CORVUS | BY TRAVELERS

Top 3 Cyber Risk Findings

Quick fixes with outsized impact on cyber risk

This is a supplement to information found in the Corvus by Travelers Cyber Risk Scan Report and Cyber Risk Dashboard. Policyholders should regularly check their dashboard to see current, prioritized findings specific to their IT environment during the policy term.

Remember: Travelers' Cyber Risk Services team is here to help! We can review findings and help prioritize the actions that will make the most impact to an organization's cybersecurity. Policyholders can contact us any time at cyberservices@travelers.com.

1. Certificate Best Practices

TIME TO FIX: One day

HELPS PREVENT: Attacker-in-the-middle attacks and lost customer trust

Report Finding

"The Travelers Cyber Risk Scan identified issues with security certificates on domains associated with the organization. Security certificates ensure that communication to and from servers is encrypted, helping to protect sensitive information and prevent threat actors from reading or modifying information in transit."

What it means

Security certificates are a core component of web security, providing a third-party stamp of approval that a website and its owner are who they say they are. Certificates need to be renewed prior to the end of a pre-set "lifetime," otherwise the browser will display an alarming warning to visitors to avoid the site.

Recently the CA/Browser Forum, a group of leading vendors of web browsers and security certificates, voted to shorten the maximum lifetime for security certificates from 398 days to 200 days, establishing a new industry standard.

What to do next

Policyholders should audit all certificates in use on public-facing systems. Any certificates that are expired or use deprecated hash algorithms that no longer meet modern security standards (e.g., SHA-1) should be reissued with SHA-256 or better. Additionally, certificate validity should be limited to a maximum of 200 days, and a renewal tracking process should be implemented so certificates are rotated before they expire.

Benefits of remediation

Properly configured certificates protect data in transit, prevent browser warnings that erode customer trust and reduce attacker-in-the-middle risk. Shorter validity periods limit the window of exposure if a private key is ever compromised.

Tip: Policyholders should go beyond solving the immediate need and set up automated certification renewals. This will help prepare for future changes, as the industry is likely to reduce the maximum lifetime of security certificates again in the next few years.

2. Common Vulnerabilities and Exposures (CVEs)

TIME TO FIX: Varies – can be as little as one day **HELPS PREVENT:** Exploitation of known software flaws

Report Finding

"Public-facing systems may be running software with known, published vulnerabilities. These vulnerabilities, commonly known as CVEs, are publicly disclosed flaws in software or hardware that have been assigned a unique identifier (e.g., CVE-2026-12345) so defenders and vendors can track and remediate them."

What it means

Travelers constantly monitors the CVE database, and if the team determines that a CVE poses a serious risk, they will check for the affected software among Travelers policyholders using the Cyber Risk Scan. If the affected software is located in a policyholder's environment, that policyholder is alerted and the recommendation appears in the Action Center on the policyholder's Cyber Risk Dashboard.

What to do next

Policyholders should work with their IT professionals to implement the remediation recommendations to patch impacted software. Organizations can often fix several patches during a single session conducted outside of core business hours to avoid disrupting operations. Going forward, policyholders should standardize their cadence of patching by setting an expectation that critical-severity vulnerabilities be fixed within 72 hours, and high-severity vulnerabilities within 30 days. Longer term, policyholders should consider adopting a Risk-Based Vulnerability Management (RBVM) approach, which prioritizes fixes by what's being actively exploited and what assets are exposed to the internet.

Benefits of remediation

According to Verizon's 2025 Data Breach Investigations Report, exploitation of known vulnerabilities now accounts for 1 in 5 breaches — a 34% increase in a single year and the fastest-growing initial access vector tracked in the study. What's more, new AI models are predicted to enable threat actors to exploit CVEs more quickly in the future. Quickly patching CVEs closes off one of the easiest paths for attackers, preventing situations like these:

- **Credit reporting bureau:** failure to patch a single flaw (CVE-2017-5638) exposed personal data on approximately 147 million people and led to a global settlement of up to $700 million.
- **Password management software:** A DevOps engineer's personal device was running software with a known vulnerability (CVE-2020-5741) that had gone unpatched for over two years. Attackers exploited it to capture the engineer's credentials and steal customer vault data. A resulting class action was settled for $24.45 million.

LEARN MORE

Common Vulnerabilities and Exposures

Risk-Based Vulnerability Management

3 . Externally Accessible Remote Access Services

TIME TO FIX: 1–2 weeks (longer if self-managed)

HELPS PREVENT: Ransomware's most common initial-access vector

Report Finding

"The Travelers Cyber Risk Scan detected the presence of publicly exposed remote access services on a system associated with the organization. Remote access services include SSH, Telnet, Telnets, IKE, and PPTP."

What it means

Enabling remote access is a fact of life for companies with many locations or remote workers. But remote access needs to be handled carefully. Travelers' predictive risk model has observed an increased rate of attacks on organizations with a large external attack surface, particularly those with externally accessible remote access ports and services on owned or dedicated servers. The compromise of one such server could lead to compromise of other internal or critical systems.

What to do next

First, Policyholders should identify all remote access services reachable from the internet at their organization. For each service found, web access should either be shut off (if it is no longer in use or redundant) or placed it behind a virtual private network (VPN) or zero-trust network access (ZTNA) tool. Policyholders should avoid secure sockets layer (SSL) VPN solutions in favor of options with strong security track records.

Whichever solution policyholders choose, they should also ensure multifactor authentication (MFA) is required on every remote access path.

> **Tip:** We're here to help! The Travelers Cyber Risk Services team can help policyholders review their existing configurations and advise on updates.

Benefits of remediation

Exposed remote access is the leading initial-access vector for ransomware:

- 56% of incident-response cases began via external remote services; remote desktop protocol (RDP), one type of external remote service, was the vector of attack in 84% of those cases[1]
- Internet-facing vulnerabilities were the initial-access vector in 39% of cases in 2023[2]
- Average ransomware recovery cost (excluding ransom payments) in 2024 was $1.53M[3]

LEARN MORE

Zero Trust Network Access (ZTNA)

Securing Network Access

Questions or need more detail on any of these findings?

Log in to the Cyber Risk Dashboard, or connect your client with a Travelers cyber risk expert by emailing

cyberservices@travelers.com

1 . Sophos, "2025 Active Adversary Report"
2 . Palo Alto Networks Unit 42, "2024 Incident Response Report"
3 . Sophos, "The State of Ransomware 2025"