



Cyber Insurance Readiness Guide: The 5 Core Security Measures

pax8.com

Digital threats never rest.

Cybercriminals constantly innovate their attack strategies. As global regulators tighten security standards, businesses must adopt these five security features to protect data and meet key cyber insurance requirements.



Email Security



**Multi-Factor
Authentication (MFA)**



**Security
Awareness Training**



**Endpoint Detection and Response/
Managed Detection and Response
(EDR/MDR)**



Segregated Backups

Pax8 provides the solutions, support and expertise to strengthen your cloud experience and position your clients for success.

The Essential Cyber Insurance Security Measures

1. Email

Email is often a hacker's gateway to sensitive data. Strong email security protects against unauthorised access, phishing, spam and malware attacks. Additionally, encryption, spam filters and strong password policies protect sensitive information from lurking threats.

Solutions in the Pax8 Marketplace:

Check Point, IRONScales and Proofpoint provide the tools to secure email communication.

2. Multi-Factor Authentication (MFA)

MFA throws a serious wrench in hackers' plans. It adds a second layer of protection to user logins, like a code from your phone, on top of your username and password.

Even if hackers manage to steal your credentials, this step stops them in their tracks. MFA is one of the most effective ways to reduce cyber security risks.

Solutions in the Pax8 Marketplace: Find enhanced MFA options like Microsoft and Keeper for scalable, user-friendly setups.

3. Endpoint Detection and Response (EDR) and Managed Detection and Response (MDR)

EDR and MDR continuously monitor endpoints—laptops, desktops, mobile devices and servers—to identify and neutralise threats in real-time.

MSPs and their clients benefit from automated threat-hunting solutions or managed detection backed by a team of experts and analysts. These solutions detect malware, ransomware and even hidden threats, eliminating them before compromising your system.

Solutions in the Pax8 Marketplace: Get leading EDR and MDR solutions from CrowdStrike, SentinelOne and Blackpoint Cyber for premium client endpoint protection.

4. Security Awareness Training

Employees are the first line of defence. Security awareness training keeps them ahead of phishing scams and ransomware attacks. By prioritising end users' knowledge and expertise, they become the most powerful security asset.

Solutions in the Pax8 Marketplace: Discover impactful and engaging training programs like usecure.

5. Segregated Backups

A strong backup and recovery strategy is critical for restoring data and minimising downtime after a cyber attack. Segregated backups ensure data is securely stored offsite, preventing attackers from encrypting or deleting them.

Solutions in the Pax8 Marketplace: Access leading backup and recovery solutions, including Acronis, Dropsuite and Axcient (not currently available in APAC).

Benefits of Cyber Insurance Readiness

Implementing these five essential measures transforms your clients' cyber security and delivers Cyber Insurance Readiness, unlocking powerful benefits.

Reduced risk of cyber attacks:

These techniques expose cybercriminals, making your clients less vulnerable to costly disasters.

Improved regulatory compliance:

Strengthen compliance readiness while reducing audit and reporting challenges.

Competitive insurance rates:

Show insurers that you mean business. Strong security frequently leads to lower rates.

Increased client confidence:

Demonstrating your dedication to cyber security defines you as a reliable source to clients, leading to better business.

Cyber Insurance from a Global Perspective

Cyber insurance requirements vary from country to country, but one common theme remains: businesses that demonstrate strong security practices are better positioned to improve resilience, meet insurer expectations and manage cyber risk with confidence.

North America

In North America, cyber insurance is often viewed as a business risk management strategy. Businesses focus on reducing the financial impact of cyber incidents, including ransomware attacks, business interruptions and incident response costs.

Common areas of scrutiny include multi-factor authentication (MFA), endpoint detection and response (EDR/MDR), vulnerability management programs, backup, recovery testing and overall ransomware preparedness. Businesses that can demonstrate mature security practices are often better positioned when seeking coverage and navigating underwriting requirements.

For MSPs, this creates an opportunity to help clients strengthen their security posture, demonstrate measurable risk reduction and better protect operations and revenue.

Solutions in the Pax8 Marketplace: Available to North American partners, UKON simplifies cyber insurance for MSPs with automated pricing, real-time risk insights and carrier matching. Now in the Pax8 Marketplace, partners can deliver faster, smarter and tailored coverage to their clients.

Europe

Across Europe, cyber insurance is often tied closely to governance, risk management and regulatory compliance. Businesses must navigate evolving requirements such as GDPR, NIS2, DORA and other regional frameworks designed to improve cyber security accountability and operational resilience. Insurers commonly assess data protection capabilities, regulatory reporting processes, third-party risk management practices and business continuity planning. Because regulations can vary significantly between countries and industries, businesses must take a strategic approach to building security.

MSPs can take the opportunity to help clients strengthen resilience, protect sensitive data and support compliance obligations with clearly documented security practices.

APAC

Cyber insurance adoption continues to grow across Asia-Pacific as businesses focus on improving cyber risk awareness, implementing foundational security controls and demonstrating trust to clients, partners and stakeholders. Insurers frequently evaluate core cyber security capabilities, security governance practices and overall organisational readiness as they assess cyber risk. As businesses continue to modernise, strong security frameworks can help improve operational resilience, support growth initiatives and strengthen confidence across the broader ecosystem.

MSPs can take this opportunity to assist and guide clients to build trust, mature their security posture and demonstrate greater readiness to clients, partners and insurers.

Take Command of Your Security Action Plan

Better security does not ensure immunity from all cyber attacks, but it greatly reduces damage and increases resilience against threats. A proactive management plan and regular evaluations are essential for staying ahead.

Partner with Pax8 for Cyber Security Success

Pax8 is your trusted cyber security partner. Our Marketplace equips you with world-class expertise, technical support and an arsenal of tools to defend, innovate and grow your business.

Ready to take your cyber security to the next level? The path starts here.



We Make More Possible for Your Clients

[Schedule a call](#)