Clear Cyber Advisory

Cyber Insurance Readiness Guide

A practical guide for small and mid-sized businesses to reduce cyber risk, strengthen cybersecurity, organize supporting evidence, and prepare for cyber insurance applications and renewals.

ClearCyberAdvisory.com

OUTLINE

martin@clearcyberadvisory.com | (825) 419-7077

Request a Review

4 CYBERSECURITY RISKS FOR SMALL AND MID-SIZED BUSINESSES

Cybersecurity incidents can affect any business

Small and mid-sized businesses depend on email, cloud services, online banking, software platforms, mobile devices, suppliers, and technology providers every day. A single **compromised account, fraudulent payment, system outage, or data exposure can disrupt operations, cause financial loss, trigger legal and privacy obligations, and damage your reputation.**

Cybercriminals target businesses of all sizes. They often look for **weak passwords, missing security updates, limited employee training, unprotected remote access, or inadequate backup and recovery processes.**

Four common cybersecurity risks

1 **Business email compromise and payment fraud**

A criminal may impersonate an executive, employee, supplier, customer, or financial institution. The attacker may request an **urgent payment**, change banking information, redirect an invoice, or ask for confidential information. These requests can appear legitimate because criminals may copy email signatures, use similar domain names, or take control of a real email account.

Possible impact: stolen funds, exposed information, damaged supplier relationships, investigation costs, and difficulty recovering transferred money.

2 **Ransomware and business interruption**

Ransomware can encrypt files, disable computers, lock employees out of systems, or threaten to publish stolen information. Even when no ransom is paid, the business may face **days or weeks of disruption** while systems are investigated, restored, rebuilt, and secured.

Possible impact: lost revenue, delayed services, overtime costs, data restoration expenses, customer disruption, and reputational harm.

3 **Data and privacy breaches**

A data breach can occur through hacking, phishing, accidental sharing, lost devices, weak access controls, or employee error. The information involved may include customer records, employee information, financial details, health information, contracts, intellectual property, or confidential business documents.

Possible impact: privacy notifications, legal or professional advice, forensic investigation, regulatory concerns, customer complaints, and **loss of trust.**

martin@clearcyberadvisory.com | (825) 419-7077

Request a Review

4 Supplier and technology-provider incidents

Businesses rely on cloud platforms, software companies, payment processors, managed IT providers, file-storage services, and other third parties. An incident affecting one of these providers can interrupt your operations or expose information even when your own systems were not directly attacked.

Possible impact: downtime, unavailable data, delayed customer service, lost income, contractual issues, and limited control over the recovery process.

Cyber readiness does not require perfection

Small and mid-sized businesses do not need perfect cybersecurity or expensive enterprise systems. They need **practical, risk-appropriate safeguards, clear ownership, reliable backups, a tested incident response plan, and evidence that key controls are in place.** The goal is not to eliminate every cyber risk, but to **reduce preventable incidents** and be ready to **respond and recover** when something goes wrong.

10 PRACTICAL WAYS TO PROTECT YOUR BUSINESS

1. Enable multifactor authentication (MFA)

Require multifactor authentication for business email, cloud platforms, remote access, administrator accounts, financial systems, and other important services. MFA adds **another layer of protection** when a password is stolen or guessed.

2. Limit administrator access

Employees should not use administrator accounts for routine work. Provide elevated access only when it is required, create separate administrator accounts, and remove access promptly when an employee or contractor leaves.

3. Update and patch systems

Keep computers, mobile devices, servers, applications, browsers, network equipment, and security tools up to date. Prioritize updates for **internet-facing systems**, remote-access tools, and software that stores or processes sensitive information.

4. Protect email and devices

Use appropriate email filtering, endpoint protection, firewalls, **device encryption**, automatic screen locking, and centralized security settings. Business devices should be protected even when employees work remotely or travel.

5. Maintain and test backups

Back up important files, systems, and business information regularly. Keep at least one backup protected from alteration or deletion during an attack. **Test the restoration process** periodically to confirm that data can actually be recovered.

6. Independently verify payment requests

Confirm changes to banking information, unusual transfers, urgent payments, password resets, and requests for sensitive information through a **separate communication method**. Use a **trusted telephone number** already on file—not the number contained in the request.

7. Train employees

Employees should know how to **recognize phishing emails**, fake login pages, suspicious attachments, fraudulent invoices, impersonation attempts, and unusual requests. Provide a simple way to report concerns without fear of blame.

8. Maintain a technology and account inventory

Keep a current list of business devices, software, cloud services, user accounts, administrator accounts, remote-access tools, critical information, and important integrations. You cannot properly secure systems or accounts that the business has forgotten about.

9. Review important vendors

Identify providers that can access sensitive information or affect essential operations. Review their access, security responsibilities, support contacts, backup arrangements, incident notification process, and contract terms. **Remove access that is no longer needed.**

10. Prepare and test an incident response plan

Document who will make decisions, contact IT support, notify the broker or insurer, communicate with customers, and coordinate recovery. Include practical steps for ransomware, email compromise, payment fraud, data exposure, and system outages. Keep an offline or independently accessible copy and test the plan through a **short tabletop exercise.**

HOW TO PREPARE FOR YOUR CYBER INSURANCE QUESTIONNAIRE

Accurate answers matter

Cyber insurance questionnaires may ask about **cybersecurity controls** such as multifactor authentication, backups, security updates, employee training, endpoint protection, remote access, incident response, vendor management, and other safeguards.

A control may be:

* Fully implemented
* Partially implemented
* Applied only to certain accounts or systems
* Implemented but not documented
* Planned but not yet completed
* Enabled but never tested

Understanding these differences helps your business give **accurate answers, gather the right evidence, identify gaps, and avoid last-minute confusion during an insurance application or renewal.**

Organize supporting evidence

Evidence helps confirm that important controls are in place and makes future insurance applications, renewals, internal reviews, and broker discussions more efficient.

Security settings

* Screenshots showing MFA settings
* Administrator-account settings
* Remote-access security settings
* Email-security configurations
* Endpoint-protection or security-status reports
* Device-encryption settings

Technology and access records

* Current user-account list
* Administrator-account list
* Employee and contractor access records
* Device inventory
* Software and cloud-service inventory
* List of remote-access tools
* List of critical technology providers and vendors

Backup and recovery records

* Backup schedules and configuration
* Systems and information included in backups
* Location and protection of backup copies
* Results of restoration tests
* Recovery responsibilities and contact information

Policies and procedures

* Information-security policy
* Acceptable-use policy
* Password and access-control procedures
* Employee onboarding and offboarding process
* Incident response plan
* Business continuity or recovery plan
* Vendor-management procedures
* Approved AI-tool list and AI-use policy

Training and review records

* Cybersecurity awareness training records
* Phishing-test results, where applicable
* Policy acknowledgment records
* Access-review dates
* Incident response exercise records
* Dates when important controls were last reviewed or tested

Start Here

5 Essential Cybersecurity Protections

* Multifactor authentication
* Tested and protected backups
* Email and endpoint protection
* Employee cybersecurity awareness
* A documented incident response plan

martin@clearcyberadvisory.com | (825) 419-7077

Request a Review

6 STEPS TO CYBER INSURANCE READINESS

1 Review your controls

Confirm what protections are currently in place and where they are applied.

2 Identify gaps

Separate fully implemented controls from partial, undocumented, untested, or missing controls.

3 Prioritize improvements

Address the gaps most likely to contribute to fraud, account compromise, ransomware, data exposure, and prolonged business interruption.

4 Organize evidence

Save supporting screenshots, reports, policies, records, and test results in a secure and accessible location.

5 Complete the questionnaire

Provide accurate answers based on verified controls and available evidence. Ask your broker or insurer for clarification when a question is unclear.

6 Start before the renewal deadline

Cyber insurance readiness is more manageable when improvements are planned well before renewal. Starting early gives the business an opportunity to fix important gaps, test recovery processes, clarify responsibilities, and gather missing documentation.

Do not wait until renewal week to discover that an important control or document is missing. Insurance questions, requirements, policy terms, and coverage vary by insurer and organization.

martin@clearcyberadvisory.com | (825) 419-7077

Request a Review

5 WAYS CYBER INSURANCE CAN HELP YOUR BUSINESS

Cyber insurance can provide financial protection and rapid access to experienced professionals when a business faces a cyber incident. Coverage varies by insurer and policy, but may include:

1. Immediate Access to Cyber Experts

Forensic investigators, cybersecurity specialists, privacy lawyers, ransomware advisers, and business-recovery professionals may be available when they are needed most.

2. System and Data Recovery

Coverage may help pay for incident investigation, system repair, data restoration, and the safe resumption of normal operations.

3. Business Interruption Support

Cyber insurance may cover lost income and additional expenses when an incident prevents the business from operating normally.

4. Cybercrime and Fraud Protection

Depending on the policy, coverage may respond to ransomware, cyber extortion, funds-transfer fraud, and certain social-engineering losses.

5. Privacy, Legal, and Reputation Support

Coverage may assist with privacy notifications, legal advice, regulatory matters, public relations, and claims from affected customers or other parties.

Strong Coverage Starts With Readiness

Insurers may ask detailed questions about: **Multifactor authentication · Backups · Endpoint protection · Security updates · Employee training · Access controls · Incident response**

Clear, evidence-based answers support a smoother application or renewal and can reveal important gaps before they become urgent.

Prepare before the questionnaire arrives. Request a Cyber Insurance Readiness Review.

Coverage, exclusions, limits, deductibles, and security requirements vary by insurer and policy. Clear Cyber Advisory does not sell insurance or guarantee approval, pricing, coverage, or claim payment.

martin@clearcyberadvisory.com | (825) 419-7077

Request a Review

WHAT YOU RECEIVE AFTER THE REVIEW

Questionnaire Readiness

Review relevant insurer questions, identify missing or undocumented controls, and prepare clearer answers backed by evidence for applications and renewals.

Evidence Checklist

Organize MFA and access-control evidence, backup and recovery records, endpoint-protection information, security policies, procedures, and cybersecurity awareness training records.

Readiness Report and Action Plan

Receive a clear summary of critical and high-priority gaps, a broker-ready evidence package, and a prioritized action plan showing what to address first.

Our goal is to help your business **understand** its current readiness, **organize** the available evidence, and **focus on the improvements** that matter most.

Scan to request a readiness review

martin@clearcyberadvisory.com | (825) 419-7077

Request a Review

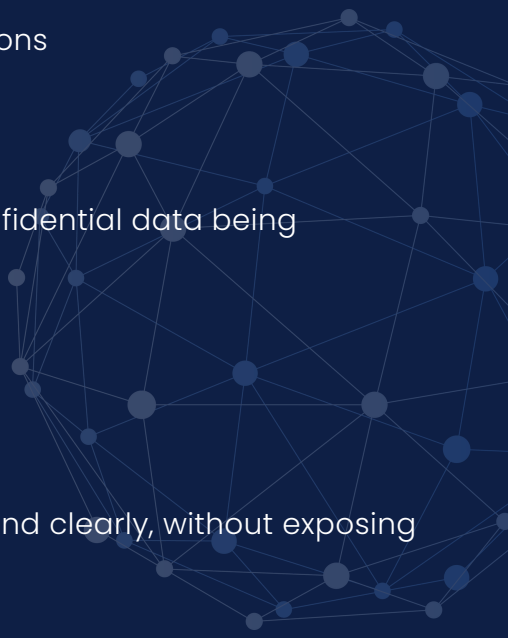
WHAT WE DO — CLEAR CYBER ADVISORY

About

Clear Cyber Advisory helps small and mid-sized businesses prepare for cyber insurance, reduce Shadow AI risk, and implement secure AI workflows through clear, practical action plans. We provide **cybersecurity readiness support** so your business can understand risks, move forward with confidence, and avoid unnecessary technical confusion. This is how we help:

1. Cyber Insurance Readiness – Be ready for cyber insurance questions and renewal conversations with insurers. What you get:

- Readiness review against common insurer expectations
- Gap list and practical action plan
- Cybersecurity evidence checklist



2. Shadow AI Risk – Identify AI tool use and reduce the chance of confidential data being exposed. What you get:

- Shadow AI discovery questions
- AI tool, vendor, and data exposure review
- Plain-English AI use policy

3. Safe AI Workflow Automation – Improve workflows with AI, safely and clearly, without exposing sensitive business data. What you get:

- Focused workflow map
- Cybersecurity checks and approvals
- Safer AI automation plan

We help businesses prepare for cyber insurance, reduce Shadow AI risk, and assist with safe AI workflow automation. You will know what to fix first, avoid surprises during insurance and client reviews, control risky Shadow AI use, and add or improve AI workflows safely.

Clarity. Focus. Confidence.
Scan to request a readiness review

This guide provides general information and does not constitute legal, insurance, or cybersecurity advice. Requirements and coverage vary by insurer and organization.

martin@clearcyberadvisory.com | (825) 419-7077

Request a Review