TOP TAKEAWAYS FOR CISOS

Stop Impersonation Attacks Targeting Federal Employees

Federal agencies face a growing wave of impersonation attacks—driven by vendor email compromise, AI-generated deepfakes, and phishing campaigns that exploit public data and trusted relationships. Traditional defenses are failing to keep pace, eroding interagency trust and placing taxpayer dollars at risk.

With the FBI warning of AI-generated messages targeting senior U.S. officials, and procurement processes becoming more streamlined, the stakes for protecting mission-critical communications have never been higher.

The following takeaways highlight how federal CISOs can strengthen defenses with Abnormal's AI-native behavioral detection.

Detect Vendor Email Compromise Before It Reaches the Inbox

- **The Problem**
  Federal agencies are especially vulnerable to vendor email compromise (VEC) due to publicly accessible contract details and frequent communications with suppliers. Attackers blend seamlessly into existing threads, making these emails nearly impossible to spot with signature-based tools.

- **Why It Matters**
  In a global analysis of 1,400+ organizations, Abnormal discovered 44% of read VEC messages are either replied to, forwarded, or both. During the observation period, attackers attempted to steal more than $300 million through VEC.

Abnormal's Solution

Abnormal models normal communication patterns and identifies anomalies in sender behavior, language, and engagement history, stopping malicious vendor messages in real time.

Prepare for the Surge in Phishing Campaigns

- **The Problem**
  Phishing is increasingly being used as the entry point for larger attacks on government agencies—opening the door to business email compromise, vendor email compromise, and account takeover.

- **Why It Matters**
  Between May 2023 and May 2024, phishing attacks on public sector organizations surged 360%, while vendor email compromise attempts against government agencies more than doubled.

Abnormal's Solution

Abnormal applies behavioral AI to detect and block advanced phishing attacks before accounts are compromised or government services are disrupted.

Neutralize AI-Generated Impersonation Attacks

The Problem

Deepfakes and AI-cloned voices are lowering the barrier to convincing impersonation. Affordable kits now allow attackers to spoof federal officials without technical expertise—dramatically increasing both volume and success rates.

Why It Matters

A joint NSA, FBI, and CISA report, Contextualizing Deepfake Threats to Organizations, warns that synthetic media (deepfakes) are accelerating social-engineering threats against organizations and leaders.

Abnormal's Solution

Abnormal's identity- and context-based anomaly detection flags deviations in writing style, target selection, and request patterns, stopping AI-powered deception before employees can engage.

Protect High-Risk Roles from Targeted Social Engineering

The Problem

Procurement officers, auditors, and compliance staff face constant pressure to respond quickly to urgent requests—making them prime targets for social engineering.

Why It Matters

Forrester's Total Economic Impact study found that Abnormal blocked over 500 fraudulent invoices, saving 1,400 hours of investigation time and preventing $1.3 million in potential phishing losses.

Abnormal's Solution

Abnormal uses role-based risk profiling to identify these high-value positions and applies heightened detection thresholds to ensure the most targeted staff are fully protected.

Eliminate Reliance on Employees as the First Line of Defense

The Problem

Legacy defenses place too much burden on staff to spot sophisticated email threats, risking operational paralysis and false positives.

Why It Matters

Forrester's TEI study also found a 278% ROI over three years and ~5,000 SOC hours saved annually from automated triage and investigation.

Abnormal's Solution

Abnormal automates the detection and removal of malicious messages, allowing employees to focus on mission-critical tasks.

Deploy Behavioral AI Protection

The Problem

Attackers are expanding their focus beyond email, exploiting collaboration platforms like Slack and Zoom. Agencies need broad coverage that can be deployed quickly without disrupting workflows.

Why It Matters

AC Transit implemented Abnormal within minutes, immediately detecting and remediating active account takeover and BEC attempts.

Abnormal's Solution

With a single API deployment, Abnormal extends behavioral AI-based detection across multiple cloud applications, protecting agencies wherever work happens.

Looking Ahead

As federal agencies modernize procurement and expand cloud adoption, impersonation and vendor compromise risks will only intensify. Defending against these AI-powered threats requires moving beyond signature-based defenses to proactive, behavior-driven protection.

FedRAMP-authorized solutions like Abnormal AI deliver the visibility and automation needed to detect anomalies, stop attacks before they reach personnel, and free staff to focus on mission success.

Is your agency's security strategy ready for AI-powered deception? Explore how Abnormal AI can protect your agency's communications at scale. **Visit abnormal.ai to learn more.**

Endnotes

- Read, Replied, Compromised Report (Abnormal): 44% employee engagement with vendor email compromise; $300M in attempted fraud (Mar 2024–Mar 2025).
- State and Local Government Email Attack Trends (Abnormal blog): Phishing attacks on public sector surged 360%; vendor email compromise attempts grew 105% (May 2023–May 2024).
- NSA/FBI/CISA – Contextualizing Deepfake Threats to Organizations (CSI): Deepfake and synthetic media attacks increasing; business email compromise schemes costing hundreds of millions.
- Forrester TEI of Abnormal Security: 500+ fraudulent invoices blocked; 1,400 hours saved; $1.3M in losses prevented.
- Ibid: 5,000 SOC hours saved annually; 278% ROI over three years.
- AC Transit Case Study (Abnormal): Deployed Abnormal in minutes for immediate detection and remediation of account takeover and BEC.

Abnormal | iSMG