HIGHSTREET
Insurance & Financial Services



Cost of a click

The 2026 cyber picture

Artificial intelligence is changing both sides of cyber risk. Yet many losses still start with ordinary openings, and some claims involve no attacker at all. This guide covers what shifted in 2026 and how cyber coverage can help.

Artificial intelligence cuts both ways in cyber risk

Everyone is talking about AI, and in cyber risk it's a tool for attackers and defenders alike. It helps cybercriminals move faster, and it helps the tools that stop them move faster too. What it hasn't changed is how most losses begin. Many of the doors cybercriminals use to breach business systems are ordinary: a password that was guessed, a vendor's access key or an old tracking code. Other cyber exposures are legal and involve no attacker at all, like privacy and copyright claims.

Each one can lead to steep costs and a large cyber insurance claim.

This guide covers three things:
how cyber risk shifted for businesses this year, what a breach costs and how coverage can offer both prevention and protection.

see possible.

What changed this year

AI changed the math

On the attack side, cybercriminals use AI to impersonate real people, build malicious software and launch attacks faster and at greater scale. More than one in four organizations hit by a malicious attack reported it was driven by AI, a 56% increase over the year before, and those attacks added about $1 million to the average breach.[1]

On the defense side, the same technology is speeding up the tools that stop them. Security teams that used AI extensively shortened their breach time by 65 days and lowered their average costs by $1.93 million.[2]

The exposure is not only external. Among small and midsize businesses, 87.3% now use AI, while 45.6% have written rules for how employees may use it.[3] Among organizations that suffered a breach involving AI, 92% lacked proper controls over who could reach those tools and the data behind them.[4]

A short, written policy naming the approved tools and the data that never goes into them is a practical first step toward closing that gap.

Attackers are scanning for easy openings

Last year, cybercriminals increasingly automated their search for unpatched weak spots in smaller businesses' systems. For businesses under $25 million in revenue, **claims became 10% more frequent while the average loss fell 15% to $77,000**.[5] That average can hit a smaller business harder than a six-figure loss hits a large company.

[1, 2 & 4] IBM (2026). Cost of a Data Breach Report 2026.
[3] National Cybersecurity Alliance (2026). 2026 Small Business Cybersecurity Awareness & Practices Survey.
[5] Coalition (2026). 2026 Cyber Claims Report.





What AI hasn’t changed

The openings behind many losses are the same ones businesses have faced for years. Here’s what they cost now, and where they start.

What a breach costs now

Measure	2026
Average US data breach[6]	$11.5 million
Average global data breach[7]	$4.99 million

A breach in the US costs more than twice the global average, because regulatory fines and other business costs run higher here. Most of any breach bill comes from investigating and managing the breach, and from the business lost while it’s handled.

Where ransomware lands

Of the ransomware cases where company size was known, 96% of victims were small and midsize businesses.[8] Ransomware lands far more often on smaller businesses than on the big names in the headlines.

How attackers got into small-business systems	Share
Unpatched vulnerability	26%
Stolen credential	13%
Phishing message	9%[9]

More than half of those breaches involved a third party.[10] A vendor’s weak spot can quickly become yours.

The ransom economy shifted

Ransom demands climbed sharply in the latest claims data, but with proper protection and planning, many victims can refuse to pay. Saying no is only possible if you can recover without the attacker’s help, which means backups you have tested and a response plan you have used.

What happened to businesses that were asked for a ransom	
Average demand	Above $1 million, up 47%
Victims who refused to pay	86%
Average payment after negotiation	$355,000[11]

Backups can mean big savings

Among small and midsize businesses, 88.4% keep backups. Only 61.4% have tested to ensure they restore.[12] Confirming your restoration capabilities before an attack can be the difference between confidently refusing a ransom and paying one.

[6&7] IBM (2026). Cost of a Data Breach Report 2026.
[8,9&10] Verizon (2026). 2026 Data Breach Investigations Report.
[11] Coalition (2026). 2026 Cyber Claims Report.
[12] National Cybersecurity Alliance (2026). 2026 Small Business Cybersecurity Awareness & Practices Survey.

What cyber insurance covers

A strong security program lowers the odds of a cyber incident. Cyber insurance can help cover what happens when that program falls short.

Response and recovery

Breach counsel, forensic investigation, customer notification, credit monitoring and crisis communications.

Business continuity

Lost income and operating expenses while your systems are down, including outages at a provider you depend on.

Extortion and fraud

Ransom and extortion payments, social engineering losses and funds transfer fraud.

Data protection

Restoring or replacing data and software that was lost or damaged.

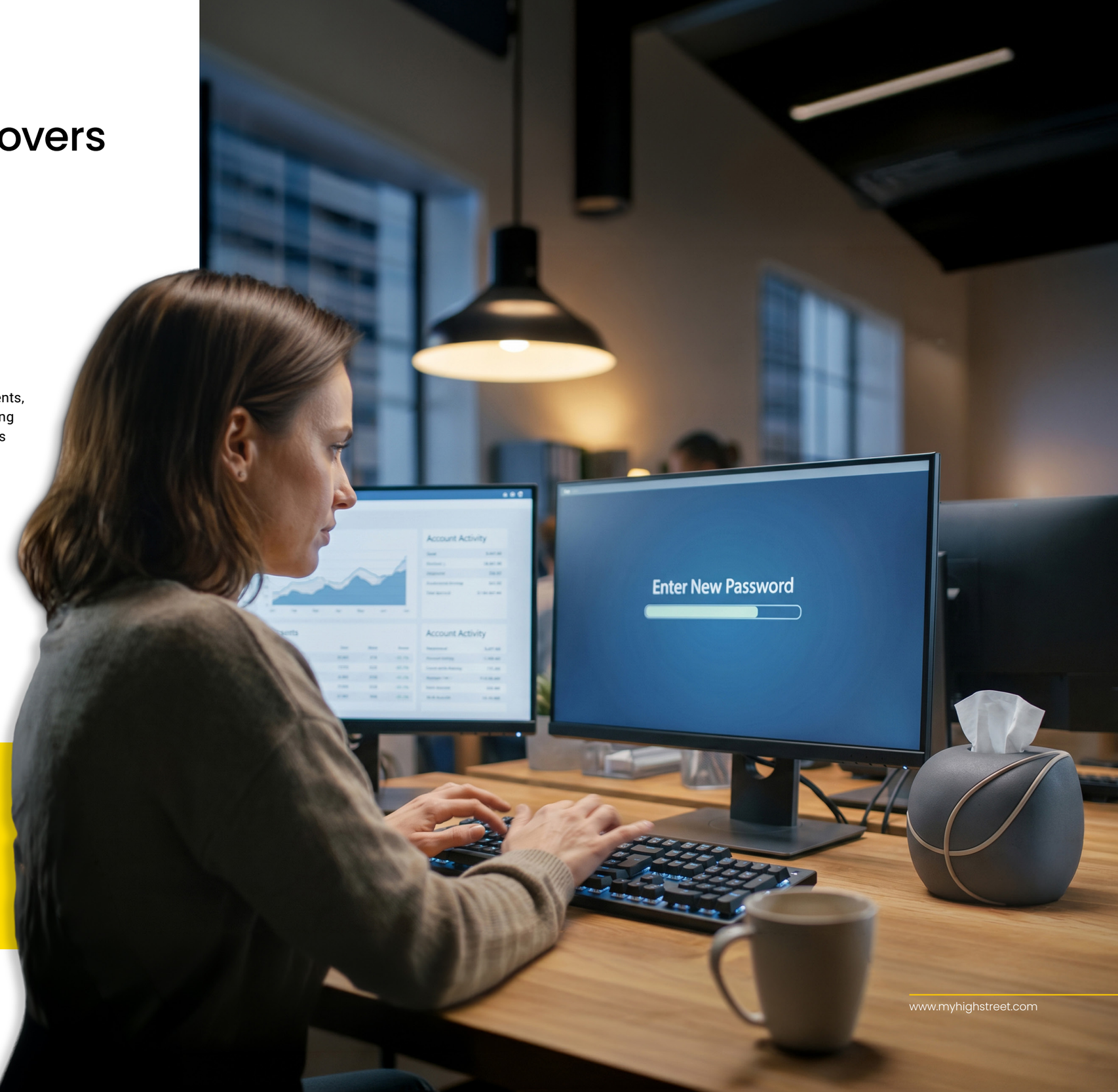
Liability

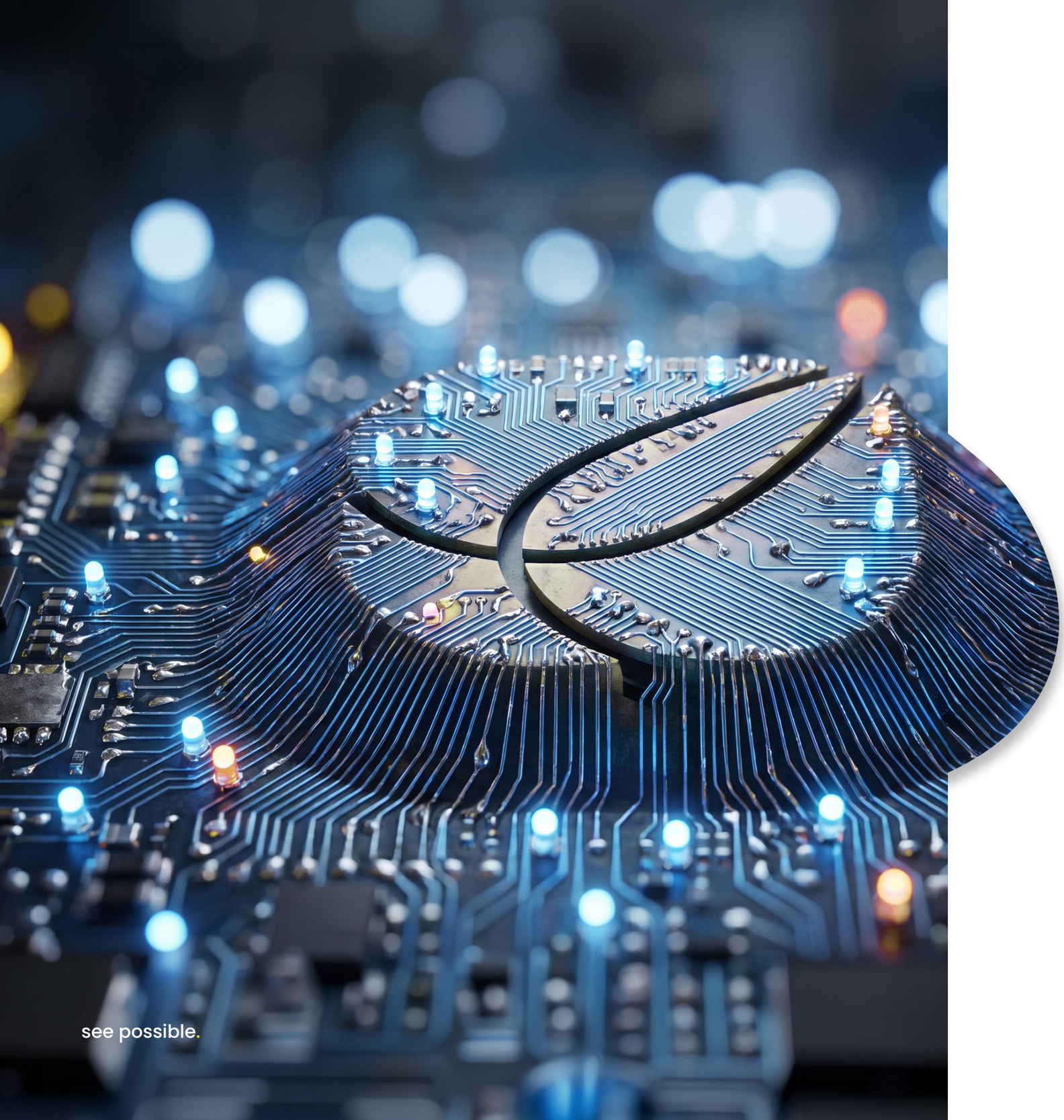
Failure to protect sensitive data, privacy and network security claims, regulatory defense and media liability.

What a policy does before the claim

A cyber policy does more than pay out after an attack. Some policies reimburse you after an incident. Others put people and tools to work before one, assessing where you are exposed, watching for threats and putting a response team on the phone while the event is still unfolding. Ask your agent which kind you are buying.

see possible.





What preparation is worth

Cyber risk reaches businesses of every size now, and not all of it arrives as an attack. Some of it is a vendor's mistake, or a tool running in the background on your own website.

What the 2026 claims show is that preparation can change the outcome. Businesses with tested backups were in a position to refuse a ransom demand. Businesses with coverage could call on counsel and a response team.

The right policy can help your business get through what comes next, and **choosing one is a decision you get to make long before anything happens.**

About Highstreet Insurance Partners

At Highstreet, our expert agents work with you to understand your business and the risks it carries, tailoring coverage to fit how you operate. **Our agents live and work where you do, backed by a national network of more than 350 offices.**

Wondering what the right cyber coverage looks like for your business? Talk with a Highstreet agent and get clear, tailored answers.

Talk to a Highstreet agent >

Want to learn more about what cyber liability insurance covers?

Explore cyber liability coverage >



HIGHSTREET
Insurance & Financial Services

©2026 Highstreet Insurance Partners Inc. All rights reserved.