ANNUAL THREAT REPORT

2025 cyber resilience checklist

Use these lessons from last year to power your strategy this year

Every year, our analysts review the data our SOC has collected over the past 365 days and report on the insights. This data comes from companies of all sizes across every industry and is ingested from tools monitoring endpoints, networks, clouds, SaaS applications, identity providers, and more.*

We've turned these insights into tasks. Take heart: cybersecurity is measured in inches, not miles. Because of cybersecurity's interconnectivity, the smallest change on one attack surface can have a positive impact on your org's overall security maturity.

Identity threats

Year-over-year, identity-based attacks continue to be the most common attack type we see across our customer base, with increasing volume. Barring major changes in cybercrime, we expect this trend to continue into 2025.

Practical ways to reduce identity risk:

- ☐ Reset passwords *and* terminate sessions for compromised accounts immediately.
- ☐ Always investigate new multifactor authentication (MFA) devices, especially when they're added after password resets or while connected to a proxy or VPN.
- ☐ Alert to new inbox rules, especially if they have simple names or contain keywords like "payroll", "malware", or "virus".
- ☐ Remind employees to be familiar with their payroll information and notify security teams of unauthorized changes.
- ☐ Require approval for sensitive information (like direct deposit details) updates in HR management systems.

> **"Protection against identity threats will remain the single most important part of most companies' security posture. Attacks will continue increasing in sophistication and speed, especially powered by artificial intelligence, which is aiding attackers to carry out tried and true methods more efficiently."**
>
> —Greg Notch, Chief Security Officer, Expel

* Our SOC monitors security activity within Expel Workbench™, a platform that integrates with over 125 different security tools and correlates data from across attack surfaces.

Cloud threats

Cloud infrastructure attacks will continue to increase in parallel with cloud adoption rates. The techniques and frequencies of these attacks evolve constantly as the cloud attack surface expands. This includes cloud platforms like Amazon Web Services (AWS), Google Cloud, Microsoft Azure, and Kubernetes, and the control and data planes of these platforms.

Practical ways to reduce cloud risk:

- ☐ Build detections to spot suspicious activity at multiple stages of the attack lifecycle.
- ☐ Use secret scanning to prevent accidental key exposure. This will check code repositories during development or after publication and can also be done through paid services or open source tools.
- ☐ For AWS customers, create detections around long- and short-term access keys (beginning with AKIA and ASIA, respectively) to detect early stages of unauthorized access.

Did you know?

In 2024, 86% of cloud infrastructure incidents targeted AWS, while only 9% accounted for impacted assets in Google Cloud and Azure. If you're an AWS cloud customer, be sure to take extra precautions.

Computer-based threats

Computer-based threats is a vast incident category that includes malware and vulnerabilities. This year's data highlights a shift from initial access tools (IATs) to infostealers as attackers' preferred malware. Additionally, attackers continue to make it clear that the age of a vulnerability doesn't matter if it's still exposed.

Practical ways to reduce computer-based risk:

- ☐ Authorize legitimate PDF editing tools and make them readily available to your employees to prevent malware risks from PDF-to-doc converter websites.
- ☐ Update Windows settings to open Notepad instead of executing a JavaScript file when a user double-clicks using the Group Policy Editor.
- ☐ Familiarize your org with the ClickFix tactic, and protect against it by:
  - Using secure web gateways to block traffic from attacker-controlled domains.
  - Ensuring hosts are monitored with EDR systems and have it in blocking mode.
  - Disable the Windows Run program for users who don't need it.

- [ ] Prepare a playbook for stolen credential incidents that includes:
  - Updating credentials saved in browsers when malware is encountered.
  - Resetting credentials saved to a host (like AWS, Azure, or Google Cloud).
  - Implementing a password management tool for your organization, and confirming contractors have access, too.
  - Ensuring unused accounts are deactivated and monitored for compliance.
- [ ] Having (and using) a clear patching plan for vulnerabilities, based on severity and impact.
- [ ] Allocating resources for vulnerability management, like network scanners, personnel, or outside vendors.
- [ ] Maintaining clear plans for server and other critical updates to reduce any risks associated with outdated tech.

Heads up

In October of 2025, Windows 10 is scheduled for end of life (EOL), meaning it'll no longer receive regular maintenance and security updates. Start planning your migration ASAP!

Phishing threats

Phishing preys on human nature, and the best way to fight back is with proper cybersecurity training programs. However, you can also take practical steps within your tech stack to reduce the risk of attackers succeeding.

Practical ways to reduce phishing risk:

- [ ] Encourage users to rely on MFA whenever possible and have MFA settings align with the Fast Identity Online 2 (FIDO2) standards.
- [ ] Remind employees that it's not just their corporate accounts at risk. These same best practices can also protect their personal information and accounts.
- [ ] Use secure email gateways to filter out a substantial amount of phishing email attempts.
- [ ] Continue to educate your employees on how to identify and report suspicious emails.

Pro tip

Microsoft Teams users are common phishing targets. In the latest campaign, attackers sign targets up for spam emails and then send messages via Teams posing as someone internally who can resolve the issue.

If the invite is accepted, Microsoft's built-in remote access support tool, Quick Assist, will launch. Attackers can then use access to install additional remote access tools (RATs) for future malicious behavior.

Update your Teams settings to restrict unauthorized invitations. Managing an "Allow List" is more work initially, but provides protection over time that's worth the effort.