

Acronis

WHITE PAPER

The ultimate cyber insurance coverage guide for MSPs

Imagine being a small or medium-sized business (SMB) applying for cyber insurance. The qualification process is daunting, with applications growing longer and audits becoming more thorough. Many businesses are turning to you to help them navigate their cyber insurance applications and ensure that they have adequate cybersecurity measures in place.

In fact, most businesses have qualms about forgoing cyber insurance, with 72% of small and medium-sized enterprises (SMEs) stating that a major cyberattack could destroy their business.



According to the U.S. Chamber of Commerce, 60% of small businesses say cybersecurity threats such as phishing, malware and ransomware are a top concern.[2] Yet, only two in five small businesses say they have established a formalized plan for future threats.[3] The demand for cyber insurance is high, but it's clear that SMBs are looking for guidance and need help knowing where to start.

What does cyber insurance cover?

The scope of coverage for liabilities and losses in cyber insurance policies varies depending on the insurance company's templates and their case-by-case risk assessment of each applicant or policyholder. Typically, most cyber insurance policies will cover loss of revenue due to business disruption, identity theft recovery assistance, data retrieval and recovery, compromised system restoral, incident-related legal fees and expenses associated with notifying regulators and law enforcement. In some cases, policies can even cover costs required to notify all individuals impacted and the recovery and restoral of identities and personal data.

That said, qualifying for a policy isn't as easy as it once was, and achieving adequate protection to maintain an existing policy is also becoming more difficult.

[1] National Association of Insurance Commissioners (NAIC). "NAIC Cyber Insurance Report." October 15, 2024. https://content.naic.org/sites/default/files/cmte-h-cyber-wg-2024-cyber-ins-report.pdf

[2] United States Chamber of Commerce. "Small Business Index Q1 2024." https://www.uschamber.com/sbindex/2024-Q1/quarterly-spotlight

[3] Ibid.

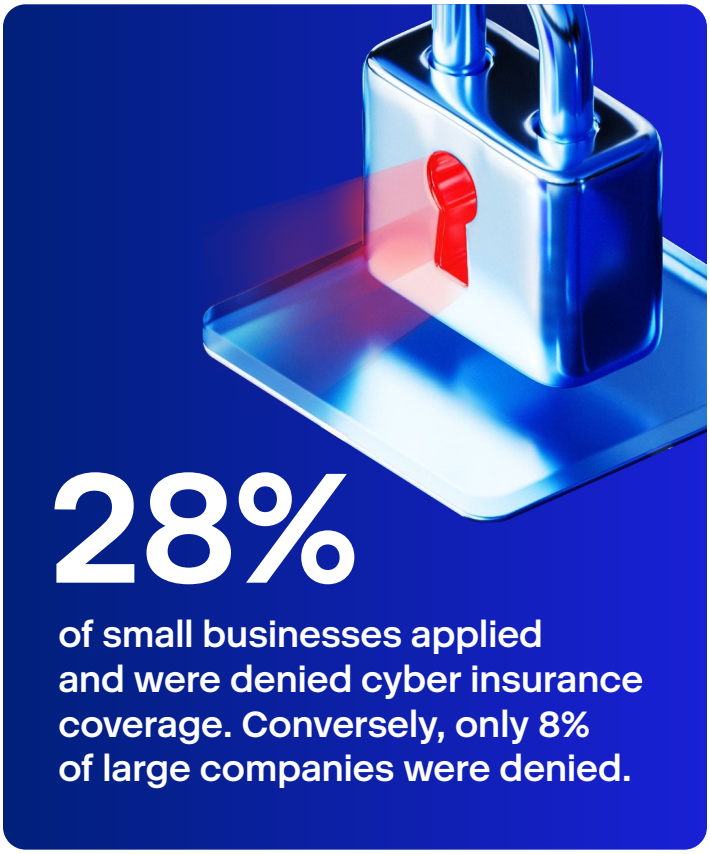
Copyright © 2002-2025 Acronis International GmbH.

Underwriters are raising the bar: Reasons behind cyber insurance application denials

It can be extremely frustrating for both you and your clients if their security measures are found to be inadequate in an insurance audit. Cyber insurance application denials often lead clients to leave and choose another, albeit cheaper, competitor MSP.

The reality is that denials are becoming more prevalent for resource-constrained applicants. Twenty-eight percent of small businesses that apply for cyber insurance coverage result in denial.[4] It's clear that these organizations are facing unique challenges that enterprises aren't.

The main culprit behind these denials: a lack of security protections and protocols in place.[5] Businesses aren't turning a blind eye to these security measures, which is a common misconception; but many are struggling to keep adequate protection in place, manage it and use it properly. Consequently, 37% of companies admit that their insurance coverage would be void if it were revealed that they lacked security controls.[6]





So, how do you prevent insurance application denials, loss of coverage and potential churn altogether? Evaluating and enhancing your clients' cybersecurity and data protection measures are practical places to start. You will not only help minimize clients' cyber risk, but also create long-term, strategic opportunities for your services in the future.

[4] Delinea. "Closing the Cyber Insurance Gap 2023 State of Cyber Insurance Report." https://delinea.com/resources/cyber-insurance-report-2023

[5] Ibid.

[6] Delinea. "Identity Security is Critical to Obtaining and Maintaining Cyber Insurance 2024 Cyber Insurance Research Report." https://delinea.com/resources/cyber-insurance-report-2024

Copyright © 2002-2025 Acronis International GmbH.

Profitable, scalable and sustainable growth: Why many MSPs consider cyber insurance in the long run

Although premiums are decreasing for enterprises that have prioritized boosting cybersecurity, the same can't be said for SMBs. According to the Cyber Readiness Institute, the average cost of cyber insurance for small and medium businesses has risen to between $500 and $5,000 per year.[7]

This price tag is influenced by several factors, including annual revenue, number of employees and types of security measures deployed such as antivirus, endpoint detection and response (EDR), extended detection and response (XDR), email security and security awareness training (SAT).

SMBs rely on your MSP business to provide effective protection, decode insurance applications and assist with obtaining or maintaining coverage. Fortunately, it's the ideal opportunity to build a trustworthy, scalable and sustainable partnership with businesses that will help them get coverage by filling critical security gaps and reducing their cyber risk.

Keep in mind that security measures that were once considered supplemental in the past are now commonplace today, and the trend will likely continue. Looking ahead, you will need to be a strategic partner to help ensure that your clients are equipped for the cyber insurance requirements of today and tomorrow.

In terms of cybersecurity, IT and security departments are seen as most responsible for protecting information. However, their perceived responsibility has dropped, with more responsibility attributed to the tech industry.[8]



What does this mean? The expectation of protecting the organization against cyberthreats and data breaches is shifting away from in-house IT departments to MSPs.

Your MSP business must now provide expanded protection to clients while also factoring in complexity and costs. Fortunately, it's the ideal opportunity to build profitable, scalable and sustainable service offerings that help clients fill their security gaps and reduce their cyber risk.

A balancing act: Advanced protection, security management and your client's cyber insurance rate

Market-leading advanced cybersecurity products such as endpoint detection and response (EDR) and extended detection and response (XDR) often require dedicated expertise to be effective, which is both expensive and labor intensive for most IT departments and service providers.

[7] Cyber Readiness Institute. "Cyber Insurance FAQs for Small and Medium Business." https://cyberreadinessinstitute.org/resources/cyber-insurance-faqs-for-small-and-medium-business/

[8] National Cybersecurity Alliance. "Oh Behave! The Annual Cybersecurity Attitudes and Behaviors Report 2024." September 24, 2024. https://www.staysafeonline.org/articles/oh-behave-the-annual-cybersecurity-attitudes-and-behaviors-report-2024

Copyright © 2002-2025 Acronis International GmbH.

50%

of U.S. companies are using AI-supported threat detection and monitoring to reduce their cyber insurance premiums.



Yet, these tools are critical to countering sophisticated cyberthreats — especially ransomware, advanced persistent threats (APTs), fileless malware and zero-day exploits. These advantages are another important reason cyber insurance auditors make advanced threat detection and response nonnegotiable requirements. As a matter of fact, 50% of U.S. companies say that having AI-supported threat detection and monitoring in place reduced their cyber insurance premiums.[9]

The question remains: How will your services drive advanced cybersecurity without adding complexity? The good news is that natively integrated cyber protection solutions empower MSP businesses to effectively manage and deliver advanced detection and response services to clients — without complicating management, burning out technicians or sacrificing margins. This enables you to develop a scalable service offering that helps your clients qualify and maintain their insurance policies while maintaining profitability.

Help your clients qualify for a policy and lower their premiums

As a service provider with clients who are seeking to qualify for cyber insurance, you must ensure that they do the following: establish and adhere to cybersecurity best practices, document policies and procedures and deploy advanced cybersecurity solutions aligned with these practices and policies. In any case, you need to understand what's required of you, document and record how you will fulfill these requirements, and ensure proper implementation.

As part of the application process, businesses will be required to complete a comprehensive questionnaire covering various aspects of cybersecurity, such as the measures in place, the value of covered data and business revenue. It is crucial to provide honest and transparent responses. Generally, the more comprehensive and well-documented cybersecurity measures, the lower the cost of the cyber insurance premium.

Upsell cybersecurity to help clients get coverage

As the standards for businesses get stricter, it's important for you to provide comprehensive protection to your clients without increasing complexity and expenses.

Acronis Cyber Protect Cloud is a solution designed for MSPs that eliminates the typical headaches that are accompanied by traditional integrations. This makes it easier to scale, offer and cross-sell and upsell protection based on individual client needs. Moreover, Acronis

[9] Delinea. "Identity Security is Critical to Obtaining and Maintaining Cyber Insurance 2024 Cyber Insurance Research Report." https://delinea.com/resources/cyber-insurance-report-2024.

Copyright © 2002-2025 Acronis International GmbH.

EDR, XDR and MDR are cost effective and accessible advanced detection and response solutions that are made for service providers looking to enhance their clients' protection across their most vulnerable attack surfaces and help them satisfy insurance requirements.

By consolidating cybersecurity, data protection and endpoint management into one solution with a single console, you not only improve IT efficiency, but also safeguard your profit margins. This means you can avoid paying for separate tools for backup, recovery, patch management, email security, endpoint protection and management, and the costs associated with hiring and training staff to manage these tools individually.

Leading cyber insurance discussions with your clients

It's critical for all businesses, including MSPs and their clients, to have complete insurance coverage. Cyber insurance is a primary part of any insurance and risk management plan. By gaining a clear understanding of insurance requirements, and the level of coverage that your client's policy will encompass, you can avoid confusion and better protect their businesses.

Explore how to help your clients qualify for insurance and adhere to compliance in our related content:

- The critical role of cyber insurance in safeguarding MSPs and their clients.
- The insurance and compliance game: How MSPs can win it.
- Why EDR is fundamental to qualifying to cyber insurance.

Acronis is a global cyber protection company that provides natively integrated cybersecurity, data protection, and endpoint management for managed service providers (MSPs), small and medium businesses (SMBs) and enterprise IT departments. Acronis solutions are highly efficient and designed to identify, prevent, detect, respond, remediate and recover from modern cyberthreats with minimal downtime, ensuring data integrity and business continuity. Acronis offers the most comprehensive security solution on the market for MSPs with its unique ability to meet the needs of diverse and distributed IT environments.

A Swiss company founded in Singapore in 2003, Acronis has 45 locations across the globe. Acronis Cyber Protect Cloud is available in 26 languages in 150 countries and is used by over 20,000 service providers to protect over 750,000 businesses.



Acronis

Learn more at
www.acronis.com

Copyright © 2002-2025 Acronis International GmbH. All rights reserved. Acronis and the Acronis logo are trademarks of Acronis International GmbH in the United States and/or other countries. All other trademarks or registered trademarks are the property of their respective owners. Technical changes and Differences from the illustrations are reserved; errors are excepted. 2025-02