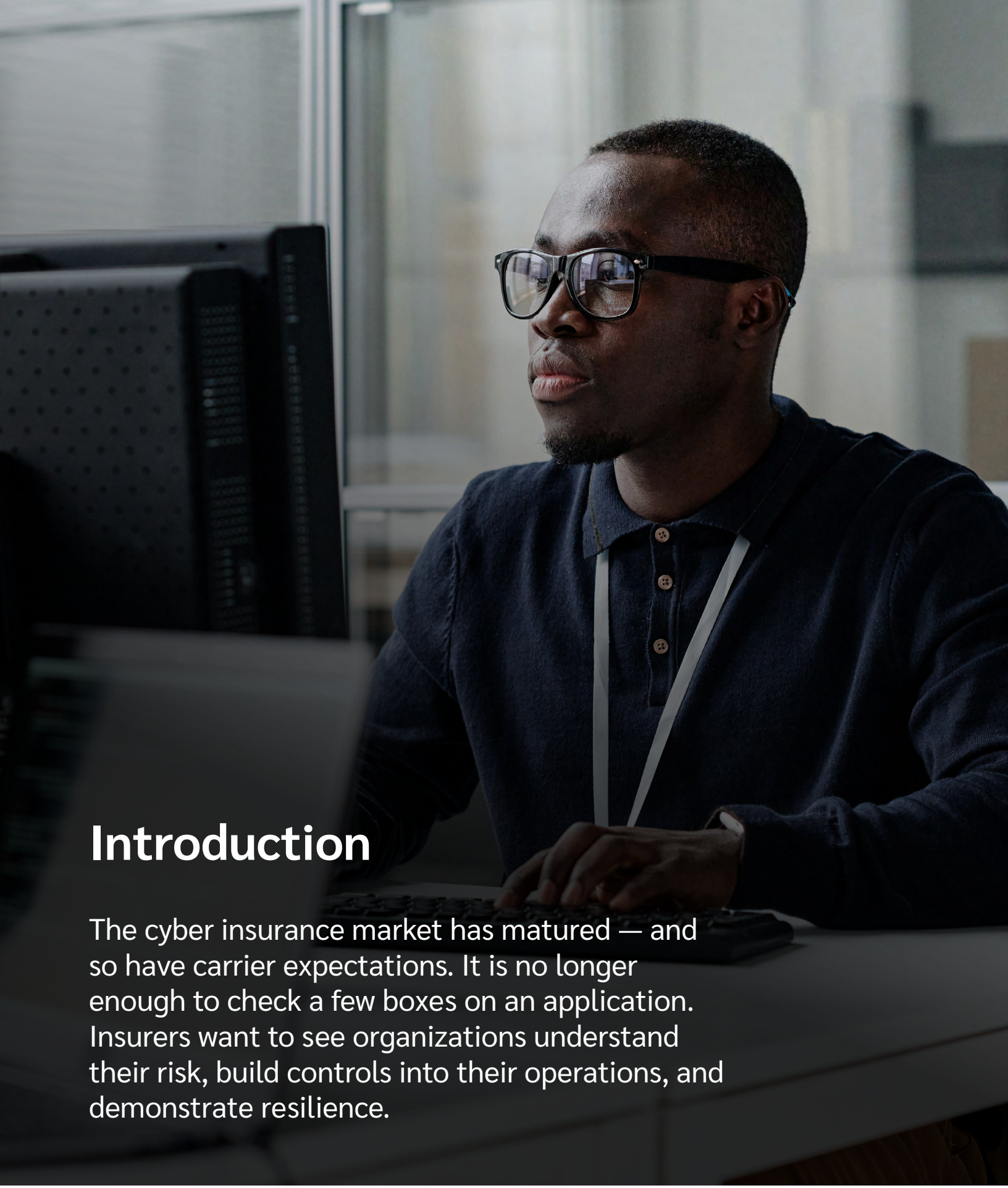
Cyber Controls Guide

Cyber & Technology

2026

LOCKTON®





Introduction

The cyber insurance market has matured — and so have carrier expectations. It is no longer enough to check a few boxes on an application. Insurers want to see organizations understand their risk, build controls into their operations, and demonstrate resilience.

This guide covers the cybersecurity controls carriers care about most:

01 **GOVERN**

02 **IDENTIFY**

03 **PROTECT**

04 **DETECT**

05 **RESPOND**

06 **RECOVER**

We've also added two areas that are rapidly reshaping the risk landscape: non-breach privacy exposures (such as tracking pixels and unsolicited communications) and artificial intelligence (AI) governance.

Each control is clearly explained, along with why it matters to your organization and your insurers, and practical steps you can take today.

This guide is not exhaustive (insurers assess risk differently), but these are the core controls that consistently influence whether coverage is available and how it is priced.



01

Govern

AI governance & acceptable use

WHAT IT IS: This is centered on the policies and frameworks that govern how your organization uses artificial intelligence — including generative AI tools like ChatGPT, Microsoft Copilot, and similar products — and how you manage the risks they introduce to your organization.

IN PLAIN TERMS: AI tools are already in your workplace, whether you've officially adopted them or not. Employees are using them to draft emails, summarize documents, write code, and analyze data. Without guardrails, employees may be feeding sensitive client data, proprietary strategies, or regulated information into tools your organization doesn't control. Meanwhile, threat actors are using AI to craft more convincing phishing emails, generate deepfake audio and video, and automate attacks at scale.

Why it matters

FOR YOUR ORGANIZATION: Uncontrolled AI use introduces significant risk, including data leakage (where sensitive information entered into public AI tools may be used to train future models), intellectual property exposure, and potential regulatory violations. AI-driven decision-making across hiring, underwriting, lending, content moderation can also create discrimination and bias liability. Meanwhile, threat actors are leveraging AI-powered deepfakes to enhance business email compromise and social engineering attacks, eroding the reliability of traditional verification methods.

FOR CARRIERS: This is a rapidly evolving area of underwriting. Carriers are increasingly asking whether organizations have formal AI use policies, and are closely monitoring emerging claims trends. For example, an employee pasting customer health records into a public AI chatbot is a privacy incident. An AI-generated decision that discriminates is an employment or regulatory claim. Organizations lacking AI governance represent an unknown and expanding risk profile.

Best practices

- Publish a clear, enforceable acceptable use policy for AI tools that specifies what data can and cannot be entered, which tools are approved, and what activities require human review.
- Inventory all AI tools currently in use across your organization — including shadow information technology (IT) (technology solutions adopted outside formal IT or cybersecurity oversight). You cannot govern what you don't know about.
- For any AI used in consequential decisions (hiring, lending, claims handling, customer-facing recommendations), document the logic, test for bias, and maintain human oversight.
- Train employees on AI-specific risks, including the dangers of entering confidential or regulated data into unapproved AI platforms and how to recognize AI-generated phishing and deepfake content.
- Review vendor contracts for any AI-related data usage terms — some SaaS platforms have begun integrating AI features that process your data in ways you may not have consented to.

Privacy governance & tracking technology management

WHAT IT IS: Policies, processes, and controls that govern how your organization collects, shares, and uses personal information — particularly around website tracking technologies (pixels, cookies, session replay tools) and digital communications (emails, texts, calls) that create regulatory exposure even without a traditional data breach.

IN PLAIN TERMS: If your website uses a Meta Pixel, Google Analytics, session replay tools (like Hotjar or FullStory), or similar tracking technologies, those tools may be collecting and transmitting your visitors' personal information — including health conditions, financial interests, or browsing behavior — to third parties. This happens automatically, often without the knowledge of your IT or marketing teams, and frequently without adequate user consent. Similarly, if your organization sends marketing text messages or makes automated calls, there are federal and state laws governing when and how you can do that.

These exposures are driving a wave of lawsuits and regulatory actions that have nothing to do with a hacker breaking into your network. They are privacy violations that arise from how your organization operates its own digital presence.

Why it matters

FOR YOUR ORGANIZATION: Tracking pixel litigation has exploded. Plaintiffs' attorneys are filing class actions under the Video Privacy Protection Act (VPPA), state wiretapping statutes, the Telephone Consumer Protection Act (TCPA), and state-level health data privacy laws. Healthcare organizations have been hit particularly hard — the FTC and HHS/OCR have taken enforcement action against companies whose pixels transmitted patient health information to advertising platforms. Settlements and defense costs in these cases routinely reach seven and eight figures. Critically, these claims frequently arise from routine marketing activity, not from any malicious acts.

FOR CARRIERS: Non-breach privacy claims are now a significant and growing portion of cyber insurance losses. Many carriers are adding specific questions around tracking technologies, cookie consent management, and TCPA compliance to their applications. Some are introducing sublimits or exclusions for privacy violations that don't involve a security breach. Organizations that cannot articulate their tracking technology practices represent a materially higher risk or may not be able to obtain insurance coverage for non-breach privacy claims.

Best practices

- Conduct a tracking technology audit: identify every pixel, cookie, and session replay tool deployed on your websites and mobile apps, what data each collects, and where that data is transmitted.
- Implement a consent management platform that provides clear, affirmative consent choices and prevents tracking technologies from activating until consent is received — rather than relying on passive cookie banners that default to full data collection.
- Review your data sharing relationships with advertising platforms. If you operate in healthcare, financial services, or any sector handling sensitive data, strongly consider whether the analytics value is worth the litigation risk.
- For digital communications, maintain documented evidence of consent before sending marketing texts or making automated calls. Scrub contact lists against do-not-call registries and honor opt-out requests immediately.
- Designate a privacy lead (or retain outside counsel) responsible for monitoring the rapidly evolving regulatory landscape across federal, state, and local levels. What was compliant last year may not be compliant today.
- Coordinate between marketing, legal, IT, and compliance teams — tracking pixel issues often fall through the cracks — no single team owns the full picture.

Third-party vendor risk management

WHAT IT IS: The policies, processes, and controls used to identify, risk-rank, perform due diligence on, contract with, and continuously monitor suppliers and other third parties throughout the life cycle of the relationship. These activities help organizations understand which vendors are critical, establish cybersecurity expectations before engagement, and maintain ongoing oversight of supplier risk.

IN PLAIN TERMS: Your security is only as strong as the organizations you trust. Many third parties store your data, connect to your network, process payments, host business-critical applications, or support essential operations. If one of those vendors experiences a cyber incident, your organization may still suffer operational disruption, data exposure, regulatory scrutiny, contractual disputes, or reputational harm. Third-party risk management helps ensure you understand which vendors matter most, what risks they introduce, and what security expectations they must meet before and throughout the relationship.

Why it matters

FOR YOUR ORGANIZATION: Organizations increasingly rely on cloud providers, managed service providers, software vendors, payment processors, consultants, contractors, and other external partners to conduct business. A vendor compromise can create the same business impact as a direct attack against your organization. Without a documented third-party risk management process, organizations often lack visibility into who has access to sensitive data, which vendors support critical operations, and whether those vendors maintain appropriate cybersecurity controls. Prioritizing suppliers by criticality, conducting due diligence before engagement, and monitoring vendors throughout the relationship helps reduce the likelihood of introducing avoidable risk into the environment.

FOR CARRIERS: Carriers increasingly view third-party and supply chain risk as a significant underwriting concern. Cyber incidents involving software providers, cloud service providers, managed service providers, and other critical vendors have demonstrated that a single supplier compromise can affect hundreds or thousands of organizations simultaneously. Insurers want to understand whether organizations maintain an inventory of key vendors, classify them according to criticality, perform security reviews before engagement, establish cybersecurity requirements in contracts, and maintain ongoing oversight of vendor risk. They may also evaluate whether organizations require critical vendors to maintain cyber insurance and other risk-transfer mechanisms.

Best practices

- Maintain an inventory of all third parties that access organizational data, systems, networks, or critical business processes, and classify them according to risk and business criticality.
- Define criteria for identifying critical vendors, including access to sensitive data, privileged access, operational dependency, regulatory impact, and business interruption potential. Prioritize oversight accordingly.
- Perform cybersecurity due diligence before entering into new vendor relationships.
- Assess security controls, incident history, regulatory compliance, and the maturity of the vendor's cybersecurity program before contract execution.
- Require vendors to complete security questionnaires and provide supporting evidence where appropriate, such as SOC reports, ISO 27001 certifications, penetration test summaries, or independent security assessments.
- Establish contractual cybersecurity requirements that are commensurate with the vendor's risk profile, including security control expectations, data protection obligations, breach notification requirements, audit rights, and subcontractor management provisions.
- Ensure contracts clearly define responsibilities for protecting sensitive information, managing vulnerabilities, maintaining access controls, and supporting incident investigation and response activities.
- Reassess critical vendors periodically and whenever significant changes occur, such as acquisitions, major technology changes, material cybersecurity events, or changes in the services provided.
- Maintain procedures for onboarding, monitoring, and offboarding vendors, including removal of access, return or destruction of data, and validation that contractual security obligations have been fulfilled.



02 Identify

Asset inventory & end-of-life management

WHAT IT IS: A current, complete inventory of all hardware, software, data, and user accounts across the organization — with a process for identifying and addressing assets that are outdated, unsupported, or no longer receiving security patches.

IN PLAIN TERMS: You need to know every device connected to your network, every application running in your environment, every cloud service you are using, and every account that has access to your systems. And when software or hardware reaches the end of its supported life — meaning the vendor is no longer issuing security updates — you need a plan to replace, isolate, or retire it. Unsupported software, also known as end-of-life software, is one of the easiest targets for attackers because known vulnerabilities will never be fixed.

Why it matters

FOR YOUR ORGANIZATION: Shadow IT (tools and devices that IT doesn't know about) and forgotten legacy systems are among the most common entry points in cyberattacks. End-of-life software is particularly dangerous because attackers know exactly which vulnerabilities exist and that no patches are coming.

FOR CARRIERS: Insurers often ask about end-of-life systems and will want to know whether they are segmented from the rest of the network, what additional protections are in place, and what the roadmap/timeline is for replacing these systems. An organization running critical operations on Windows Server 2012 or an unpatched version of Exchange is a materially different risk than one that has a disciplined life cycle management process.

Best practices

- Maintain a centralized asset inventory that is updated continually (not just once a year), and includes hardware, software, cloud services, and data stores.
- Identify assets nearing end-of-life or end-of-support status and establish clear timelines for migration or retirement before support expires.
- If end-of-life systems cannot be immediately replaced, segment them from the rest of the network and apply compensating controls (restricted access, enhanced monitoring, no internet connectivity).
- Include SaaS applications and cloud workloads in your inventory — not just on-premise systems.
- Establish a formal decommissioning process so unused systems are removed from your environment



03 Protect

Access management & privileged account controls

WHAT IT IS: The policies, procedures, and tools used to control who can access what within your organization's IT environment — with special emphasis on privileged accounts (administrators) and service accounts that have elevated permissions.

IN PLAIN TERMS: Think of your network as a building. Access management determines who gets a key, which doors each key opens, and who gets the master key. Privileged accounts — domain admins, local admins, and service accounts — are the master keys. If an attacker compromises one of these accounts, they can go anywhere and do anything. The fewer master keys you have and the more tightly they're controlled, the harder it is for an attacker to cause widespread damage.

Why it matters

FOR YOUR ORGANIZATION: Compromised privileged credentials are involved in the vast majority of serious cyber incidents, including ransomware. If an attacker gains domain admin access, they can encrypt your entire environment, exfiltrate your data, and disable your security tools — often in a matter of hours.

FOR CARRIERS: This is consistently one of the first areas carriers examine. Insurers want to know how many privileged accounts and service accounts exist, whether they are managed through a privileged access management (PAM) solution, and how frequently access rights are reviewed. Poor privileged account and service account hygiene is a red flag that can result in higher premiums, restrictive terms, or an outright declination.

Best practices

- Implement the principle of least privilege: Give every user only the minimum access they need to do their job.
- Deploy a privileged access management tool (e.g., CyberArk, Delinea, BeyondTrust) to vault, rotate, and monitor privileged credentials.
- Restrict domain administrator accounts to the minimum necessary for operations, and eliminate persistent privileged access wherever possible in favor of just-in-time, task-based access.
- Privileged account separation, administrators must log out of their standard user account and log in using a separate privileged account to perform administrative tasks.
- Inventory and review all user accounts, service accounts, and their privileges at least quarterly. Remove or disable accounts that are no longer needed.
- Separate duties so that no single person has unchecked control over critical systems.

Multifactor authentication (MFA)

WHAT IT IS: Requiring users to verify their identity with at least two separate factors before granting access — typically something they know (a password) combined with something they have (a phone, hardware token, or authenticator app) or a biometric credential (fingerprint or face scan).

IN PLAIN TERMS: A password alone is no longer enough. Passwords get stolen through phishing, data breaches, and brute-force attacks. MFA adds a second lock on the door — even if someone steals your password, they still can't get in without the second factor. It is the single most effective control for preventing unauthorized access.

Why it matters

FOR YOUR ORGANIZATION: MFA blocks the vast majority of credential-based attacks. Organizations without MFA on remote access, email, and admin accounts are dramatically more likely to experience a successful intrusion.

FOR CARRIERS: MFA is a baseline requirement for most if not all cyber insurers. Lack of MFA on remote access, email, or privileged accounts is one of the most common reasons applications are declined or quoted with exclusions. MFA is non-negotiable.

Best practices

- Enable MFA on all remote access points (VPN, remote desktop), all email accounts, all privileged/admin accounts, and all cloud platforms containing sensitive data. Consider MFA for all backup data.
- Prefer phishing-resistant MFA methods (hardware security keys like YubiKey, or FIDO2/passkeys) over SMS-based one-time codes, which are vulnerable to SIM-swapping attacks.
- Extend MFA to all users — not just administrators. Attackers routinely target standard user accounts and then escalate privileges.
- Enforce MFA on third-party and vendor accounts that have access to your environment.

Email, web, & network filtering

WHAT IT IS: Tools and protocols that scan, filter, and block malicious content before it reaches your users — including email security gateways, web proxies, Domain Name System (DNS) filtering, and intrusion prevention/detection systems at the network perimeter.

IN PLAIN TERMS: Most cyberattacks originate through phishing emails, malicious websites, or network-delivered exploits. Filtering solutions act as a critical first line of defense, identifying and quarantining threats before users are exposed or required to decide. Think of these tools as the security checkpoint before someone enters the building.

Why it matters

FOR YOUR ORGANIZATION: Phishing remains the No. 1 attack vector. A single click on a malicious link can lead to credential theft, malware installation, or ransomware deployment. Layered filtering at email, web, and network levels dramatically reduces the volume of threats that reach your users.

FOR CARRIERS: Carriers expect to see email filtering with anti-phishing capabilities at a minimum. Organizations that also deploy web proxies, DNS filtering, and intrusion prevention/detection systems receive more favorable underwriting treatment. Email authentication protocols (SPF, DKIM, and DMARC) are increasingly asked about on applications — they prevent attackers from spoofing your domain to send phishing emails that appear to come from your organization.

Best practices

- Deploy an email security gateway that scans attachments and URLs, quarantines suspicious messages, and inspects attachments in a sandbox before delivery.
- Implement SPF, DKIM, and DMARC email authentication to prevent domain spoofing. Set your DMARC policy to “reject” or “quarantine” — a “none” policy provides visibility but no protection.
- Route outbound web traffic through a web proxy or DNS filtering service that blocks known malicious and high-risk domains.
- Deploy intrusion prevention/detection capabilities at the network perimeter to identify and block malicious traffic patterns.
- Review and tune filtering rules regularly — overly permissive rules erode protection, while overly aggressive rules create alert fatigue and workarounds.

Network segmentation

WHAT IT IS: Dividing your network into separate zones or segments so that a compromise in one area cannot spread easily to others.

IN PLAIN TERMS: Instead of having one flat network where everything can talk to everything, segmentation creates internal walls. If an attacker compromises a workstation in your marketing department, they shouldn't be able to reach your financial systems, your customer database, or your operational technology from there. Segmentation limits the blast radius of any single incident.

Why it matters

FOR YOUR ORGANIZATION: In a flat, unsegmented network, ransomware can spread from a single infected machine to every connected system within minutes. Segmentation buys you time and limits damage — it turns a potential catastrophe into a contained incident.

FOR CARRIERS: Insurers want to understand how your network is architected. Segmentation between IT and operational technology (OT) is particularly important for manufacturers, utilities, and healthcare organizations. Carriers also look for segmentation between internet-facing systems, backup data, and internal crown jewels.

Best practices

- Segment the network by function, sensitivity, or geography — at minimum, separate production systems from corporate networks, and separate internet-facing systems from internal systems.
- If you have operational technology (OT) environments, they must be segmented from IT networks. A compromise of your email system should not be able to reach the systems that control physical processes.
- Use firewall rules and access controls between segments — segmentation without enforcement is just an organization chart, not a security control.
- Test segmentation regularly to confirm that the boundaries are held. Penetration testing should include lateral movement testing between segments.

Patch & vulnerability management

WHAT IT IS: The process of identifying, testing, and applying security updates (patches) to software and systems when vulnerabilities are discovered.

IN PLAIN TERMS: When software vendors discover security flaws in their products, they release patches to fix them. The window between when a vulnerability is publicly known and when you apply the patch is your period of maximum exposure — attackers actively scan for and exploit known vulnerabilities, sometimes within hours of public disclosure. Patch management is the discipline of closing those windows as fast as possible.

Why it matters

FOR YOUR ORGANIZATION: Unpatched systems are one of the most common ways attackers gain initial access. Many of the most damaging cyberattacks in history exploited vulnerabilities for which patches were available but not yet applied.

FOR CARRIERS: Insurers typically ask about patching cadence on applications. The expectation is that critical patches are applied within 24 to 72 hours, and non-critical patches within one to two weeks. Organizations that cannot demonstrate a disciplined patching process face scrutiny.

Best practices

- Establish a formal patch management process with defined timelines: critical/zero-day patches within 24-72 hours, high-severity within one week, and routine patches within 30 days.
- Subscribe to vulnerability advisories from your key vendors and from Cybersecurity and Infrastructure Security Agency.
- Prioritize patching for internet-facing systems and systems that handle sensitive data.
- Where immediate patching is not possible (e.g., due to operational constraints), document compensating controls (network isolation, enhanced monitoring) and a timeline for remediation.
- Conduct regular vulnerability scanning, informed by an up-to-date asset inventory, to identify systems that have fallen behind on patching.
- Establish a procedure for how patch notifications are received, tested, and deployed — including documentation of any sandbox testing or exceptions.

Remote access, firewall, & virtual private network (VPN) security

WHAT IT IS: The controls that protect how users connect to your organization's network from outside the office — including VPN, firewalls, virtual desktops, and remote desktop protocol (RDP) — and the infrastructure that governs what traffic is allowed in and out.

IN PLAIN TERMS: Remote work is now standard, which means your network perimeter extends to every employee's home, every coffee shop, and every airport. The tools that manage this boundary — firewalls and VPNs — are only as good as their configuration, their maintenance, and their capabilities. RDP remains one of the most exploited attack vectors, essentially leaving a back door propped open on the internet if improperly secured. Increasingly, carriers are seeing claims that trace back to consumer-grade or misconfigured VPN and firewall appliances that simply weren't built for the job they were being asked to do.

A consumer-grade VPN or a low-end firewall appliance designed for home use might technically create an encrypted tunnel, but it often lacks the logging, access controls, firmware update cadence, and configuration complexity needed to protect a business environment. Misconfigured VPN, default credentials left on firewall management interfaces, and outdated firmware on edge devices have all been root causes in significant claims.

Why it matters

FOR YOUR ORGANIZATION: Exposed or poorly secured remote access points are a top entry method for ransomware operators. RDP brute-force attacks are automated and constant. A VPN that isn't properly configured — or a firewall that hasn't been updated in two years — creates a false sense of security that is arguably worse than having no perimeter protection at all, because the organization believes it is protected when it is not.

FOR CARRIERS: Carriers specifically ask about RDP (including AnyDesk, AnyViewer, Ewon, or TeamViewer), and remote access on applications. Open RDP without MFA is, for most insurers, an automatic declination. Beyond RDP, carriers are now asking more pointed questions about the firewall and VPN infrastructure itself — what products are in use, whether firmware is current, whether configurations are reviewed regularly, and whether the organization is relying on enterprise-grade solutions or consumer-grade equipment. Claims stemming from misconfigured or inadequate VPN/firewall infrastructure are a recognized pattern, and underwriters are adjusting their questions accordingly.

Best practices

- Block RDP access from the open internet entirely. If remote desktop functionality is required, use it only through a securely configured enterprise-grade VPN or RDP gateway with MFA enforced.
- Require MFA on all remote access methods — VPN, virtual desktop infrastructure, cloud applications, and any direct RDP connections.
- Use enterprise-grade firewall and VPN solutions appropriate for your organization's size and complexity. Consumer-grade routers and VPN appliances lack the security features, logging capabilities, and vendor support needed to protect a business environment.
- Keep firewall and VPN firmware current. Edge devices are a primary target for attackers, and vulnerabilities in popular firewall/VPN platforms are routinely exploited — often within days of disclosure.
- Review firewall rules and VPN configurations at least annually. Remove overly broad rules, close unnecessary ports, and disable unused features.
- Implement account lockout policies that block IP addresses after a defined number of failed login attempts.
- Audit remote access logs regularly and investigate unusual connection patterns (off-hours access, connections from unexpected locations, or connections from unapproved devices).
- Perform external vulnerability scans on a regular basis, at least quarterly.

Backup & data recovery

WHAT IT IS: The practice of regularly duplicating your organization's data and system configurations so that they can be restored if data is lost, corrupted, or encrypted by ransomware.

IN PLAIN TERMS: Backups are your insurance policy within your insurance policy. If ransomware encrypts your systems, if a disgruntled employee deletes files, or if a hardware failure destroys data, backups are what let you rebuild without starting from scratch — or paying a ransom. But backups only work if they're current, protected from unauthorized deletion, and actually tested.

Why it matters

FOR YOUR ORGANIZATION: The difference between a ransomware incident that costs you a week and one that costs you months (or forces a ransom payment) almost always comes down to the quality of your backups. Organizations with robust, tested, offline, or immutable backups recover faster and at dramatically lower cost.

FOR CARRIERS: Backup practices are a core underwriting question. Carriers want to know your backup frequency, whether backups are encrypted and protected, and whether you've actually tested restoring from them. The 3-2-1 rule (three copies, two media types, one off-site) is an example of a leading best practice.

FOLLOW THE 3-2-1 RULE

Maintain at least three copies of your data, on at least two different types of media, with at least one copy stored off-site or in a disconnected/immutable cloud environment.

Best practices

- Back up critical data and system configurations at least weekly. Daily or real-time backups are preferred for mission-critical systems.
- Encrypt all backups, both in transit and at rest.
- Ensure at least one backup copy is air-gapped or immutable so it can't be accessed, altered, or deleted from your production network. This prevents ransomware from encrypting your backups along with everything else.
- Test your ability to restore from backups regularly (at least annually, quarterly preferred). Validate the data integrity during your testing.
- Define your recovery point objective (RPO — how much data you can afford to lose) and recovery time objective (RTO — how quickly you need systems back) and build your backup strategy around those targets.
- Enforce policies so users save critical files to shared drives or file servers — not to individual workstations — and account for data on personal devices used for work.
- Restricted access and MFA; limit backup system access to dedicated accounts and utilize principle of least privilege.
- Monitor for backup failures, deletions, retention changes, and unusual access patterns.
- Document backup and recovery procedures, including who can restore, what order the systems are restored, and what legal/insurer notifications are required.
- Separate backup credentials, where backup admin credentials not shared with standard IT admin accounts or domain admin accounts.
- Align retention to threat dwell time, where retention is long enough to recover from delayed ransomware activation and support forensic and legal needs.

Cybersecurity awareness & training

WHAT IT IS: Ongoing education programs that teach your workforce to recognize and respond to cyber threats — including phishing simulations, privacy compliance training, and awareness of emerging risks like AI-powered social engineering.

IN PLAIN TERMS: Technology can catch a lot of threats, but people are still the most targeted vulnerability. Training ensures that when a phishing email slips through your filters — and some always will — your employees know how to spot it, report it, and avoid clicking. Training also covers the human-side risks around privacy compliance, data handling, and increasingly, how to use AI tools responsibly.

Why it matters

FOR YOUR ORGANIZATION: Human error is a contributing factor in the majority of cyber incidents. A well-trained workforce is a force multiplier for every other security control you have.

FOR CARRIERS: Carriers expect to see annual cybersecurity awareness training (includes training users to spot social engineering and phishing) for all employees and contractors, plus regular phishing simulations. Organizations that can show declining click rates on phishing tests over time demonstrate a maturing security culture.

Best practices

- Conduct mandatory cybersecurity and privacy training for all employees and contractors at least annually, with supplemental training for high-risk roles (finance, HR, executives).
- Run phishing simulations at least semiannually and provide targeted remedial training to users who click.
- Update training content to address current threats — including AI-generated phishing, deepfake voice/video attacks, business email compromise, and the proper handling of sensitive data in AI tools.
- Make training engaging and relevant. Compliance checkbox exercises don't change behavior; real-world scenarios and examples do.
- Track and report on training completion rates and phishing simulation results as part of your security metrics to leadership.



04 Detect

Endpoint detection & response (EDR)

WHAT IT IS: Security tools deployed on end-user devices (laptops, desktops, servers, mobile phones) that continuously monitor behavior, detect suspicious activity, and enable rapid investigation and containment.

IN PLAIN TERMS: Traditional antivirus works like airport security checking IDs against a do-not-fly database — it checks files against a database of known threats. EDR is fundamentally different. It watches how applications and users behave in real time and asks: "Should this program be doing this thing, on this machine, at this time?" When something looks wrong, EDR can alert your security team, isolate the device, and preserve evidence — all before the threat can spread.

Why it matters

FOR YOUR ORGANIZATION: Modern threats — including fileless malware, living-off-the-land attacks, and zero-day exploits — often evade traditional antivirus entirely. EDR provides the behavioral visibility needed to catch these sophisticated attacks. It also significantly accelerates incident investigation and containment.

FOR CARRIERS: EDR deployed across all endpoints (not just some) is a baseline expectation for most cyber insurers. Carriers distinguish clearly between EDR and traditional antivirus — antivirus alone is no longer considered adequate. Managed EDR (where a third-party security team monitors the alerts 24/7) is viewed even more favorably.

Best practices

- Deploy EDR on all endpoints — workstations, laptops, and servers — with no gaps. Partial deployment leaves blind spots that attackers will find.
- Ensure EDR alerts are monitored and actioned, ideally by a 24/7 security operations capability (in-house or outsourced). If an in-house team is monitoring and addressing alerts, ensure that the in-house team has the capacity to handle the workload of monitoring and addressing. A late or later response to an EDR alert could be the difference between a manageable intrusion and a catastrophic shutdown of operations.
- Integrate EDR with your SIEM or security monitoring platform for correlated visibility.
- Keep EDR agents and detection signatures current, and regularly review and tune detection rules.

Security monitoring (SIEM & SOC)

WHAT IT IS: The people, processes, and technology that continuously monitor your IT environment for signs of unauthorized activity — typically anchored by a security information and event management (SIEM) platform and managed by a security operations center (SOC).

IN PLAIN TERMS: An SIEM collects and analyzes log data from across your entire environment — firewalls, servers, email systems, cloud platforms, EDR tools — and looks for patterns that indicate something malicious is happening. An SOC is the team (in-house or outsourced) that watches those alerts, investigates them, and takes action. Together, they are your organization's security nervous system. Without them, an attacker can be inside your network for weeks or months before anyone notices.

Why it matters

FOR YOUR ORGANIZATION: The average time to detect a breach without dedicated monitoring capabilities is measured in months — during which time an attacker can exfiltrate data, map your network, and position for maximum damage. Continuous monitoring shrinks that window from months to hours or minutes.

FOR CARRIERS: Carriers increasingly expect organizations to have SIEM capabilities monitored by an SOC — either in-house or through a managed security service provider (MSSP). 24/7 monitoring is strongly preferred, as attacks frequently occur outside business hours. The presence of active monitoring signals that an organization takes detection seriously and can respond quickly.

Best practices

- Deploy a SIEM platform that aggregates logs from all critical systems: endpoints, network devices, cloud environments, identity platforms, and email.
- Define what you want the SIEM to achieve, retention period of logs, prioritization of high valued log sources, threat detection, compliance reporting, incident response support and forensics.
- Ensure the SIEM is monitored 24/7 — either by an in-house SOC or by a reputable MSSP/MDR (managed detection and response) provider. If an in-house SOC is used, ensure that the in-house team has the capacity to handle the workload of monitoring and addressing.
- Monitor active directory and identity systems specifically for signs of compromise — credential abuse, privilege escalation, and unusual account behavior are early indicators of a serious attack.
- Regularly review and tune alerting to reduce false positives without creating blind spots.



05 Respond

Incident response planning

WHAT IT IS: A written, tested plan that defines the steps your organization will take to contain, investigate, remediate, and communicate about a cybersecurity incident — including the roles and responsibilities of internal teams and external partners.

IN PLAIN TERMS: When a cyberattack hits, the clock starts ticking. The decisions made in the first few hours — who to call, what to shut down, what to preserve, who to notify — have an outsized impact on the final cost and outcome. An incident response plan is your playbook for those critical first hours and days. It should answer every question you won't have time to figure out during a crisis.

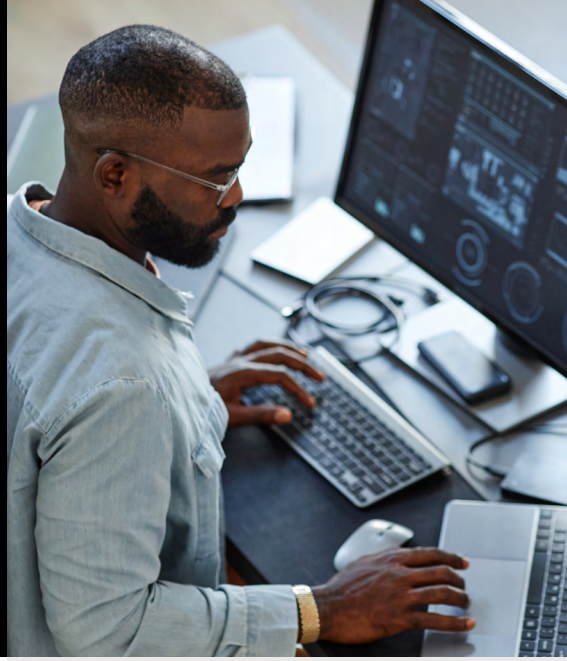
Why it matters

FOR YOUR ORGANIZATION: Organizations that respond effectively to incidents contain them faster, lose less data, experience shorter business disruptions, and face fewer regulatory penalties. Organizations without a plan make costly mistakes under pressure — destroying forensic evidence, making premature public statements, or failing to notify regulators within required time frames.

FOR CARRIERS: A written incident response plan that has been exercised within the past 12 months is a baseline underwriting requirement for most cyber insurers. Carriers want to see that the plan includes specific roles, contact information for key vendors (cyber insurance broker and insurer, breach counsel, forensic investigators, crisis communications), and a ransomware response playbook that outlines the steps the organization should take in the event of a ransomware attack. A plan that sits in a drawer untested is treated very differently from one that has been practiced through a tabletop exercise.

Best practices

- Maintain a written incident response plan that covers cyber-specific scenarios: ransomware, business email compromise, data exfiltration, insider threats, and privacy incidents (including tracking technology and regulatory inquiries).
- Include contact information for your key employees and decision-makers in the organization who will lead the process during a cyber incident, cyber insurance carrier(s) (and how to invoke your policy[ies]), pre-selected breach counsel, digital forensics and incident response firm, and crisis communications support.
- Conduct tabletop exercises at least annually — walk through realistic scenarios with participants from IT, legal, Human Resources (HR), communications, and executive leadership.
- Print and store copies of the plan in multiple locations (including offline) so it is accessible even if your network is down.
- Define escalation criteria clearly — what constitutes a security event versus a confirmed incident, and at what point each level of the organization (and your insurer) needs to be notified.



06 Recover

Business continuity & disaster recovery

WHAT IT IS: The plans, processes, and infrastructure that enable your organization to continue operating during and after a significant cybersecurity incident, and to restore systems and data to full functionality.

IN PLAIN TERMS: Business continuity planning answers the question: "If our systems are down for a week, can we still serve our customers, pay our employees, and keep the lights on?" Disaster recovery is the technical side — the specific procedures for rebuilding servers, restoring backups, and bringing systems back online. Together, they determine whether an incident is a temporary disruption or an existential crisis.

Why it matters

FOR YOUR ORGANIZATION: The business interruption costs from a cyber incident frequently exceed the direct costs of the breach itself. Organizations without tested continuity plans face extended downtime, lost revenue, customer attrition, and, in severe cases, permanent closure.

FOR CARRIERS: Business continuity and disaster recovery planning is a core underwriting question. Carriers want to see written plans, evidence of annual testing, and an established recovery time objective (RTO) and recovery point objective (RPO) for the most critical systems. The ability to recover from backups without paying a ransom is a key factor in claim severity.

Best practices

- Maintain written business continuity and disaster recovery plans that are reviewed and updated at least annually.
- Define RTO and RPO for each critical system and validate that your backup strategy supports them.
- Test recovery procedures at least annually through full restoration exercises — not just tabletop discussions. Confirm that you can actually rebuild critical systems from backups within your stated RTO.
- Plan for degraded operations: Identify manual workarounds for critical business processes so that essential functions can continue while systems are being restored.
- Incorporate lessons learned from incidents and exercises into plan updates — recovery planning is a living process, not a document.



Brendan Fitzpatrick
Vice President
Privacy and Cyber Risk Consultant
brendan.fitzpatrick@lockton.com
703.309.7338



John Nahas Jr.
Vice President
Privacy and Cyber Risk Consultant
john.nahas@lockton.com
816.381.3034

Get in touch

Visit our website

Looking to strengthen your cyber controls and resilience? We help you keep pace with today's cyber threats.

For general inquiries, please contact: cyber@lockton.com

About Lockton

As the world's largest privately held, independent insurance broker, we don't cater to shareholders or have external investors. We answer to the only voice that matters: **yours.**

This independence allows us to create a partnership with you where every interaction, decision, and solution is solely focused on your risk needs.

65,000+	13%	150+
CLIENTS WORLDWIDE	ORGANIC GLOBAL GROWTH	OFFICES WORLDWIDE
94%	$85B+	17
CLIENT RETENTION	PREMIUM VOLUME WORLDWIDE	CONSECUTIVE YEARS AS BEST PLACES TO WORK

This guide is for educational and informational purposes. The controls described here are not an exhaustive list of all insurer requirements, and specific carrier expectations will vary. Please consult your cyber insurance advisor for guidance tailored to your organization's specific risk profile and coverage needs.



UNCOMMONLY INDEPENDENT

lockton.com | © 2026 Lockton Companies. All rights reserved.

FS: 8341418