The Danger of Being "Too Small to Matter"

Cydney Howard | Cyber Analyst | CISPOINT
Jacqui Magnes | CEO and Owner | COMSO, Inc. dba CISPOINT
Jeremy Lemke | IT Director | CISPOINT

In the cyber world of 2025, the most disruptive threats no longer require sophisticated zero-day exploits or the backing of nation-state arsenals. More often, they begin with what is mundane and easily overlooked: a reused password, an unlocked laptop, or an unattended browser session. This was precisely the case for a small federal construction contractor who believed their size granted them obscurity. They assumed they were "too small to be a target". A dangerous misconception disproved in devastating fashion. The breach began with a session hijack. Within hours, it spiraled into a full-blown compromise attempt. The attacker leveraged the stolen session to access the contractor's Microsoft 365 account, then quickly moved laterally. The result: credential abuse, brute-force login attempts, and the exposure of hundreds of external contacts. The incident was only prevented from becoming a total compromise through rapid, policy-driven intervention by their Managed Security Service Provider (MSSP).

> *Small businesses are not only on attackers' radars, but they are also a preferred target.*

In the cyber world of 2025, the most disruptive threats no longer require sophisticated zero-day exploits or the backing of nation-state arsenals. More often, they begin with what is mundane and easily overlooked: a reused password, an unlocked laptop, or an unattended browser session. This

was precisely the case for a small federal construction contractor who believed their size granted them obscurity. They assumed they were "too small to be a target". A dangerous misconception disproved in devastating fashion. The breach began with a session hijack. Within hours, it spiraled into a full-blown compromise attempt. The attacker leveraged the stolen session to access the contractor's Microsoft 365 account, then quickly moved laterally. The result: credential abuse, brute-force login attempts, and the exposure of hundreds of external contacts. The incident was only prevented from becoming a total compromise through rapid, policy-driven intervention by their Managed Security Service Provider (MSSP).

According to the 2025 Verizon Data Breach Investigations Report (DBIR), this is hardly an anomaly. Small businesses are not only on attackers' radars, but they are also a preferred target. The report reveals that small organizations experienced 3049 incidents, with 2842 confirmed data disclosures. In stark contrast, large businesses faced just 982 incidents and 751 confirmed disclosures (DBIR, p85). That is over 210% more data breaches in small businesses, despite their limited size and perceived lower value.

In the construction industry specifically in 2024, 145 of 252 breaches involved small contractors, underscoring how deeply vulnerable this sector remains (DBIR, p. 68). The idea that obscurity equates to security has never been more outdated.

THE INCIDENT AND POST-BREACH ESCALATION

On May 1, 2025, the contractor's false sense of security, the comforting lie that they were too small to matter, was violently stripped away, as reality delivered a harsh and calculated blow. An attacker cloned a session token, possibly harvested from an unattended device in a public space such as a coffee shop and gained unauthorized access to their Microsoft 365 environment. From there, they posed as the contractor's accounting department and launched a targeted phishing campaign. A total of 823 email addresses were targeted and exposed, while 283 phishing messages were successfully delivered to external contacts. Once inside, the attacker altered the user's identity and attempted to assign Cloud Device Administrator privileges to a newly registered device within the client's online tenant.

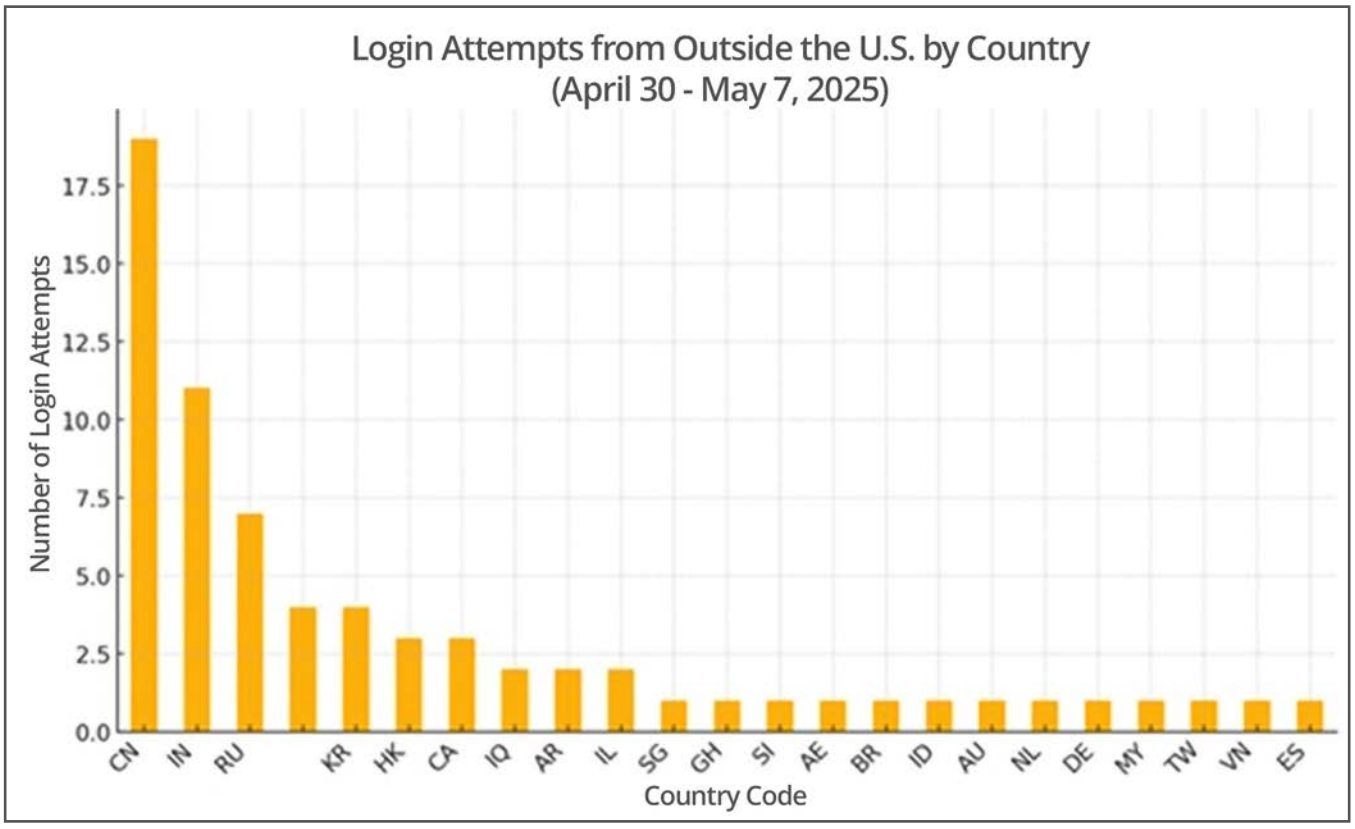
But the intrusion did not end there. Within hours, the threat actor began launching password spray and brute-force attacks on high-value accounts, including those of executive leadership. These attempts spiked by more than 200%, indicating active reconnaissance and a clear focus on privileged identity exploitation.

This sequence closely mirrors national threat trends outlined in the 2025 DBIR. The report states that 88% of breaches involved the use of stolen credentials, and 56% featured brute-force techniques (DBIR, p. 52). In this case, both vectors were present, credentials were compromised, and brute-force tactics followed in quick succession.

This incident did not happen in isolation. It was a textbook example of the very patterns that the Verizon report highlights, cybercriminals systematically exploit under protected small businesses, with construction firms high on the hit list. The only difference between disaster and recovery in this case was preparation—and a swift, capable response by the MSSP's security team.

GEOGRAPHIC SIGN-IN TELEMETRY (APRIL 30 – MAY 7, 2025)

Security Information and Event Management (SIEM) telemetry detected persistent login attempts originating from over thirty foreign locations, including China, India, Russia, and Brazil. These geographies closely aligned with known dark web marketplaces actively trading in compromised credentials, strongly suggesting a coordinated campaign facilitated by access brokers. The telemetry reinforces the likelihood of credential exposure being weaponized at scale. The following chart illustrates the distribution of login activity by country during the attack window:



IMMEDIATE MSSP RESPONSE AND RISK CONTAINMENT

The contractor's MSSP executed a rapid containment strategy within hours of the breach discovery. Their team immediately revoked all active sessions, performed emergency password resets, and enforced Conditional Access rules to restrict sign-ins to U.S.-based geolocations. Additionally, the MSSP

activated 24-hour token expiration policies, notified affected contacts with tailored remediation steps, scanned all endpoints for malware, and completed a cloud-side forensic analysis, which confirmed no sensitive data was exfiltrated. The MSSP also initiated dark web scanning for the client's domain, along with known email addresses and usernames, to identify any exposed credentials. One of the most critical findings was the exposure of the contractor CEO's credentials on dark web forums, both the username and password were fully exposed and unmasked. Using these, the attacker successfully bypassed the CEO's multi-factor authentication (MFA) but was ultimately blocked from full account compromise by geo-restrictions that prevented non-U.S. login attempts. The MSSP collaborated directly with the executive to conduct a secure password reset and reauthorize the MFA device. Following these changes, password spray attempts targeting the CEO account were reduced significantly.

TOP 5 PREVENTATIVE CONTROLS

1. ****Multi-Factor Authentication (MFA)**** – Prevents access via compromised tokens or credentials.
2. ****Conditional Access Policies**** – Geofencing and device health checks block untrusted sign-ins.
3. ****Token Expiry and Session Limits**** – Short-lived sessions limit exposure from stolen sessions.
4. ****Privileged Role Creation Alerts**** – Immediate notification of cloud admin assignments to detect privilege escalation.
5. ****Dark Web Credential Monitoring**** – Identifies exposed accounts for preemptive remediation.

CONCLUSION

This incident highlights the inherent fragility of cloud identity perimeters, particularly in environments lacking Conditional Access enforcement, session lifetime restrictions, privileged access monitoring, and credential hygiene protocols. Without these foundational controls, identities become soft targets, especially in federated environments like Microsoft 365 where access tokens, session persistence, and lateral privilege escalation are routinely exploited by attackers. In the context of federal contracting, such breaches extend far beyond the organization itself, potentially triggering compliance violations under the Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation Supplement (DFARS) the core rulebooks governing cybersecurity and procurement standards for federal and Department of Defense contracts, respectively. Such incidents also risk exposing supply chain dependencies and causing cascading impacts across critical infrastructure sectors.

This small federal contractor came perilously close to a full-scale compromise, averted only by the playbook-driven response from their MSSP, a seasoned IT and cybersecurity team tasked with defending the organization's cloud infrastructure, identity perimeter, and network environment. Their expertly coordinated containment strategy serves as a blueprint for effective response under fire. The long-standing belief that size grants immunity is not only outdated, but also actively dangerous. In the IT and cybersecurity landscape of 2025, one truth is undeniable: small businesses, especially those in high-trust sectors like federal contracting, are no longer on the margins. They are now high-value soft targets for threat actors armed with credential harvesting caches, mass-scanning tools, and password spray kits. Preying on Small and Medium sized Businesses (SMBs) that neglect foundational cybersecurity controls and leave themselves defenseless through negligence, misconfiguration, or willful ignorance.

ABOUT THE AUTHORS

Cydney Howard is the Cyber Analyst at CISPOINT, where she helps clients achieve cybersecurity compliance and resilience through risk assessments, incident response, and regulatory alignment with standards like CMMC, ISO, and PCI. After earning her B.S. in Cybersecurity Analytics and Operations from Penn State in 2022, she served as a contracted Technical Report Assessor for NIST's Cryptographic Module Validation Program, reviewing security policies and validating encryption standards, before joining CISPOINT two years ago. With certifications including CompTIA Security+ and Certified CMMC Professional (CCP), she brings a strong foundation in threat mitigation and small business cybersecurity defense.

Jacqui Magnes is the owner and CEO of COMSO, Inc., an IT services firm supporting the Intelligence Community with cutting-edge solutions in system integration, software development, and training. Since acquiring the company in 2017, she has built a top workplace culture and launched initiatives like the Empowering Women in Technology Scholarship.

In 2023, COMSO acquired CISPOINT, Inc., a Managed Security Service Provider (MSSP) that is a CyberAB Registered Practitioner Organization (RPO) specializing in managed services and CMMC 2.0 compliance for small to mid-sized businesses. Prior to COMSO, Ms. Magnes spent over two decades at Bristol-Myers Squibb in leadership roles across sales, training, federal policy, and market access.

She holds a B.S. in Medical and Research Technology, an M.S. in Marketing Management, and an MBA. Ms. Magnes serves on the Cybersecurity Association Board and the Early College Cyber Advisory Board for Howard County Public School System.

Jeremy Lemke is the IT Director at CISPOINT, bringing over a decade of experience in enterprise IT, networking, and cybersecurity. He began his career in 2011, starting in help desk and network administration roles before progressing into systems and SharePoint administration. Early on, he also helped launch and operate a Wireless Internet Service Provider (WISP), gaining valuable experience in wireless infrastructure and rural connectivity.

Over the course of his career, Jeremy has focused on secure networking, wireless technologies, and identity-driven security. He spent nearly 10 years at Amazon, where he advanced from Support Engineer to Senior Technical Infrastructure Program Manager, leading large-scale infrastructure projects, software development, and security initiatives. In early 2025, he briefly served as a Senior Project Manager for the USDA before joining CISPOINT as IT Director in April 2025.

Jeremy has previously held multiple industry certifications, including CompTIA A+, Network+, Security+, and Linux+, as well as the Cisco Certified Network Associate (CCNA) and AWS Certified Solutions Architect. His professional focus includes identity perimeter defense, cloud and network security architecture, and supporting small businesses and federal contractors in aligning with modern security frameworks such as NIST 800-171 and CMMC.

CISPOINT
MSSP Focused on Rightsizing Your IT