HISCOX
encourage courage

The Hiscox Cyber Readiness Report 2026

US focus





Cyber security is a significant challenge for small businesses, but not just for the more well-known reasons like getting employees to use secure passwords or recognize phishing emails. In addition to the financial and reputational costs of cyber-attacks, employees can suffer an emotional toll.

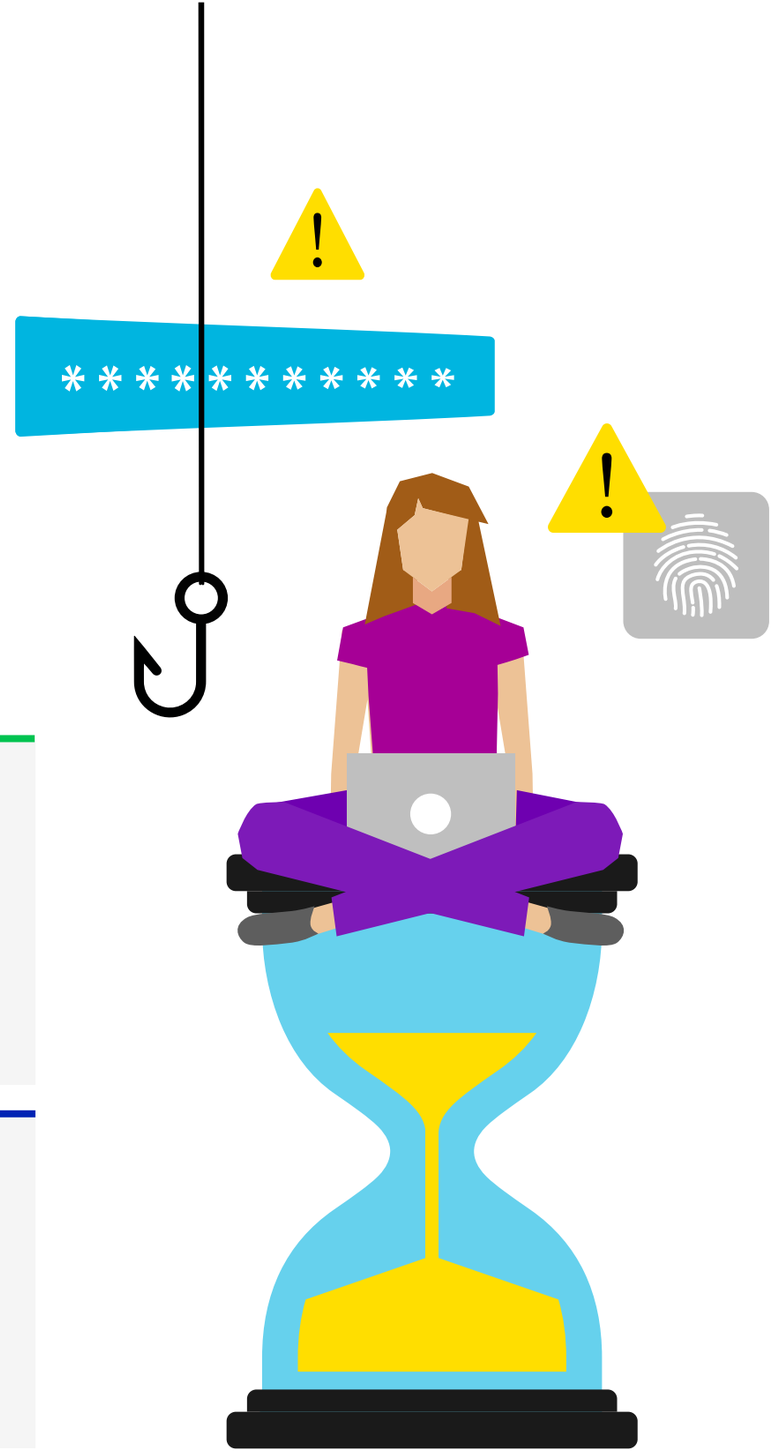
Knowledge is power when it comes to cyber security. It's important for small business owners to learn how they're likely to be attacked and to lessen the risk, and what to do and not do when it happens.

The Hiscox Cyber Readiness Report is based on a survey of 1,000 small businesses in the US and provides insight into the frequency of cyber attacks, how they can impact a business, and how to best prepare.

It’s not a case of if you’ll be attacked, but when

It’s more likely than not that a US company will suffer a cyber-attack. In fact, in the past 12 months, more than half (56%) of US small businesses experienced at least one cyber-attack and the average number of attack attempts per business was 2.38.

The costs of an attack are varied and significant.



Following a cyber attack:

31%
incurred costs to notify customers

28%
saw a reduction in business performance

25%
indicated the solvency or viability of their company was materially threatened.

29%
experienced bad publicity

26%
incurred substantial fines

Despite the frequency of attacks, 81% of the small businesses surveyed reported their cyber resilience has improved lately.

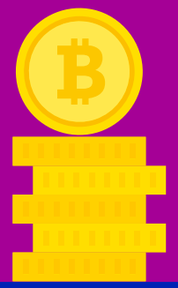
Does paying a ransom ever work?

A ransomware attack is a common and particularly unsettling cyber threat. During a ransomware attack, data is inaccessible until a ransom is paid. But there is no guarantee the data will be restored after payment, and it often isn't.

Of those businesses that paid a ransom, only

50%

recovered all of their data.



27%

sustained another attack.

To add insult to injury, ransomware victims paid a ransom an average of 2.24 times to recover.



The best defense: Helping employees keep devices safe

Keeping your devices safe and training your employees on best practices can go a long way to preventing a cyber incident.

The first point of entry for a threat actor is usually corporate-owned internet of things devices within company assets.

30%

followed by supply chains

28%

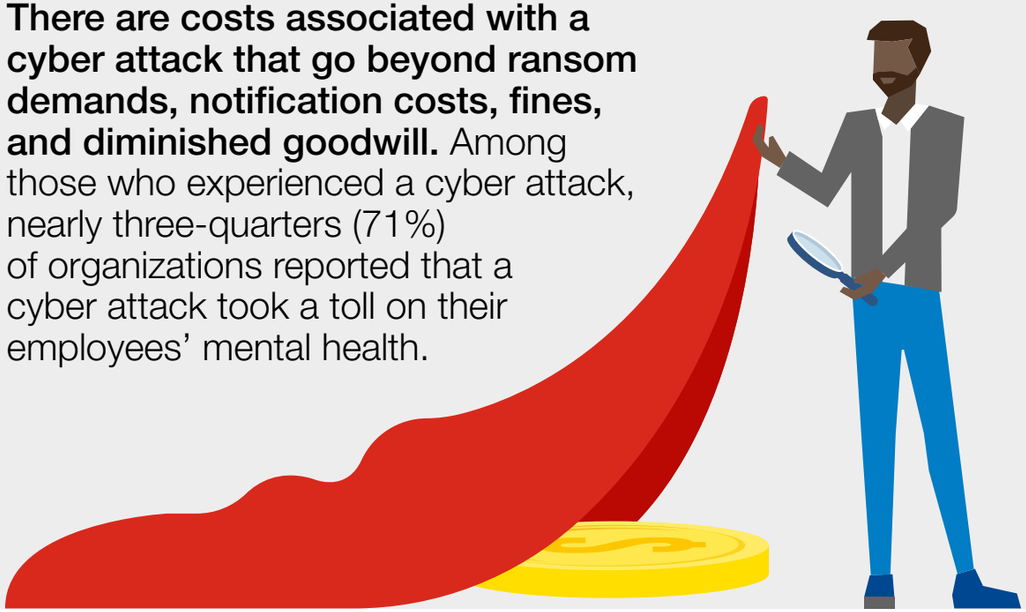
and employees

27%



The hidden costs of a cyber attack

There are costs associated with a cyber attack that go beyond ransom demands, notification costs, fines, and diminished goodwill. Among those who experienced a cyber attack, nearly three-quarters (71%) of organizations reported that a cyber attack took a toll on their employees' mental health.



42%
saw high stress among employees

35%
noted employee burnout

26%
saw increased employee sick days

25%
noticed a toxic work culture

Positive news

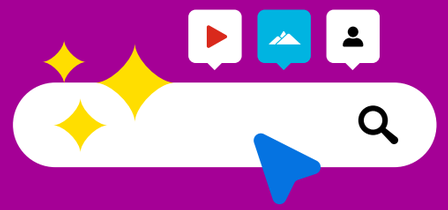
40%
reported that loyalty to the organization actually increased in the wake of an attack.

The impact of AI on cyber security

US small businesses that use AI reported an average of 1.63 AI-related cyber attacks in the past 12 months.

Despite this,

58%
of businesses report AI is more of an asset than a vulnerability when it comes to their cybersecurity.



Three ways to protect your business from cyber threats

Small businesses can take steps to reduce the likelihood they will be attacked, and to minimize the consequences if an attack happens. Here are some steps to consider.

1

Educate employees on preventing attacks by using strong passwords and multifactor authentication. Provide training on how to spot a suspicious email. Keep all software up to date.

2

Make sure your cyber security insurance is adequate. It can provide access to professional help in the event of a breach, plus coverage for costs associated with an attack.

3

Get professional advice as soon as an attack happens, especially before interacting with cyber criminals or paying a ransom.



Survey methodology

The Hiscox Cyber Readiness Survey was conducted by Wakefield Research among 5,750 professionals responsible for their company's cyber security strategy. This included subject matter experts (SMEs) and decision-makers (DMs), defined as being responsible for their organization's cybersecurity strategy, in the US, France, Germany, Spain, UK, Ireland and Portugal; respondents work at companies with fewer than 250 employees; the following titles qualify: Owner, Principal, Partner (Less than 50 employees) and CIO, CISO, Dir+ Security, Dir+ IT (50-249 Employees); between July 29th and August 8th, 2025, using an email invitation and an online survey.

Hiscox Cyber Readiness Report was first launched in 2016.

About Hiscox

Hiscox is a global specialist insurer, headquartered in Bermuda and listed on the London Stock Exchange (LSE:HSX). Through its retail businesses in the UK, Europe, and the US, Hiscox offers a range of specialist insurance for professionals and business customers as well as homeowners. In the US, Hiscox Small Business Insurance is underwritten by Hiscox Insurance Company Inc., a Chicago-based insurer that is licensed across the United States. For more information, please visit **www.hiscox.com.**

THIS COMMUNICATION IS FOR INFORMATIONAL PURPOSES ONLY.

The contents of this article and the linked materials do not offer legal, business or insurance advice related to the needs of any specific individual business. The insurance coverage described herein is subject to and governed by the terms and conditions of each policy that may be issued. The publication and delivery of this information is not intended to be a solicitation for the purchase of insurance on any US risk.

© 2026 Hiscox Inc. All rights reserved. Hiscox USA, 5 Concourse Parkway, 21st Floor, Atlanta, GA 30328 02/26

HISCOX | encourage courage®