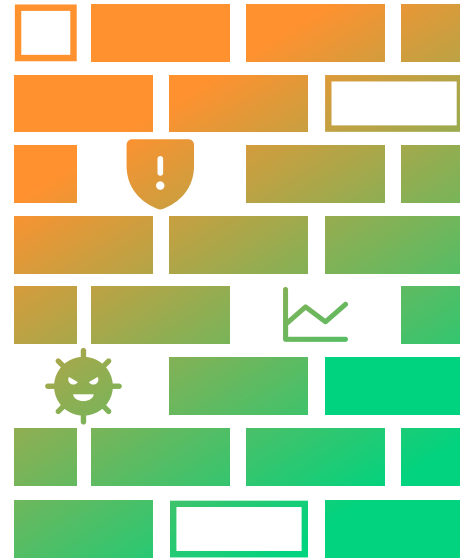


From threat to defense: Ransomware and cyber insurance

Ransomware plagues security professionals — and, in turn, the companies that insure them — more than ever before. It's now one of the most significant cybersecurity challenges, with 89% of enterprises identifying it as a top-five threat to their business. No longer limited to isolated incidents, ransomware has evolved into a booming global economy as attackers expand their capabilities and collaborate across networks.

[This was a key focus of discussion during a recent Keepit webinar](#), where Kim Larsen, CISO at Keepit, engaged a panel of cybersecurity and IT experts to discuss trends in ransomware and how they affect an organization's ability to secure cyber insurance today.



Actionable strategies to build resilience against the threat

1. Proactive defense

- Ensure active monitoring and conduct regular vulnerability assessments to identify and mitigate potential entry points.
- Focus on initial access points, as most breaches occur here.
- Deploy compartmentalization strategies to contain threats and prevent lateral movement within systems.

2. Comprehensive backup systems

- Store backups offsite and frequently check for corruption to maintain recovery readiness.
- Implement robust detection systems to identify compromises before restoration is necessary.
- Conduct regular restoration exercises, at least annually, to verify backup integrity.

3. Insurability controls

- Develop a cybersecurity maturity framework that includes multi-factor authentication (MFA), Endpoint Detection and Response (EDR), privileged access management, and employee awareness training.
- Test incident response plans and conduct tabletop exercises regularly to ensure operational resilience.

4. Resilience building

- Shift to a "we are being attacked" mindset. Resilience, not just defense, is essential to maintaining operations during and after an attack.
- Use established frameworks like NIST or ISO to create structured and measurable security policies.



Read more about how one of our customers recovered from a cyber attack

The role of cyber insurance to mitigate risk

Cyber insurance has become a cornerstone of risk management, providing financial protection against cyberattacks. It complements proactive initiatives like incident response planning and data recovery processes, acting as a safety net against increasingly sophisticated threats.

However, securing coverage is not straightforward. As threats evolve, so do insurer requirements. Insurers now demand evidence of cybersecurity maturity, often rejecting applicants without critical safeguards such as MFA, monitoring, or access controls. Policies also require proof of implementation rather than mere declarations of compliance, underscoring the need for demonstrable cybersecurity practices.

“You cannot get an insurance policy without controls. Insurance policies now overlap with cybersecurity maturity frameworks, demanding organizations strengthen their defenses.”

Dara Gibson, Senior Manager Cyber Insurability Services at Optiv

Here’s a look at the Top 10 cyber insurability controls



Identity and access controls

MFA, PAM, managed identity



Data privacy and governance

State/federal regulations, compliance, privacy-by-design



Business resilience

CRS, backup, TPRM



Logging and monitoring

SIEM, WAF, SOAR, email



Vulnerability management

VM programs, patch, management, remediation



Detection response

EDR, NDR, MDR, MXDR, threat hunting



Data security

Cloud, discovery, encryption, protection (DLP, CASB)



Incident response readiness

Plans, playbooks, tabletops



Cybersecurity awareness

Phishing, education



Network and OT security

SASE, architecture, management, protocols

Data recovery guide

Check out our 7-step guide for data recovery and business continuity

[Download now](#)



Keepit provides next-level SaaS data protection purpose-built for the cloud by securing data in a vendor-independent cloud to safeguard essential business applications, boost cyber resilience, and future-proof data protection.

For more information visit www.keepit.com or follow Keepit on [LinkedIn](#)

© 2024 Keepit. All rights reserved.