CYBERGEN®

CYBER INSURANCE READINESS PACK

Preparing Your Business Before Applying for Cyber Insurance

CYBERGEN®

95% of cyber incidents now stem from human error
A single mistaken click can unleash a chain reaction. Cyber insurance cushions the fallout when people slip, because eventually, they do.

Purpose of This Pack

This readiness pack helps you:

- Understand insurer expectations
- Identify critical cybersecurity controls
- Document policies and processes before applying
- Strengthen your cyber risk posture (and potentially reduce premiums)

This toolkit is designed specifically for lean teams that lack dedicated security resources but still face strict insurance requirements. It provides a structured way to evaluate current protections, identify gaps, and implement the necessary controls, such as MFA, endpoint protection, and incident response planning.

With built-in checklists, policy templates, and a letter of readiness, it helps businesses not only meet insurer expectations but also improve their overall cyber resilience. Whether applying for new coverage or renewing, this pack ensures you're fully prepared and insurable.

Key Benefits of Preparation

- Faster approval process for insurance.
- Better negotiation position on policy terms.
- Reduced likelihood of claim disputes.
- Improved overall resilience against attacks.
- Common Cyber Risks for Businesses.
- Business email compromise (BEC).
- Ransomware, phishing, and credential theft.
- Data breaches and third-party vendor compromise.
- Insider threats and misconfigurations.
- Cloud and supply chain attacks.

CYBERGEN®

Cyberattacks now hit a business every 39 seconds
It's no longer "if" but "when." Insurance turns an almost-certain disruption into a recoverable event.

1. Introduction & Purpose

Why Cyber Insurance Alone Isn't Enough

Cyber insurance is a safety net, not a shield. Insurers increasingly require demonstrable security controls before approving coverage or paying claims. Many SMEs are denied coverage or face higher premiums due to poor cyber hygiene and insufficient documentation.

The Shared Responsibility Reality

Cybersecurity risk doesn't disappear once a policy is purchased—organisations must actively reduce exposure. Insurers now expect businesses to prove due diligence through evidence-based programs: employee training, vulnerability management, incident response planning, and continuous monitoring. Strong internal controls not only protect assets but also ensure that coverage remains valid when incidents occur.

Aligning Security Investments With Coverage Requirements

The most cost-effective approach is to integrate cyber insurance with a strategic cybersecurity program. This alignment reduces financial risk, improves insurability, and increases the likelihood of claims being honoured. Ultimately, the goal is resilience—protecting continuity, customer trust, and financial stability.

Quick Facts About Cyber Insurance

Cyber insurance premiums continue to rise, often due to increased ransomware activity and expanding regulatory penalties.

Many insurers now require MFA, endpoint protection, employee awareness training, and tested backups before issuing or renewing policies.

Policies frequently exclude outdated systems, unpatched vulnerabilities, and social engineering losses without explicit add-ons.

Coverage denials are increasing when companies fail to meet required controls or cannot prove compliance during an investigation.

CYBERGEN®

Average ransomware demands have jumped above £700,000, and recovery costs often climb far higher. Cyber insurance helps stop ransom notes from becoming financial sinkholes.

2. Technical & Policy Foundations

Baseline Cybersecurity Controls

- Endpoint Protection: Managed antivirus/EDR on all devices
- Firewalls & Network Segmentation: Properly configured and updated
- Multi-Factor Authentication (MFA): Enforced on email, VPN, and key systems
- Email Security: Anti-phishing filters and DMARC/SPF/DKIM setup
- Patching Policy: Critical systems updated within 30 days
- Access Control: Least-privilege model; regular access reviews
- Encryption: For sensitive data at rest and in transit

Identity & Access Management (IAM)

- Centralised IAM (e.g., Microsoft Entra ID/Azure AD)
- Regular password audits and MFA enforcement
- Disable dormant accounts promptly

Backup & Recovery

- Backups are encrypted and tested quarterly
- Offline and off-site copies are maintained
- Documented Recovery Time Objective (RTO) and Recovery Point Objective (RPO)

Vendor & Supply Chain Management

- Maintain a vendor risk register
- Review third-party security reports (Cyber Essentials Plus, ISO 27001)
- Include cybersecurity clauses in supplier contracts

60% of small businesses close within six months of a major cyber breach
It's brutal, but true. Cyber insurance helps a company survive long enough to fight back.

3. Governance, Compliance & Training

Insurers typically expect written and implemented policies for:

- Acceptable use
- Incident response
- Data protection & privacy
- Remote work and BYOD
- Password management
- Business continuity

Incident Response Plan (IRP)

A well-defined IRP should include:

- Incident classification levels
- Roles and responsibilities (including insurer notification timelines)
- Contact lists for internal teams and external partners (forensics, PR, legal)
- Communication templates for stakeholders

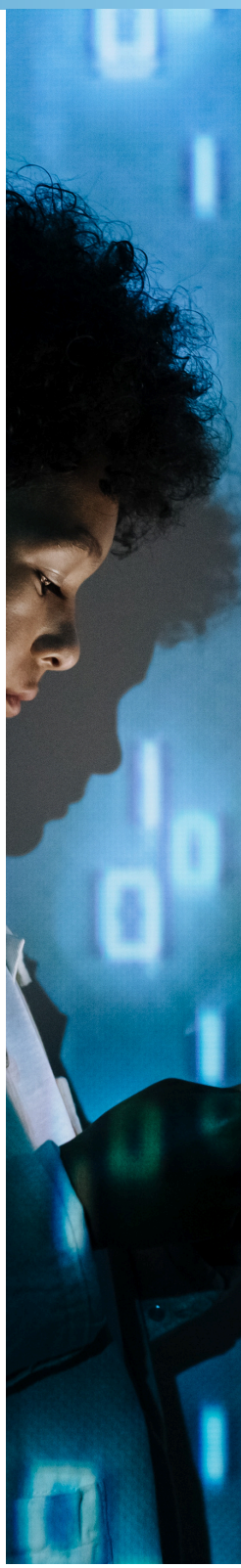
Security Awareness & Training (SAT)

- Mandatory annual training for all employees
- Phishing simulation exercises
- Role-based security education (e.g., IT admins, executives)

Regulatory & Compliance Readiness

Check alignment with applicable standards and regulations:

- SMEs: Cyber Essentials, ISO 27001:2022, GDPR, PCI DSS (if applicable)
- Enterprise: NCSC CAF, CIS Controls, DORA (for financial services)
- Maintain evidence of compliance (audits, reports, policy reviews).



Data breaches cost UK businesses an average of £4.5M
That includes downtime, legal costs, recovery teams, and lost customers, exactly the things cyber insurance is built to absorb.

4. Readiness Checklist & Next Steps

Complete this checklist before applying for cyber insurance.

Checklist			
Category	**Key Controls**	**Status (Y/N)**	**Notes**
Governance	Security policy in place		
Incident Response	Plan documented and tested		
Endpoint Protection	EDR/AV deployed on all devices		
MFA	Enforced on all accounts		
Backup & Recovery	Encrypted, tested quarterly		
Access Control	Least privilege, reviewed quarterly		
Vendor Management	Supplier risk assessments		
Employee Training	Phishing simulations completed		
Compliance	Audit or certification evidence		

CYBERGEN®

80% of businesses without cyber insurance pay out-of-pocket for attacks
And many never financially recover. With insurance, the burden shifts off the balance sheet and onto a specialist response team.

Proof of MFA, backup strategy, and incident response plan.

Record of the last penetration test or vulnerability assessment.

Evidence of data encryption and access control.

Board-level cybersecurity oversight.

Recommended Next Steps

1. Conduct a gap analysis using this checklist.
2. Address critical weaknesses (especially MFA, backups, IRP).
3. Gather evidence and documentation for insurer review.
4. Engage a cybersecurity partner to assist with compliance validation.
5. Proceed to the insurance application once all controls are verified.

Useful Resources

- NCSC Cyber Essentials: https://www.ncsc.gov.uk/cyberessentials/overview
- NIST Cybersecurity Framework: https://www.nist.gov/cyberframework

Securing your business today.

Get in touch with Cybergen to strengthen your cyber security, ensure you're compliance-ready, and stay ahead of evolving threats. Our expert-led security services, global partnerships, and tailored solutions help protect critical assets and meet regulatory demands with confidence. **Let's secure your future together. Reach out to start the conversation with us today.**

Cybergen Security
Hexagon House
Avenue 4
Station Lane
Witney
Oxfordshire
OX28 4BN

+44 (0) 1865 950 828

sales@cybergensecurity.co.uk

www.cybergensecurity.co.uk

Join Our Social Community

LinkedIn

CYBERGEN®