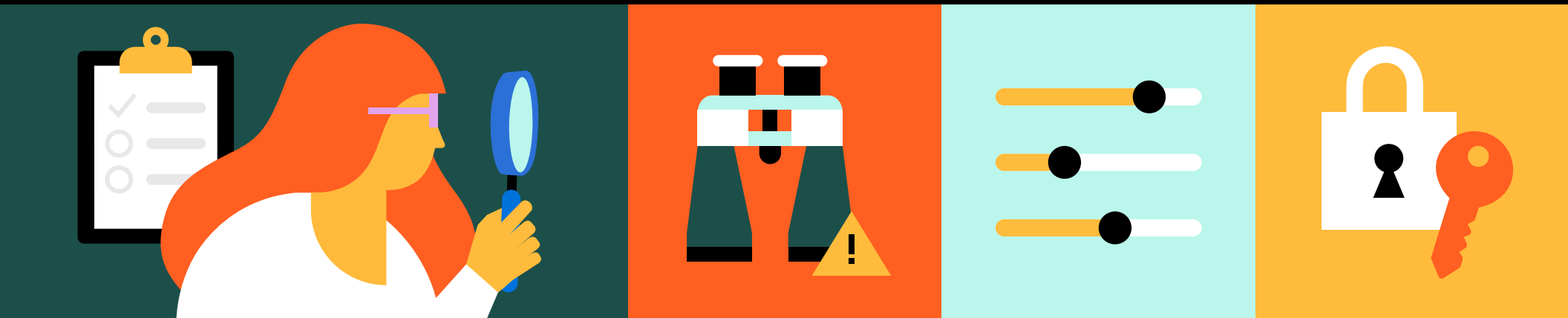
Coalition®

BOOST YOUR CYBERSECURITY IQ

14 Must-Know Security Controls for Insurance Brokers

A FIELD GUIDE FOR ADVISING CLIENTS ON CYBERSECURITY



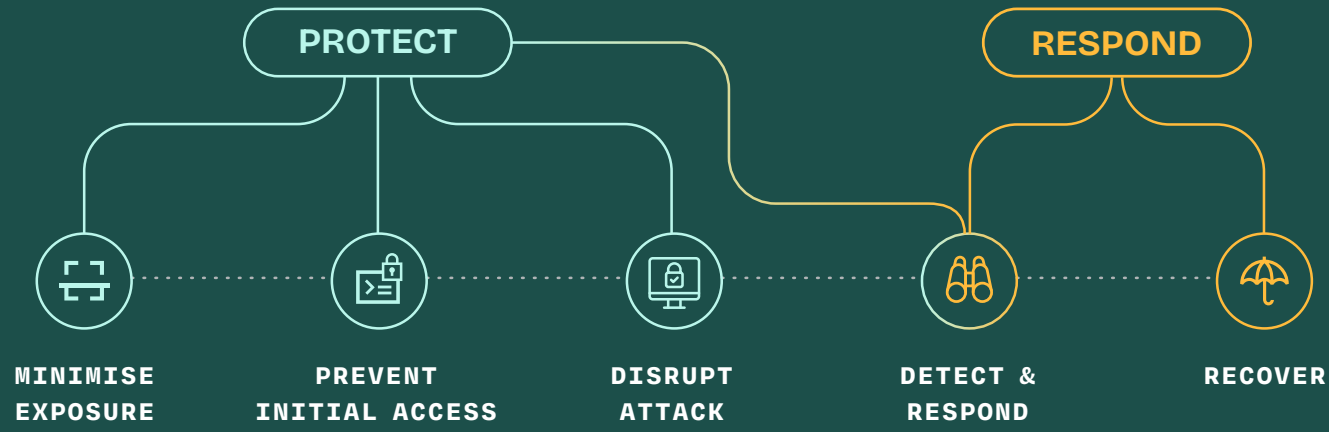
Using your field guide to advise like a pro

Cybersecurity is no longer a niche concern.

It's a core business risk. As demand for cyber insurance continues to grow, so does the expectation that brokers can speak confidently about how their clients' security postures should align with real-world threats. This field guide is designed to give you a clear, practical understanding of the security controls that are most relevant to cyber insurance.

Security controls are technology solutions or measures a business can put in place to help protect computer systems and networks, and sensitive data against cyber attacks. No single security control can prevent all cyber attacks. Effective cybersecurity strategies require a layered defense, often called **Defense in Depth**, in which each security control serves a specific purpose in preventing an attack.

Each security control in this guide has been carefully selected for its significance to coverage, claims impact, and client insurability. The security controls are organised based on how each control can contribute to your clients' Defense in Depth strategies:



Explaining technical cybersecurity concepts can sometimes push even the most experienced brokers outside of their comfort zone. Use this guide to skillfully navigate the intersection of cybersecurity and insurance so you can advise like a cybersecurity pro while staying true to your role as an insurance advisor.

REMEMBER

You don't need to be a cybersecurity expert. You just need to know enough to have a conversation.

	SECURITY CONTROL	WHAT IT IS	WHY IT MATTERS
Minimising Exposure	**Vulnerability Management**	A continuous process enabled by technology and human oversight that detects and analyses new vulnerabilities to help security teams prioritise and develop a remediation strategy for the exposures that pose the greatest risk to the organisation.	With 45,000 new software vulnerabilities expected in 2025[1], effective vulnerability management is essential for prioritising and addressing critical risks before cyber criminals can exploit them, reducing the likelihood of costly breaches and claims.
	Third-Party Risk Management	Technology and process used to evaluate the stability, security practices, and vulnerabilities of third parties that handle sensitive data, access network resources, or are responsible for business functions.	52% of all miscellaneous first-party claims were due to a third party breach.[2] Even when a business does everything right, external providers can expose an organisation to cyber risk.
Preventing Initial Access	**Multi-Factor Authentication (MFA)**	A security best practice that requires two or more forms of verification to access a system, application, or account. It's most often associated with email but should be applied to all vital technologies.	Many attacks starting with credential theft are carried out by criminals looking for easy targets. Implementing MFA — a solution accessible to most businesses — reduces risk by making the organisation less appealing to attackers.
	Single Sign-On (SSO)	Allows users to access multiple apps with one login, minimising password fatigue. Combined with MFA, it adds security while minimising extra login steps for users.	Nearly half (47%) of ransomware attacks begin with stolen credentials.[1] Using MFA and SSO adds security, reduces complexity, and helps reduce the most disruptive cyber insurance claims, like ransomware.
	Security Awareness Training	Scenario and simulation-based training designed to educate users about cyber risks — such as phishing, social engineering, and password security — and equip participants with practical skills to reduce the chance of human error.	Social engineering is the third-most common initial access vector in ransomware attacks.[2] Training employees on how to recognise social engineering can help minimise likelihood of a claim.
	Email Security	Technology solutions and policies designed to help prevent phishing attacks, filter malicious emails, block malware, and protect users data.	Email based attacks like business email compromise (BEC) and Funds Transfer Fraud (FTF) account for 60% of all cyber insurance claims.[2] Protecting email is essential for all organisations.

[1] Coalition 2025 Cyber Threat Index [2] Coalition 2025 Cyber Claims Report

	SECURITY CONTROL	WHAT IT IS	WHY IT MATTERS
Attack Disruption	**Network Segmentation**	An IT best practice that divides a network into separate zones to improve monitoring, control access, and limit the impact of cyber attacks by restricting attacker movement in the event of a breach.	Just as physical access is restricted to high-risk areas like the server room or roof, segmentation limits who can access specific parts of the digital network, protecting sensitive information and reducing company risk.
	Privileged Access Management (PAM)	An extra layer of security that protects admin accounts that have the highest access to a company's systems and data. By allowing only authorised users to reach your most valuable resources, these solutions help contain and limit attacks — even if a hacker gets in with stolen credentials.	If a hacker obtains an employee's password, PAM helps prevent privilege escalation and access to critical accounts, limiting the scope of the attack and likelihood of a costly claim.
	Financial Controls	Processes and procedures — such as verifying payments by phone, requiring dual approval for electronic transfers, and training employees on common scams — that help prevent threat actors from stealing money electronically and through social engineering.	FTF is when cyber criminals manipulate businesses into unknowingly sending money to fraudulent accounts controlled by cyber criminals. FTF was a leading cyber event type in 2024, accounting for nearly 30% of all claims.[2]
Detection & Response	**Endpoint Detection & Response (EDR)**	Technology that monitors endpoints — such as workstations, servers, laptops, and others connected to the network — to flag and stop malicious activity that makes it past traditional defenses like firewalls and anti-virus software.	If a sophisticated attacker tricks an employee into clicking a malicious link, uses stolen credentials, or exploits a known vulnerability, EDR technology can detect the suspicious activity and alert the company's IT or security team.
	Extended Detection & Response (XDR)	Enhances endpoint security by integrating detection and response across networks, servers, cloud, and email. This unified approach correlates data from multiple sources, making it easier to spot and stop complex attacks that siloed tools might miss.	As businesses shift to the cloud, security gaps can increase the risk of breaches or downtime. XDR protects sensitive data and applications across environments, helping prevent costly data privacy or business interruption claims.
	Managed Detection Response (MDR)	Helps achieve enterprise-level security capabilities, like 24/7 monitoring without hiring and managing an internal security team. Security experts fully manage the process and use advanced EDR technology to spot suspicious activity before it can cause harm.	When suspicious activity is detected, the MDR team quickly investigates and isolates affected assets to contain the threat. This rapid response reduces the likelihood and impact of claims by preventing attackers from accessing data, stealing information, or launching disruptive attacks like ransomware.

	SECURITY CONTROL	WHAT IT IS	WHY IT MATTERS
Recovery	**Incident Response Planning**	Incident response plans help businesses prepare for, manage, and recover from cyber incidents. These plans outline key roles, responsibilities, and action steps to minimise downtime and effectively address threats. They should be customised for each organisation, regularly updated, and reviewed by stakeholders to stay effective as the business evolves.	In 2025, IBM identified incident response planning as one of the top three investments businesses make after a breach.[3] Documented and tested incident response planning not only aligns with cyber insurance requirements, it can also improve response times and minimises the impact of claims.
	Backups & Data Recovery	The process of regularly backing up essential business data and implementing supporting technology to ensure the backups are immutable, inaccessible from the corporate network, and tested. This process helps minimise disruption by ensuring data can be recovered and restored after data loss and business interruption events.	The average business interruption loss in ransomware claims, over and above extortion payments, was £77,000 in 2024.[4] The ability to recover quickly from secure, tested backups can significantly reduce the severity of these types of claims.

KEY TAKEAWAY

By sharing insights derived from insurance claims data, it's easier to stay in your comfort zone and enhance your credibility as a trusted advisor. Use this field guide and other resources during discussions rather than relying on memory alone, and you'll be well-equipped to guide clients through their cybersecurity insurance decisions with confidence.

[3] IBM Cost of a Data Breach Report 2025 [4] Coalition 2025 Cyber Claims Report, figures converted from USD to GBP

Maximise Active Insurance with Coalition Security®

Coalition Security® complements cyber insurance at all phases of the policy term. Our products and services are informed by real-time risk and insurance insights from 100,000+ policyholders worldwide to help prioritise threats and remediation based on potential business impacts.[5]

Coalition Control®

Every Coalition policyholder receives access to Coalition Control®, where businesses can view their unique cyber risk profiles, monitor security alerts, access security support, and explore enhanced security services.

Security Awareness Training (SAT)

Educate employees on threat actor tactics, learn how to spot and avoid cyber attacks with phishing simulations, and meet compliance requirements.

Managed Detection & Response (MDR)

Prevent and mitigate attacks with 24/7/365 protection for computing assets and monitoring by seasoned cybersecurity experts. Businesses hat use a leading MDR solution, including Coalition Managed Detection & Response, can be eligible for a premium discount.[6]

Coalition Incident Response (CIR)

Respond to cyber attacks faster, recover with minimal business disruption, and receive hands-on support with incident response plans and tabletop exercises. In the event of an incident, Coalition policyholders that select CIR are eligible for a £0 retention for covered forensic investigation claim expenses.[7]

Have Questions or Need Additional Guidance?

Contact your Coalition Business Development representative, or our security experts for technical support:

- **Contingencies (pre-bind):** Schedule a call with a Coalition Security Engineer
- **Security Questions and Mid-Term Alerts:** Email us at securitysupport@coalitioninc.com
- **Coalition Security solutions pricing and demos:** Email your questions to securitysales@coalitioninc.com

[5]Security products and services are provided by Coalition Incident Response Inc. or its affiliates, including Coalition Incident Response UK Ltd., trading as Coalition Security. Coalition Security does not provide insurance products. Non-insurance products and services may be provided by independent third parties, and may require separate payment. [6]Premium discount eligibility (a reduction in the amount of premium paid on cyber insurance policies offered by Coalition Risk Solutions, Ltd.) is determined during the quote or renewal process and will depend on overall risk profile, applicable policy terms (which may include exclusions and limitations), and underwriting qualifications. Customers with MDR other than Coalition Security's MDR may be eligible for a premium discount. Contact MDRsales@coalitioninc.com for more information. [7] Incident response services are provided by Coalition Security and offered to Coalition policyholders as an option via Coalition's Panel Provider List. Subject to availability.

Coalition®

coalitioninc.com/en-gb

34-36 LIME STREET
LONDON, EC3M 7AT