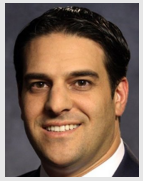


Michael Parrant
Cyber and Technology Specialist, Pacific
michael.parrant@wtwco.com

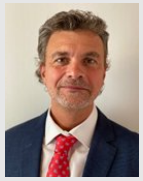
GB

Adrian Ruiz
Head of FINEX Cyber, UK
adrian.ruiz@wtwco.com

Claims



Dan Twersky
Head of Cyber Claims Advocacy
dan.twersky@wtwco.com



Adrian Cousins
Head of FINEX Claims
adrian.cousins@wtwco.com

Disclaimer

WTW offers insurance-related services through its appropriately licensed and authorised companies in each country in which WTW operates. For further authorisation and regulatory details about our WTW legal entities, operating in your country, please refer to our WTW website. It is a regulatory requirement for us to consider our local licensing requirements.

The information given in this publication is believed to be accurate as of June 2026. This information may have subsequently changed or have been superseded and should not be relied upon to be accurate or suitable after this date.

This publication webinar offers a general overview of its subject matter. It does not necessarily address every aspect of its subject or every product available in the market and we disclaimer all liability to the fullest extent permitted by law. It is not intended to be, and should not be, used to replace specific advice relating to individual situations and we do not offer, and this should not be seen as, legal, accounting or tax advice. If you intend to take any action or make any decision on the basis of the content of this publication you should first seek specific advice from an appropriate professional. Some of the information in this publication may be compiled from third party sources we consider to be reliable, however we do not guarantee and are not responsible for the accuracy of such. The views expressed are not necessarily those of WTW.

About WTW

At WTW (NASDAQ: WTW), we provide data-driven, insight-led solutions in the areas of people, risk and capital. Leveraging the global view and local expertise of our colleagues serving 140 countries and markets, we help you sharpen your strategy, enhance organisational resilience, motivate your workforce and maximise performance. Working shoulder to shoulder with you, we uncover opportunities for sustainable success — and provide perspective that moves you. Learn more at wtwco.com.

FPS: 12923804M

Thank you for reading

Getting value from cyber insurance

Cyber claims in focus 2026