CYBER INSURANCE READINESS CHECKLIST



18 Critical Questions, Analysis & Action Items for Small Businesses

By Joseph Imperato Sr.
Founding Partner, XSolutions

Copyright: © 2026 XSolutions Consulting Services LLC

All Rights Reserved

DISCLAIMER

This guide is provided for informational purposes only and does not constitute legal, insurance, financial, or compliance advice. Cyber insurance policies vary by carrier, industry, state, coverage form, exclusions, endorsements, application answers, and claim facts.

Always review your policy with a qualified insurance broker, attorney, and cybersecurity professional before making coverage decisions.

XSolutions assumes no liability for actions taken based on this content.

Who Am I and Why Should You Listen to Me



From Finance to IT & Cybersecurity

My name is Joseph Imperato Sr. Before co-founding XSolutions in 1999, I spent decades in management and finance at a $3 billion Savings Bank and later a Fortune 500 company. During those years, I learned something critical: when data disappears, businesses lose everything.

My Cybersecurity Wake-Up Call

It was the late 1990s, and I was surfing the internet at home, when I received the following pop-up, "YOUR COMPUTER IS INFECTED! CALL THIS NUMBER NOW! “

Panicked, because I didn’t have any backups, I frantically ran anti-virus and anti-malware programs. For hours, my son (now my partner), and I went over every inch of that computer. Nothing. The verdict—scareware. A social engineering scam designed to trick me into giving criminals computer access.

That near-miss became my mission. I studied books, videos, and online courses, learning that hackers exploit human psychology, not just technology. Twenty-five years later, that moment still drives my passion. It taught me, preparation is everything. And, when all else fails, cyber insurance can save the day!

No matter the size, all businesses need cyber insurance. Data breaches, including Ransomware, can cause devastating downtime with hundreds of thousands of dollars in recovery fees, lost business, customer ill-will, and even regulatory fines. Cyber insurance can be the key to a company’s survival when all else fails.

Why This eBook Exists

Throughout my years in IT, I discovered that many businesses know they need cyber insurance, but treat the questionnaire as a “tick box,” selecting or inserting responses they think the insurance company wants to see, just to get coverage.

What they don’t realize is that when the time comes to file a claim, that same insurance provider will investigate and compare the responses on the questionnaire to what the company actually does in practice, asking for evidence of compliance. If satisfactory evidence cannot be produced, the claim will either be denied, or the payout greatly reduced. This can be financially devastating for a small business.

This guide will help you. Read on!

Table of Contents

Introduction 5

Section 1 — Governance & Policy 7

Section 2 — Backup & Recovery 8

Section 3 — Network & Access Security 9

Section 4 — Endpoint & Patch Management 10

Section 5 — Email & Security Awareness 11

Section 6 — Business Continuity & Vendor Management 11

Section 7 — Identity & Access Lifecycle Management 12

Quick Reference: Risk Priority Summary 14

A Final Word: Insurance Is the Safety Net, Your MSP Is the Foundation 15

About XSolutions 16

Why Work With Us? 17

Introduction

You Would Not Leave Your Front Door Unlocked. Why Leave Your Business Open to a Cyber Attack?

Imagine arriving at your office one morning to find every computer on the network frozen. A message on every screen demands a six-figure ransom in cryptocurrency before your files are released. Your customer database is locked. Your billing system is offline. Your emails are inaccessible. Every minute that passes, you lose revenue, burn staff hours, and watch your reputation erode as clients wait for work you cannot deliver.

This is not a hypothetical scenario reserved for large corporations. According to the Cybersecurity and Infrastructure Security Agency (CISA), small and medium-sized businesses now represent the majority of ransomware victims, precisely because they are perceived as having valuable data but weaker defenses. The average cost of a ransomware attack on a small business, including downtime, recovery, and reputational damage, can cost hundreds of thousands of dollars!

Cyber insurance exists to protect you from this kind of catastrophic financial loss. But here is what many business owners do not realize until it is too late: **insurance companies are not simply selling you a policy. They are evaluating whether your business has earned the right to be covered.** And increasingly, they are saying no, or attaching steep exclusions, to businesses that cannot demonstrate basic cybersecurity hygiene.

The Insurance Landscape Has Changed

Not long ago, obtaining cyber insurance was relatively straightforward. A business could answer a handful of general questions, pay a modest premium, and walk away with a policy. Those days are gone. The surge in ransomware attacks between 2020 and 2024 caused cyber insurance claim payouts to skyrocket, prompting insurers to overhaul their underwriting standards completely.

Today, cyber insurance applications ask detailed, technical questions about your organization's security controls. They want to know whether you use multi-factor authentication on every privileged account, whether your backups are stored in a location that Ransomware cannot reach, if your employees receive regular phishing awareness training, are your firewalls running current firmware, and whether you have an incident response plan ready to activate on the day disaster strikes.

If your answer to too many of those questions is "no" or, "I am not sure," you may be denied coverage, offered a policy with significant exclusions that gut the protection you thought you were buying, or charged premiums so high that the insurance becomes financially impractical. Worse, if you are granted coverage based on your responses, and the insurance company later finds that you are not performing those tasks as described, your insurance claim can be denied.

This Checklist Is Your Roadmap

The document you are holding was built directly from the questions that insurance underwriters actually ask. Every item in this checklist represents a control that insurers have identified as

critical to determining whether a business is an acceptable risk to cover. Think of it not as a bureaucratic form, but as a prioritized security improvement plan written in the language of the people who decide whether to protect your business.

For each of the 18 most important questions, this guide tells you three things: **why the question matters** from a risk and insurance perspective, **what an acceptable answer looks like,** so you know the standard you are working toward, and **what concrete action to take** if your current answer is "no." It is designed to be used in two ways: as a pre-application gap assessment before you apply for coverage, and as an ongoing compliance tool to maintain your insurability year after year as your business grows.

The Stakes Have Never Been Higher for Small Businesses

Cybercriminals have become highly sophisticated at identifying and targeting vulnerable organizations. Automated scanning tools continuously probe the internet for businesses running outdated software, exposed remote access ports, or weak authentication. Small businesses are specifically targeted because attackers know that a company with 20 employees is far less likely to have dedicated security staff watching threats around the clock.

The checklist items that follow are not theoretical best practices developed in a laboratory. They are the hard lessons learned from thousands of actual breach investigations, distilled into the controls that consistently make the difference between a business that recovers quickly and one that does not recover at all. Multi-factor authentication, immutable backups, endpoint detection, patch management, and employee training are not expensive luxuries. They are the minimum viable defenses for any business that stores customer data, processes payments, or depends on digital systems to operate.

How to Use This Guide

Work through each section honestly. For every question where your current answer is "yes," document the specific tool, policy, or process that supports that answer, because when your insurer asks for evidence, you will need to provide it. For every question where your answer is "no" or "partially," treat the corresponding action item as a project with a deadline, not a note to revisit someday.

Prioritize the items marked Critical first. These represent the controls that insurers most frequently cited as reasons for denial or exclusion. Addressing them will have the greatest immediate impact on your insurability and, more importantly, on your actual security posture.

Bring this document to your IT provider or internal IT team and use it as the basis for a security roadmap. The language in this guide mirrors exactly what your insurance broker and underwriter will expect to see, which means that closing the gaps identified here is the most direct path to securing the coverage your business needs.

Cyber insurance is not the finish line. It is the safety net below the tightrope. This checklist is how you learn to walk the rope. Start today.

18 Critical Questions, Analysis, & Action Item Guide

The Critical Questions You Need To Answer

Find What You Need To Do BEFORE Requesting Cyber Insurance

This document analyzes the 18 most critical questions from a typical cyber insurance application questionnaire. For each question, it provides the rationale for why insurers consider it important, an example of an acceptable response, and the action items required if the organization answers 'No.' Organizations should use this guide to prepare accurate responses and address any gaps before submission.

Why It Matters	Acceptable Response	Action Item if 'No'

SECTION 1 — GOVERNANCE & POLICY

Q1 Does your organization have a Cyber/Information Security Program that includes an Incident Response Plan specifically addressing Ransomware?

Why It Matters	Acceptable Response	Action Item if 'No'
Ransomware is the leading cause of cyber insurance claims. Organizations without a documented IR plan experience longer downtime, higher remediation costs, and a greater likelihood of paying the ransom. Insurers treat this as a foundational control and will frequently deny coverage without it.	Yes, we maintain a formal, documented Incident Response Plan reviewed and updated at least annually. The plan includes ransomware-specific playbooks with defined roles, escalation paths, and communication procedures.	Engage a cybersecurity consultant or MSP to develop a formal IR plan with ransomware-specific playbooks. Establish a target completion date within 60–90 days and document interim compensating controls. Notify your insurer of the remediation timeline.

Q2 Do you use Multi-Factor Authentication (MFA) for all cloud provider services (AWS, Azure, Google Cloud)?

Why It Matters	Acceptable Response	Action Item if 'No'
Compromised cloud credentials are a primary attack vector. Without MFA, a single stolen password grants full access to cloud infrastructure. Insurers frequently exclude or restrict coverage when MFA is absent from cloud services.	Yes, MFA is enforced for all cloud provider consoles and APIs via hardware tokens or authenticator apps. No admin or service accounts are exempt without documented compensating controls.	Enable MFA immediately for all cloud admin and user accounts. Prioritize root/global admin accounts. Document any service accounts that cannot use MFA and implement IP allowlisting as a compensating control. Report progress to insurer within 30 days.

Q3 Do you require Multi-Factor Authentication (MFA) for all privileged account access?

Why It Matters	Acceptable Response	Action Item if 'No'
Privileged accounts are the primary target in ransomware attacks. MFA on privileged accounts is considered a minimum baseline by most cyber insurers and is frequently a hard coverage prerequisite.	Yes, MFA is mandatory for all accounts with administrative privileges, enforced via a conditional access policy or other solution. Shared or generic admin accounts have been eliminated.	Audit all privileged accounts immediately. Enable MFA for all admin accounts. Eliminate shared credentials. Implement an identity and access Management (IAM) solution and document a remediation plan with a timeline.

SECTION 2 — BACKUP & RECOVERY

Q4 Are your backups disconnected from and inaccessible through your network (air-gapped), immutable, and protected with credentials unique from all other systems?

Why It Matters	Acceptable Response	Action Item if 'No'
Modern Ransomware specifically targets backup systems. Air-gapped or immutable backups are the single most important recovery control. Without them, attackers encrypt backups alongside production data, making recovery impossible without paying.	Yes, backups are stored offsite in an immutable format (object lock enabled). Backup credentials are unique, stored separately from Active Directory, and no production accounts can access backup systems. Restoration is tested quarterly.	Implement an offsite, immutable backup solution. Rotate backup credentials to be completely separate from network credentials. Schedule a backup restoration test within 30 days and document the results.

Q5 Does your backup platform require MFA, encrypt data at rest, and maintain an offsite secondary backup inaccessible from the company network?

Why It Matters	Acceptable Response	Action Item if 'No'
Backup platforms accessible from the main network are routinely encrypted during ransomware attacks, rendering recovery options unavailable. Insurers treat backup security as a direct indicator of the potential recoverable loss.	Yes, our backup platform requires MFA for all admin and user access, encrypts all data at rest with AES-256, and replicates to a geographically separate offsite location with immutability enabled. Restoration is tested monthly.	Enable MFA on the backup management console. Enable AES-256 encryption for all backup data at rest and in transit. Establish an offsite, immutable secondary copy. Document and test the restoration process and submit compliance screenshots to the insurer.

SECTION 3 — NETWORK & ACCESS SECURITY

Q6 Is your network segmented to separate critical systems, servers, and sensitive data from general user workstations, guest access, and IoT devices, limiting an attacker's ability to move laterally?

Why It Matters

Most small-business networks are "flat," every device can reach every other device. Once an attacker gains a foothold on one workstation, a flat network lets ransomware spread unchecked within minutes. Segmentation contains a breach to a single zone, dramatically reducing the blast radius and the size of the resulting claim. Insurers increasingly treat segmentation as a core control for limiting loss severity, particularly for organizations that store sensitive client or financial data.

Acceptable Response

Yes, our network is logically segmented using VLANs and firewall rules that separate servers, user workstations, guest Wi-Fi, backup infrastructure, and IoT/operational devices. Inter-segment traffic is denied by default and permitted only where required, sensitive data resides in its own protected segment, and cross-segment access is logged and monitored.

Action Item if 'No'

Map your current network and identify critical assets (servers, backups, and systems holding PII or financial data). Implement VLANs to separate these from general workstations, guest access, and IoT devices. Configure firewall rules to deny inter-segment traffic by default and allow only necessary connections. Isolate backup systems on their own segment and place any legacy/EOL devices in a restricted zone. Document the segmentation design for your insurer.

Q7 Do you have End-of-Life (EOL) or unsupported operating systems within your network?

Why It Matters

EOL systems no longer receive security patches, leaving permanent vulnerabilities. Attackers frequently target them and may trigger coverage exclusions or premium surcharges if undisclosed to the insurer.

Acceptable Response

No, all systems run supported, vendor-maintained operating systems. Any legacy systems have an approved replacement project with a defined and documented timeline.

Action Item if 'No'

Conduct an immediate OS inventory. For any EOL systems: isolate them in a network segment with no internet access, document a replacement timeline, implement enhanced monitoring, and disclose to the insurer with a formal remediation plan.

Q8 If remote access (SSL VPN, RDP, etc.) is allowed, do you require MFA for all users, and is direct RDP blocked from the internet?

Why It Matters

RDP exposed to the internet without MFA is the single most exploited initial-access vector in ransomware incidents. Even VPN with username/password only is considered high risk. MFA on remote access is a near-universal insurer requirement.

Acceptable Response

Yes, all remote access is gated by MFA (Microsoft Authenticator, Duo, or equivalent). RDP is not exposed directly to the internet; it is accessible only through the VPN gateway. External RDP is firewall blocked.

Action Item if 'No'

Immediately disable any direct internet-exposed RDP. Implement MFA on all VPN and remote access solutions. If technically constrained, implement network-level authentication and IP allowlisting as interim controls. Disable remote access for accounts that do not require it.

Q9 Are you operating with a current firmware Firewall/IPS, and is an automated monitoring system or SIEM in use for real-time alerts on configuration changes?

Why It Matters	Acceptable Response	Action Item if 'No'
Perimeter security is the first line of defense against external threats. Outdated firmware contains exploitable vulnerabilities. Without SIEM integration, configuration changes or bypass attempts may go undetected for days or weeks.	Yes, we operate a next-generation firewall/IPS with the latest firmware. All configuration changes trigger real-time SIEM alerts. Firewall rules are reviewed quarterly and documented in a change management log.	Update all firewall/IPS firmware to the latest vendor-supported version immediately. Enable logging integrating with a SIEM for real-time alerting. Conduct a firewall rule review and remove unused or overly permissive rules. Submit a screenshot of the firmware to the insurer.

SECTION 4 — ENDPOINT & PATCH MANAGEMENT

Q10 Do you use an Advanced Endpoint Detection and Response (EDR) solution on all servers and workstations?

Why It Matters	Acceptable Response	Action Item if 'No'
Traditional antivirus cannot detect modern fileless malware and living-off-the-land attacks used in ransomware campaigns. EDR provides behavioral detection, which is essential for identifying attacks before they spread.	Yes, we use an enterprise-grade EDR, **[NAME THE SOLUTION]**, on 100% of servers and endpoints, with active threat hunting and 24x7 alerting.	Deploy an enterprise-grade EDR solution immediately. Conduct an asset inventory to identify any unprotected devices. Establish a process to verify EDR coverage for all new devices at the onboarding stage. Provide the insurer with a dashboard screenshot showing coverage percentage.

Q11 Does the company have a formalized patch management program that applies critical security patches to all servers and endpoints within 48 hours of release?

Why It Matters	Acceptable Response	Action Item if 'No'
Unpatched vulnerabilities are a leading initial-access vector. Many large ransomware outbreaks exploit known, patchable vulnerabilities. A 48-hour SLA for critical patches is the industry benchmark insurers use to evaluate risk.	Yes, we use an automated patch management solution to deploy critical patches within 48 hours for servers and 7 days for endpoints. Patch compliance is tracked via a dashboard and reviewed weekly by IT leadership.	Implement an automated patch management solution. Define patch SLAs by severity (Critical: 48 hours, High: 7 days, Medium: 30 days). Generate a current compliance report and immediately remediate all Critical and High-priority outstanding patches. Document exceptions.

SECTION 5 — EMAIL & SECURITY AWARENESS

Q12 Do you enforce SPF, DKIM, and DMARC on all domains, and are external emails tagged to alert employees they originated outside the organization?

Why It Matters

Business Email Compromise (BEC) and phishing are responsible for the majority of initial access events. SPF/DKIM/DMARC prevents domain spoofing. External email tagging prompts employees to scrutinize unexpected messages.

Acceptable Response

Yes, SPF and DKIM are enforced with DMARC set to 'reject' or 'quarantine' policy. All inbound external emails display a visible banner that warns employees that the email originated outside the organization.

Action Item if 'No'

Implement SPF, DKIM, and DMARC records for all domains. Set DMARC initially to 'monitor' mode, then progress to 'quarantine' and then 'reject' within 90 days. Enable external email tagging in Microsoft 365 or your email gateway.

Q13 Do all employees receive cybersecurity awareness training covering phishing and Business Email Compromise (BEC), using a commercially purchased program?

Why It Matters

Humans remain the most exploited attack surface. Recurring training with simulated phishing exercises reduces click rates on malicious emails. Insurers look for evidence of a recurring commercial program, not a one-time orientation.

Acceptable Response

Yes, all employees complete training on a commercial security awareness platform, **[NAME YOUR SECURITY AWARENESS TRAINING SOLUTION]**, on a quarterly basis, including simulated phishing campaigns. Completion is tracked, and non-completers are escalated within 72 hours.

Action Item if 'No'

Enroll the organization in a commercially available security awareness platform and schedule initial training for all employees within 30 days. Run a baseline simulated phishing campaign. Establish at least a quarterly cadence (monthly is better), and document completion of metrics. Upload the most recent training report to the insurer.

SECTION 6 — BUSINESS CONTINUITY & VENDOR MANAGEMENT

Q14 Does the company have a formal, documented Business Continuity Plan (BCP) that addresses cyber threats and is updated and tested at least annually?

Why It Matters

A BCP ensures the organization can sustain critical operations during a cyber incident. Without a tested BCP, organizations experience significantly longer recovery times and greater reputational damage. Insurers use BCP maturity to assess residual risk.

Acceptable Response

Yes, our BCP is formally documented, reviewed annually by leadership, and tested via tabletop exercise each year. The plan includes Ransomware, data breach, and cloud outage scenarios with defined RTOs and RPOs.

Action Item if 'No'

Engage your Managed Services Provider (MSP) to develop a formal BCP. Define RTOs and RPOs for all critical systems. Schedule a tabletop exercise within 90 days. Share the remediation timeline with the insurer.

Q15 Are third-party vendors that connect to your networks required to use MFA and unique login IDs, and is vendor access reviewed at least quarterly?

Why It Matters	Acceptable Response	Action Item if 'No'
Supply chain attacks demonstrate that vendor access is a major risk vector. Without MFA and unique vendor IDs, a compromise at one third party can cascade into your environment. Insurers scrutinize third-party access controls heavily.	Yes, all third-party vendors are required by contract to use MFA and unique, individual login credentials. Vendor access is reviewed quarterly and revoked immediately upon contract termination.	Audit all active third-party connections. Require MFA for all vendor accounts immediately. Eliminate shared or generic vendor credentials. Implement a quarterly vendor access review process. Document findings and remediation timelines for the insurer.

SECTION 7 — IDENTITY & ACCESS LIFECYCLE MANAGEMENT

Q16 Does your organization have a formal process for immediately removing access, to both internal systems and cloud services, when an employee is separated, and are dormant accounts reviewed at least quarterly?

Why It Matters	Acceptable Response	Action Item if 'No'
Inactive and orphaned accounts are a critical but frequently overlooked attack vector. Former employees, contractors, or service accounts that retain valid credentials provide attackers (and disgruntled ex-staff) with legitimate-looking access that bypasses most security controls. Insurers view poor offboarding as a direct indicator of access-control immaturity.	Yes, we have a documented offboarding checklist that triggers immediate deactivation of all accounts (Active Directory, email, SaaS applications, VPN, and cloud consoles) on the day of separation. A quarterly audit identifies and removes any dormant accounts.	Create a formal, documented offboarding procedure and assign ownership to HR and IT, or appropriate management. Implement an account deactivation workflow. Conduct an immediate audit of all Active Directory accounts and deactivate any that has not been used in 90+ days. Schedule quarterly reviews for the future.

Q17 Does your organization enforce the principle of least privilege, ensuring users have access only to the systems and data required for their specific role?

Why It Matters	Acceptable Response	Action Item if 'No'
Overprivileged accounts dramatically amplify the blast radius of a compromise. When a single user account can access all file shares, all cloud storage, and all applications, one successful phishing email can encrypt the entire organization. Least-privilege access limits damage and is a key underwriting factor.	Yes, user access rights are defined by role and reviewed at least annually (or upon role change). No standard user accounts have administrative rights. Access to sensitive data (payroll, customer PII, financial records) is restricted to roles that require it.	Conduct an access rights audit across all systems. Remove administrative rights from standard user accounts. Implement role-based access controls (RBAC) in Active Directory and all major SaaS applications. Establish a process requiring manager approval and IT review for any access to elevation requests.

Q18 Are controls in place to provide real-time notification of Active Directory or identity changes, such as new accounts created, privilege escalation, and bulk failed logon attempts?

Why It Matters	Acceptable Response	Action Item if 'No'
Attackers often create rogue admin accounts or escalate privileges hours or days before deploying Ransomware. Real-time identity monitoring is the primary early-warning mechanism for detecting an in-progress attack before widespread damage occurs.	Yes, we use a SIEM or AD monitoring solution**, [NAME YOUR SOLUTION]**, with alerts configured for new account creation, privilege changes, and multiple failed logon attempts. Alerts are routed to a monitored mailbox and to a SOC 24x7.	Implement a SIEM or dedicated AD monitoring solution. Configure real-time alerts for: new admin account creation, privilege escalation, 5+ failed logon attempts, and new GPO changes. Ensure alerts route to a monitored endpoint at all hours. Document the tool's and the insurer's alert thresholds.

QUICK REFERENCE: RISK PRIORITY SUMMARY

#	Question Topic	Category	Insurer Priority
1	Incident Response / Ransomware Plan	Governance	🔴 Critical
2	MFA on Cloud Services	Governance	🔴 Critical
3	MFA on Privileged Accounts	Governance	🔴 Critical
4	Air-gapped / Immutable Backups	Backup & Recovery	🔴 Critical
5	Backup Platform MFA, Encryption, Offsite	Backup & Recovery	🔴 Critical
6	Network Segmentation	Network Security	🟠 High
7	No EOL / Unsupported Operating Systems	Network Security	🔴 Critical
8	MFA on Remote Access / No Exposed RDP	Network Security	🔴 Critical
9	Current Firewall Firmware + SIEM	Network Security	🟠 High
10	EDR on All Endpoints & Servers	Endpoint Security	🔴 Critical
11	48-Hour Critical Patch SLA	Patch Management	🟠 High
12	SPF / DKIM / DMARC / Email Tagging	Email Security	🟠 High
13	Security Awareness Training	Email Security	🟠 High
14	Tested Business Continuity Plan	Business Continuity	🟡 Medium
15	Third-Party Vendor MFA & Unique Credentials	Vendor Management	🟠 High
16	Employee Offboarding & Dormant Account Review	Identity & Access	🔴 Critical
17	Least Privilege / Role-Based Access Controls	Identity & Access	🔴 Critical
18	Real-Time Identity Change Monitoring	Identity & Access	🟠 High

A Final Word: Insurance Is the Safety Net, Your MSP Is the Foundation

Cyber insurance is no longer a luxury or an afterthought. it is a core component of modern business survival. A single ransomware attack, data breach, or business email compromise can generate costs that climb well into six figures once you account for downtime, data recovery, legal fees, regulatory fines, customer notification, and lasting reputational damage.

For most small and mid-sized businesses, an uninsured incident of that magnitude is not a setback; it is a business-ending event. The right policy transfers that catastrophic financial risk off your balance sheet and gives you access to the incident-response specialists, forensic investigators, and legal counsel you will need in the worst moment of your business life. But as this guide has made clear, coverage is earned, not simply purchased, and a policy is only as dependable as the security controls standing behind the answers on your application.

That is precisely why the partner you choose to manage your technology matters as much as the policy itself. The eighteen controls in this checklist: multi-factor authentication, immutable backups, endpoint detection and response, disciplined patch management, security awareness training, identity monitoring, and the rest are not one-time projects. They are ongoing disciplines that must be implemented correctly, maintained continuously, and documented thoroughly, both to satisfy an underwriter and, far more importantly, to stop an attack.

A capable Managed Service Provider (MSP) does much more than keep the lights on. The right MSP becomes the engine that makes your business insurable, keeps it insurable year after year, and ensures that if you ever have to file a claim, the controls you attested to are genuinely and verifiably in place. The wrong MSP, or no MSP at all, leaves those gaps quietly unaddressed until the day they are exposed by an attacker or, just as painfully, by a denied claim.

Choosing the right MSP is therefore one of the most consequential decisions a business owner can make. Look for a partner who understands the underwriting landscape, can measure your environment against the controls insurers now demand, remediate the gaps that surface, and supplies the documented evidence you need to stand behind every answer on your application. When your technology partner and your insurance strategy are aligned, you are no longer merely hoping to survive a cyber incident, you are genuinely prepared for one. That alignment is the difference between a business that recovers and one that does not.

Hope isn’t a strategy. Preparation is.

Note: This document is intended as a preparatory tool for insurance applications and internal cybersecurity gap assessments. Organizations should consult with a qualified cybersecurity professional, attorney, and insurance broker when completing cyber insurance applications.

ABOUT XSOLUTIONS

XSolutions Consulting Services LLC is a Managed IT Services Provider headquartered in New City, New York. Since 1999, we have helped small and mid-sized organizations across New York, New Jersey, and Connecticut run on technology that is reliable and secure, backed by a World-Class Helpdesk.

Our work goes far beyond keeping systems online. We build layered cybersecurity programs that protect users, devices, networks, and sensitive data, the very controls cyber insurers expect every applicant to have in place. From multi-factor authentication, managed detection and response, and email security to immutable backups, disaster recovery, security awareness training, and incident response planning, we help you close the gaps this guide identifies and document that you have done so. Put simply, we close the gaps that help make your organization insurable.

We specialize in the industries where downtime and data loss carry the highest stakes: law firms, construction and the trades, distribution and supply chain, nonprofits, and professional services. Because we understand how these businesses operate, our guidance is practical, compliance-aware, and built around the way you actually work.

What sets us apart:

- 15-minute response time on emergency tickets, with phones answered live by a real person.
- A 100% satisfaction guarantee, backed by more than 200 five-star Google reviews.
- Sophos Gold Security Partner status and enterprise-grade protection from trusted partners, including Sophos and Datto.
- A proven three-step approach: Listen, Align, Excel, that connects technology decisions to your business goals.
- Strategic guidance on technology budgeting, lifecycle planning, and the safe, practical use of AI.

Our mission is simple: deliver resilient IT and security that protect your operations, reputation, and future. When your technology partner and your insurance strategy are aligned, you are no longer hoping to survive a cyber incident, you are prepared for one.

Because, when it comes to your business, there is no time for downtime.

XSolutions Consulting Services, LLC • 20 Squadron Blvd., Suite 320, New City, NY 10956 • (877) 807-1332 • www.xsolutions.com

WHY WORK WITH US?



At XSolutions, we help businesses turn cyber insurance requirements into real-world controls: MFA, backups, endpoint protection, monitoring, patching, user training, incident response planning, and documentation your broker and carrier can understand.

Don’t delay! Call (877) 807-1332 now and ask for a Cyber Insurance Readiness Review.