blackbeltsecure.com

January 2026

DIGITAL DEFENSE DIGEST

Insider Tips To Make Your Business Run Faster, Easier And More Profitably

WHAT'S NEW

Critical Infrastructure Win: Complexul Energetic Oltenia targeted by Gentlemen ransomware (Dec 2025)—OT isolation and immutable backups blocked disruption; quick recovery, no ransom paid.

Ransomware Surge Confirmed: Over 4,700 global incidents reported Jan-Sep 2025 (34% up from 2024), with half targeting essential services–highlighting why basics like segmentation and patching remain your strongest shield.

AI Threats Accelerating: Emerging groups leverage AI for adaptive phishing and automation; prepare for mainstream autonomous attacks in 2026 with behavioral detection and deepfake training.

This monthly publication is provided by Black Belt Secure

BLACK BELT SECURE

OUR MISSION:

To empower businesses of all sizes with the knowledge and tools they need to thrive in today's increasingly complex cyber threat landscape. We are dedicated to providing cutting-edge cybersecurity solutions and expert guidance to help our clients

LESSONS FROM 2025: BUILDING RESILIENCE FOR 2026

YOUR GUIDE TO DEFENDING AGAINST EVOLVING THREATS AND THRIVING IN THE NEW YEAR.

The perception that SMBs have limited resources, smaller budgets and often a “that won’t happen to us” mindset makes them attractive to hackers. Although it’s true that SMBs don’t have the resources of Fortune 500 companies, you don’t need that kind of money to protect your business. Here are six simple strategies hackers hate because they’re affordable, surprisingly easy to set up and highly effective.

Key Lessons from 2025's Major Cyber Incidents

1 Energy Sector Targeted Heavily

In late December 2025, Romania's largest coal-powered energy provider, Complexul Energetic Oltenia, was hit by the "Gentlemen" ransomware group on December 26. Business IT systems, including ERP, email, and the website, were encrypted, partially affecting operations. However, isolated operational technology (OT) networks prevented any impact on power generation, and the national energy system remained unaffected. The company quickly isolated systems, rebuilt on new infrastructure using existing backups, and restored functionality without paying any ransom. This incident highlights growing threats to energy infrastructure worldwide. **Lesson:** Strict network segmentation between IT and OT environments, combined with regular, immutable, and offline backups, is essential for maintaining resilience in critical infrastructure sectors facing increasingly sophisticated ransomware attacks.

continued on page 2...

...continued from cover

2 Ransomware Surge Across Critical Sectors

2025 saw over 4,701 confirmed ransomware incidents globally from January to September, marking a 34% increase compared to the same period in 2024. Approximately half of these attacks targeted essential services, including energy, healthcare, manufacturing, transportation, and finance, underscoring ransomware's evolution into a national security concern. Manufacturing experienced the sharpest rise at 61%, driven by high downtime costs, legacy systems, complex supply chains, and the potential for widespread economic disruption. High-profile cases, such as disruptions to major automotive and component suppliers, highlighted attackers' focus on operational leverage. Despite the surge in volume, ransom payment rates hit historic lows around 23-25%, as more organizations recovered via backups and improved incident response capabilities.

Lesson: Prioritize robust network segmentation to restrict lateral movement by attackers, implement multi-layered defenses, and rigorously test backups through simulated recovery exercises—organizations with reliable, immutable backups paid ransoms in only 23-25% of cases, significantly reducing financial and operational impact while building long-term resilience against evolving threats.

3 Old Vulnerabilities Remain a Top Entry Point

Exploits of known, years-old vulnerabilities continued to drive a substantial portion of breaches in 2025, with unpatched edge devices such as VPNs, firewalls, and remote access gateways serving as prime initial access vectors for ransomware actors. For instance, older FortiGate CVEs—like CVE-2020-12812 (a 5-year-old 2FA bypass flaw) and similar flaws in perimeter devices were frequently chained with newer exploits to gain footholds, often targeting internet-facing systems in critical infrastructure and enterprises. These neglected issues accounted for around 20-32% of successful intrusions (per reports like Verizon DBIR and Sophos), turning otherwise secure infrastructure into easy targets due to delayed patching cycles, resource constraints, overlooked legacy assets, and prolonged exposure windows that allow global scanning. Attackers capitalized on these persistent gaps, automating scans and rapid exploitation to enable initial access, lateral movement, privilege escalation, data exfiltration, and eventual ransomware deployment with minimal effort.

Lesson: Prolonged delays in applying security updates for internet-facing systems create low-hanging fruit for opportunistic attackers; establish automated patch management processes, prioritize high-risk edge devices with exposure assessments, implement virtual patching where possible, and conduct regular vulnerability scans alongside penetration testing to close these persistent gaps before they are weaponized in ransomware campaigns, preventing initial access and downstream disruption while enhancing overall cyber resilience.

FREE REPORT:

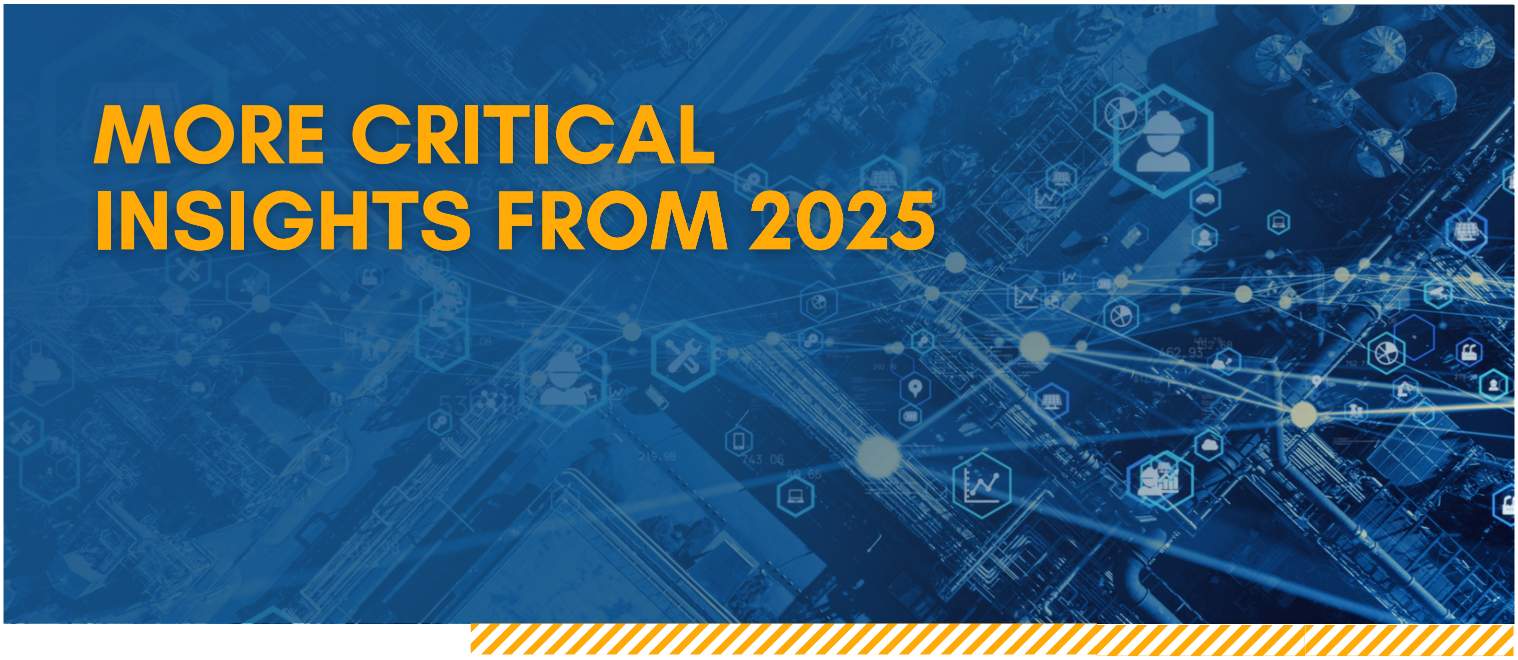
2025 Cybersecurity Year in Review

2025 saw a relentless escalation in cyber threats, with nation-state espionage surges, cascading supply-chain compromises, and AI-amplified attacks exposing critical vulnerabilities across sectors (CSIS, IBM Cost of a Data Breach Report). Black Belt Secure delivers an in-depth analysis of the 12 most impactful global incidents, dominant trends, and actionable 2026 priorities to build proactive resilience—backed by verified disclosures and threat intelligence.

Claim Your FREE Copy Today At: blackbeltsecure.com/reports

DID YOU KNOW?

Basics like segmentation, backups, and patching defeated most 2025 attacks—yet many organizations still overlook them!



MORE CRITICAL INSIGHTS FROM 2025

1 Supply Chain and Third-Party Risks Doubled

Third-party breaches accounted for nearly 30% of all incidents in 2025, doubling from previous years, often stemming from vulnerabilities in vendors, software suppliers, or cloud service misconfigurations. High-profile examples included lingering effects from the MOVEit file transfer exploits that continued to impact organizations well into the year, alongside numerous partner compromises where attackers infiltrated trusted third parties to reach primary targets. This surge highlighted systemic weaknesses in multi-tier supply chains, with over 70% of enterprises reporting at least one material third-party incident, underscoring the need for continuous monitoring, rigorous vendor assessments, and integrated incident response capabilities to mitigate cascading risks across interconnected ecosystems.

Tip: Rigorously vet vendors, monitor shared access, and limit third-party permissions.

2 AI Begins Amplifying Threats

Early AI-powered phishing and deepfakes significantly boosted social engineering success rates, with nearly 83% of phishing emails AI-generated and deepfake attempts reported by 62% of organizations, while ransomware groups used automation and generative tools for faster, more persuasive attacks and polymorphic malware. AI tools enabled highly personalized lures, voice cloning for CEO fraud, and even autonomous intrusions, marking a shift where attackers scaled operations effortlessly.

Lesson: Train teams regularly on emerging tactics like spotting AI-generated content, deploy behavioral detection tools and phishing-resistant MFA, implement AI-driven defenses for anomaly detection, and establish verification protocols for high-risk actions to counter these evolving, convincing threats effectively.

3 Disruption Costs Soar in Key Industries

Healthcare and manufacturing sectors endured severe operational disruptions from ransomware in 2025, with prolonged downtime leading to recovery costs often exceeding millions per incident—averaging over $10 million in U.S. healthcare breaches alone—due to regulatory fines, lost revenue, and patient or production impacts. Critical infrastructure faced heightened targeting, with attacks causing widespread supply chain halts and patient care delays. Organizations with robust preparedness, including regularly tested incident response plans, offline backups, and rapid recovery strategies, experienced significantly lower downtime and financial losses compared to those unprepared. This disparity emphasized the vital role of proactive resilience measures in minimizing the escalating economic and operational toll of ransomware in high-stakes industries.

Tip: Conduct regular tabletop exercises and simulations to refine response strategies, build operational resilience with offline backups and segmented networks, invest in rapid recovery tools, and prioritize vulnerability management alongside comprehensive, tested incident response plans to minimize downtime and protect essential services.

QUICK TIP

Patch Relentlessly 40% of exploited CVEs in 2025 were years old. Automate vulnerability management to close gaps before attackers exploit them.

> ***“2025 proved: Strong fundamentals block most threats. Defend the basics to thrive tomorrow.”***

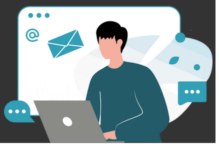
BLACK BELT SECURE

Defend Today, Thrive Tomorrow.

READER CHALLENGE

What's your top resolution for 2026 security? Share and we'll feature the best in February!

Questions? Email **info@blackbeltsecure.com** or visit **blackbeltsecure.com** for a free assessment.



EMERGING THREATS FOR 2026 AND ACTIONABLE TIPS TO START STRONG

AI-Powered Attacks Go Mainstream

Expect autonomous AI agents to revolutionize reconnaissance, enabling adaptive phishing campaigns, hyper-personalized social engineering, and highly convincing deepfakes that spoof executive voices or video identities in real-time. These agentic systems will automate vulnerability scanning and exploit chains at machine speed.
What to Do: Deploy AI-based detection tools for behavioral anomalies, implement multi-layered verification for high-risk actions, and train employees extensively on identifying synthetic media risks through regular simulations.

Identity and Ransomware Evolution

Surge in biometric bypasses, credential attacks, and multi-extortion (leaks + DDoS). Critical infrastructure remains prime target.
What to Do: Enforce zero trust and monitor for anomalies.

Supply Chain, Cloud, and Geopolitical Risks

Third-party and SaaS vendor attacks will accelerate dramatically, while "harvest now, decrypt later" schemes target encrypted data in anticipation of quantum breakthroughs that could render current cryptography obsolete. Nation-state actors will exploit these vectors amid rising geopolitical tensions.
What to Do: Audit vendors and prepare crypto-agility.

NEW YEAR SECURITY TIPS

As we head into 2026, the threat landscape is evolving rapidly with AI-powered attacks, increasingly sophisticated deepfakes, and persistent vulnerabilities in supply chains and human behavior. Strengthening your defenses requires focusing on foundational practices that address both current risks and emerging ones like AI-driven social engineering. Here are key actionable tips to prioritize:

1. Inventory & Patch Everything
Audit assets regularly and prioritize patching internet-facing devices to close exploitable vulnerabilities quickly.

2. Enforce MFA Everywhere
Especially for admins; use app-based or hardware tokens over SMS to prevent unauthorized access effectively.

3. Wearable Tech:
Ensure offline/immutable storage and run full restore tests to guarantee recovery from ransomware or disasters.

4. improving response times.
Run realistic simulations tailored to 2026 threats, including AI-generated voice and video scams.

5.Adopt Zero Trust & Segment Networks
Verify all access continuously and segment networks to limit lateral movement during breaches.