Salt Typhoon: A Wake-up Call for Critical Infrastructure

By Gabrielle Hempel

Published: 2025-03-13 · Archived: 2026-04-05 21:10:44 UTC

4 Min Read

Source: Andrii Yalanskyi via Alamy Stock Photo

COMMENTARY

The Salt Typhoon cyberattacks marked a sobering milestone in the evolution of large-scale cyber threats. These sophisticated intrusions targeted critical infrastructure across the United States, specifically US Internet service provider (ISP) networks, thus disrupting essential services in sectors that include energy, transportation, and healthcare. Leveraging advanced tactics like zero-day exploits and obfuscation, the attackers not only caused operational downtime and financial losses but also evaded detection with alarming precision. Likely linked to state-sponsored actors, the scale and persistence of these attacks highlight the urgent need for a coordinated and unified response to mitigate future risks.

At least nine major US telecommunications companies, including Verizon, AT&T, and T-Mobile, were affected. Sensitive systems, such as those used for lawful intercepts, were breached, exposing government communications and jeopardizing ongoing investigations. The attackers also accessed metadata for more than a million users, raising significant privacy and security concerns. Although specific financial losses have not been disclosed, the affected telecom companies collectively generate more than $334 billion in annual revenue, indicating the

potential economic magnitude of the attack. These disruptions have not only strained public trust but also emphasized the vulnerabilities within critical infrastructure that adversaries can exploit.

Challenges in the Aftermath: Rebuilding Trust and Compliance

The aftermath of Salt Typhoon has left industries grappling with various challenges. Many companies are now facing regulatory compliance costs, the need for rapid implementation of enhanced security measures, and legal battles stemming from sanctions against the attackers. Beyond these tangible impacts, the public disclosure of these breaches has tarnished corporate reputations and heightened concerns over data privacy. For industries operating in critical sectors, the stakes are higher than ever: failure to address these vulnerabilities could lead to follow-up attacks that destabilize essential infrastructure, compromise sensitive data, and even erode public trust in national institutions.

The growing complexity of these threats demands a multifaceted response. Salt Typhoon underscored systemic weaknesses, such as outdated systems, inadequate threat detection, and insufficient identity verification mechanisms. These shortcomings amplify the difficulty of mitigating nation-state-level threats, forcing organizations to rethink their cybersecurity strategies. The adoption of advanced defense architectures, such as zero-trust frameworks and AI-driven monitoring, is no longer optional but imperative to restoring trust and fortifying resilience.

The Role of Federal Agencies: Public-Private Collaboration for Effective Response

The private sector cannot tackle these challenges alone. Federal agencies such as the Cybersecurity and Infrastructure Security Agency (CISA) and the FBI must lead efforts to mitigate threats and assist with recovery. A coordinated response that prioritizes public-private collaboration is critical to preventing future incidents. Real-time threat intelligence sharing between federal agencies and the private sector can enable organizations to detect and respond to advanced threats more effectively. Additionally, federal resources, including technical expertise and funding, can accelerate recovery efforts, helping affected industries address vulnerabilities and restore operations.

However, the recent decision by the Department of Homeland Security (DHS) to terminate all of its advisory committees raises new concerns about the continuity of government-industry collaboration in cybersecurity. Advisory committees have long played a vital role in shaping security policies, facilitating information exchange, and ensuring that private sector concerns are integrated into federal decision-making. Without these advisory bodies, industries may face additional challenges in obtaining clear guidance and streamlined coordination from federal agencies, potentially slowing response efforts in the wake of future cyber incidents.

Beyond immediate recovery, long-term strategies must focus on resilience. National cybersecurity training programs and preparedness initiatives can equip organizations with the tools needed to defend against increasingly sophisticated attacks. Federal agencies should work closely with the private sector to strengthen the overall cybersecurity posture, ensuring a robust framework that can withstand evolving threats. Despite the DHS's restructuring, it is imperative that new channels for collaboration be established to maintain a strong national cybersecurity defense.

Key Takeaways: Federal Support, Unified Defense, and Proactive Measures

The lessons from Salt Typhoon are clear. Federal involvement is essential for industries to recover and build long-term resilience. Enhanced threat intelligence sharing fosters unified defenses, while federal resources provide the expertise and support needed to recover from large-scale cyber incidents. In addition, proactive measures such as adopting AI-driven threat detection and zero-trust architectures can help organizations mitigate vulnerabilities and prevent future attacks.

The coordinated actions taken in response to Salt Typhoon will yield significant benefits. Streamlined recovery efforts supported by federal resources will minimize operational downtime and financial losses. Enhanced collaboration between public and private sectors will strengthen defenses, reducing the likelihood of future incidents. However, with the dissolution of DHS advisory committees, the cybersecurity community must remain vigilant in establishing alternative avenues for engagement with federal agencies to ensure continued information-sharing and effective cyber-defense strategies.

Salt Typhoon served as a wake-up call for industries and federal agencies alike, underscoring the need for unity, innovation, and resilience in the face of an increasingly sophisticated cyber-threat landscape. While the structure of federal advisory support may be shifting, the mission remains the same: safeguarding national security through proactive collaboration and technological advancement.

About the Author

Security Operations Strategist, Exabeam

Gabrielle Hempel is security operations strategist at Exabeam and a law student specializing in cybersecurity and policy management.
