WHITE PAPER

11 Security Controls to Reduce Cyber Risk

Practical ways to strengthen your defenses, improve cyber resilience, and lower organizational risk.

SOPHOS

Executive summary

It's important for leadership in any organization to understand that optimizing your security controls is about more than just protecting data and systems, it's about reducing your organizational risk tied to brand reputation, customer trust, and business continuity. Cyberattacks such as ransomware and business email compromise (BEC) can have major operational and financial consequences. Cybercrime is predicted to cost the world $1.2 trillion USD in 2025,[1] according to Cyber Defense Magazine. Even when mitigated, attacks can cause serious disruption if systems must be taken offline to reset and rebuild. Some organizations can weather this kind of storm. Others face existential questions they never anticipated.

$1.2 trillion USD

In 2025, cybercrime is predicted to cost the world $1.2 trillion USD.[1]

The role of security controls in maximizing cyber defenses

Security controls are the levers security teams can pull to reduce risk and shield the organization from threats. There are many types of controls, but they share the common goal of either preventing incidents and breaches or minimizing damage when security events do occur. Some are geared toward prevention, others deliver different levels of mitigation across threat prevention, detection, and response. Having the proper mix of strong security controls in all areas is a key part of establishing defense-in-depth.

Strong security controls are also a critical component of managing risk through cyber insurance. Insurers consider the organization's controls when setting premiums and coverage limits.

These typically cover:

First-party liabilities include direct harm your organization may incur from a cyberattack or breach. This can involve business interruption, data restoration costs, theft, or ransomware payments.

Third-party liabilities stem from customers, partners, regulators, or others and may include lawsuits, compensation demands, or regulatory fines imposed by government agencies and/or trade associations.

Why it matters

Better controls don't just protect your operations—they can reduce insurance premiums and improve claims outcomes.

Reduce cyber risk with these 11 security controls

Investing in strong controls helps reduce cyber risk and can help improve insurability and potential policy terms. Here are eleven foundational controls that strengthen defenses across a range of prevention and impact reduction categories.

Properly implemented, these security controls bolster your cybersecurity posture, making it ready to take on both the threats of today and those in the future.

1. Identity and access management
2. Endpoint security
3. Multi-factor authentication
4. Vulnerability management
5. Email security
6. Privileged session management
7. Asset management
8. Segmentation and architecture
9. Extended detection and response (XDR)
10. Backup and business continuity
11. Network security and traffic control

1. Identity and access management

Identity and access management (IAM) ensures that only authorized individuals can access systems and data. Privileged Access Management (PAM) further limits access to what users strictly need. It may sound simple, but this can quickly become a quagmire—especially in larger organizations. All businesses should maintain strict onboarding/offboarding processes, enforce strong password hygiene, and routinely audit access.

Regardless of size, every organization must have clear rules for removing stale identities—otherwise, attackers can exploit forgotten accounts to escalate privileges and move laterally through your environment undetected.

2. Endpoint security

Every device connected to your environment is a potential target. Hybrid work has increased exposure, making endpoint protection more critical than ever. Many attacks start with low-effort "commodity" threats that strong endpoint tools can detect and neutralize. However, unsupported or forgotten endpoints often become weak points and are a common entry point for remote ransomware attacks. Ensure every device is covered.

3. Multi-factor authentication

Multi-factor authentication (MFA) validates a user's identity with multiple factors: something they know (e.g., password), have (e.g., token), or are (e.g., fingerprint). With compromised credentials remaining one of the leading causes of attacks,[2] MFA is a vital control for modern organizations. Consider more advanced forms like geolocation and numerical matching to improve resilience against attacker bypass tactics, while also balancing user experience and privacy.

Takeaways

Dormant accounts and unused privileges are low-effort entry points for attackers. Once inside, they can be used to gain elevated access and quietly expand the reach of an attack.

The most common entry point is often the least visible. Don't let outdated endpoints become backdoors.

Implement adaptive MFA to increase verification in high-risk scenarios without creating unnecessary friction.

4. Vulnerability management

Vulnerability management is the ongoing process of identifying, assessing, and remediating security weaknesses across your environment. It includes common practices like software and system patching, configuration updates, and monitoring for newly disclosed vulnerabilities. Strong threat intelligence is critical to help stay ahead of emerging risks.

Understanding where all assets reside on your network is essential for comprehensive scanning. With that visibility, organizations can take a risk-based approach to prioritizing which vulnerabilities to address first—based on exposure, likelihood of exploitation, and business impact.

5. Email security

Despite being an older technology, email remains one of the top entry points for attackers. Phishing, in particular, is a common vector for ransomware and credential theft. Business Email Compromise (BEC) is also among the most frequent cyber insurance claims.[3] Strong email security can prevent malicious content from ever reaching the inbox—making it a critical first line of defense. As generative AI improves phishing tactics with better grammar and messaging, protections must evolve to reduce the success rate of these attacks before they reach users.

But protection shouldn't stop at delivery. URLs and attachments that appear safe at first can become malicious after a message lands in the inbox. Advanced email security solutions now offer post-delivery detection and remediation—automatically rescanning content, retracting malicious messages, and neutralizing links if their risk profile changes. These controls help catch threats that sneak past initial defenses and minimize the time harmful messages remain in user inboxes.

Takeaways

Look for vulnerabilities in your third-party apps and cloud services—not just your core systems.

One click is all it takes. The best way to stop phishing is to make sure users never see the bait—even after delivery.

6. Privileged session management

Administrative accounts offer a threat actor the most power—especially when those privileges include access to identity systems, configuration controls, and security tools. If an attacker can gain admin-level access, they can disable defenses and deploy ransomware at scale.

To reduce this risk, organizations should implement a tiered model for privileged access and actively monitor how those accounts are used. Privileged Session Management (PSM) provides oversight by logging, recording, and in some cases, controlling admin sessions in real time—helping detect suspicious activity, prevent misuse, and support compliance.

7. Asset management

You can't protect what you don't know you have. Organizations must maintain up-to-date inventories of both physical and data assets. During an incident, knowing where sensitive data is stored is critical for a timely and effective investigation, accurate reporting, and fast containment. Proper asset management supports a thorough investigation, helps streamline responsibilities, and reduces the impact of a breach.

8. Segmentation and architecture

If a threat actor gains access to your environment, their next step is typically lateral movement—seeking to escalate privileges, access sensitive systems, or deploy ransomware. Strong network segmentation and architectural design can make that movement far more difficult. By creating friction and forcing attackers to make more noise, segmentation increases your chances of detecting them earlier in the attack chain.

Your system architecture should be built on the principles of confidentiality, integrity, availability, and resiliency. That includes limiting system-to-system and user-to-system access through a zero trust model, where every transaction is verified based on the user's identity, device, and permissions.

Takeaways

Can you see who accessed your admin layer last Tuesday—and exactly what they did? If not, it's time to tighten oversight.

Retaining unneeded records can inflate insurance costs and multiply reputational damage during a breach.

Use network segmentation to isolate critical systems from routine access points.

9. Extended detection and response (XDR)

Juggling dozens of disparate tools can fragment alerting, slow triage, and hide threat activity. Extended detection and response (XDR) remedies this by providing a unified view of activity across endpoints, firewall, network, email, identity, backup, and cloud security systems, reducing alert noise and enabling faster, more confident decision-making. It eliminates the “swivel chair” scenario where analysts must bounce between siloed tools to investigate and respond to threats.

More robust XDR systems also apply advanced analytics, AI-prioritized detection, deep data search, and automated alert correlation and escalation. This convergence of capabilities improves detection accuracy, accelerates investigations, and helps security teams focus on the highest-risk threats without getting bogged down in tool friction.

10. Backup and business continuity

When a cyber incident disrupts operations or corrupts systems, well-prepared backups and a strong business continuity plan can be the difference between fast recovery and extended downtime. But not all backups are created equal. To be effective, backups must be validated, tested regularly, and capable of restoring systems and data with integrity.

One common failure point is setup. Many organizations discover too late that their backups only partially restore systems or miss critical data, turning a short-term outage into a weekslong scramble.

It’s equally important that backups are protected through out-of-band authentication. Without it, a threat actor with broad access may attempt to disable or delete backup data as part of their attack.

Takeaways

XDR transforms disconnected alerts into decisive action, accelerating investigations and improving response outcomes.

Keep backups segmented and offline whenever possible. Your recovery should never rely on a single channel.

11. Network security and traffic control

The network is more than a connection layer—it's a strategic control point for inspecting, filtering, and managing traffic across your environment. Firewalls, intrusion prevention systems (IPSs), DNS filtering, and secure web gateways form the backbone of layered enforcement.

But not all firewalls are created equal. Legacy, misconfigured, or underutilized solutions can leave exploitable gaps. Regularly evaluating your defenses, keeping them patched and up to date, and aligning them with your current threat landscape is essential to maintaining resilience.

Modern controls like Zero Trust Network Access (ZTNA) offer more granular, context-aware access enforcement. Together with traditional protections, they help reduce the attack surface, prevent lateral movement, and stop exfiltration across hybrid and cloud environments.

Takeaways

Integrate network telemetry into your detection stack to improve visibility, accelerate investigations, and flag anomalous activity—especially lateral movement and command-and-control traffic.

From holistic view to holistic approach

Cybersecurity isn't just about deploying the right tools—it's about having a strategy that brings people, processes, and technology together. These 11 controls, when implemented thoughtfully and consistently, can materially reduce your organization's exposure to risk.

Long-term resilience comes from building a strong cybersecurity program that's repeatable, adaptable, and rooted in clear ownership. Technology is powerful, but it takes skilled teams and structured processes to ensure it's used effectively.

Threats will evolve, technologies will shift, and your business will change. Staying ahead means thinking holistically, adapting continuously, and building a culture where security is not just a checkbox, but a core business enabler.

[1] Cyber Defense Magazine: The True Cost of Cybercrime: Why Global Damages Could Reach $1.2-$1.5 Trillion by End of Year 2025
[2] Sophos, Annual Threat Report 2025
[3] Dark Reading, "Email-Based Attacks Top Cyber-Insurance Claims", May 8, 2025

SOPHOS

Ready to assess your cybersecurity program?

Speak to a Sophos expert today.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

North America Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com