Government Business Council

ISSUE BRIEF

The Threat Inside

Mitigating Risk from Employee Data Theft

Forcepoint

Data breaches are becoming alarmingly common within the federal government. The 2021 Thales Data Threat Report notes that nearly half of federal government respondents had experienced a data security breach, 47% within the last year.[1] The size and impact of these breaches varied, but the scope demonstrates that cyberattacks are becoming smarter and more rapid as time goes on. Many of these data breaches come from external attacks. However, the threat is sometimes coming from inside the agency itself.

THE BIG PICTURE

Across the federal government, the possibility of data breaches from insider threats remains a significant concern. High-profile events, like the disclosure of classified information from Edward Snowden or the exposure of personal identifiable information (PII) through attacks like those on OPM or through SolarWinds, demonstrate the depth and breadth of damage that data exfiltration can cause.

WHY IT MATTERS

Protecting national data is often seen as a battle with external actors, but headline news over the past few years has shown the dangers posed by data breaches, whether intentionally through a disgruntled employee or through carelessness that allows malicious actors to gain unauthorized access. These data breaches can be dangerous for national security, compromising valuable or classified information and aiding America's adversaries. As the cyber world becomes the next battlefield, ensuring that insider threat risk is managed is crucial to national security.

Data Exfiltration and the Insider Threat

Data exfiltration, also known as data exfil, data leakage, or data theft, is any movement of data that is unauthorized by the agency. The most common types include:

OUTBOUND EMAIL

Sharing data through email, file attachment, or text message

UNAUTHORIZED BEHAVIOR IN THE CLOUD

Either from an unauthorized access point or by a third party, can open up channels for malicious actors to insert code or modify the digital environment

UPLOADS TO EXTERNAL DEVICES

Such as a thumb drive

DOWNLOADS TO UNSECURE DEVICES

Sending to or accessing data on a device, such as a smartphone or laptop, that has not been authorized by the agency

Insider threat is defined as the threat that an employee or contractor will use their authorization, wittingly or unwittingly, to do harm to the security of the United States through espionage, theft, or sabotage. Insider threats can be major sources of loss in critical infrastructure industries, and within the federal government.[2]

The Malicious Insider

Whether for financial gain, as revenge against the organization, or for a competitive advantage, malicious insiders knowingly leverage their authorization to exfiltrate data from their agency.

The federal government has seen some high-profile cases of this in recent years. In 2010, U.S. Army intelligence officer Chelsea Manning exfiltrated 750,000 classified and sensitive defense documents, which were then published on Wikileaks.[3] In 2013, National Security Administration contractor Edward Snowden used his credentials to provide journalists with thousands of top-secret documents about domestic surveillance by the U.S. government.[4] Both incidents had significant impacts on American security and society.

The Negligent Insider

In other cases, the exfiltration is not intentional on the part of the employee. The Department of Homeland Security (DHS) notes that third-party actors can sometimes pose as a government employee by stealing their credentials if employees are careless. Email Account Compromise (EAC), phishing, and vishing, are all common ruses; an ill-advised click can allow malicious actors to infiltrate a government employee's account and enter the secure system. Data can even be shared accidentally, by sending the wrong email to the wrong person. Training on cyber hygiene policy can mitigate these risks to an extent, but they remain potential areas of leakage if other protection protocols are not in place.

Federal Guidance

NATIONAL INSIDER THREAT TASK FORCE

To combat this growing threat, the Federal Bureau of Investigation (FBI) and National Counterintelligence and Security Center (NCSC) joined forces to create the National Insider Threat Task Force (NITTF). The NITTF builds programs that "deter, detect, and mitigate actions by insiders who might represent a threat to national security," focusing on working with agencies and industry partners to identify anomalous activity.[5]

INSIDER THREAT PROGRAMS

Organizations that handle classified information are required under the 2011 Executive Order 13587 to establish insider threat programs for their agency. These programs use mitigation approaches to detect and identify observable and concerning behaviors within their departments. Most of these programs use a "humans-as-sensors" approach — relying on the organization's personnel to notice changes in behavior that might indicate a threat. The National Institute of Standards and Technology (NIST) notes that there is "compelling evidence to show that some types of insider crimes are often preceded by nontechnical behaviors in the workplace (e.g., ongoing patterns of disgruntled behavior and conflicts with coworkers and other colleagues). These precursors can better inform and guide organizational officials in more focused, targeted monitoring efforts."[6]

The Department of Homeland Security has several insider threat programs with different mandates.

The DHS Science and Technology Insider Threat Cybersecurity Program seeks advanced R&D solutions to provide needed capabilities to address six areas: Collect & Analyze, Detect, Deter, Protect, Predict, and React.

The DHS National Intellectual Property Rights Coordination Center connects 23 federal and international partners to defend against global intellectual property theft and enforcement of international trade laws.[7]

The Federal Bureau of Investigation also has several resources, including reporting mechanisms, checklists for reporting espionage or theft of intellectual property, and deterrence strategies for managers.[8]

All insider threat programs are required to protect the individual privacy and civil liberties of employees.[9]

Remote Risk

The sudden and massive shift to telework as a result of the COVID-19 pandemic also radically shifted the way that employees interact with data — and each other. The Intelligence and National Security Alliance (INSA) released a paper in 2021 that found that the impact of the pandemic created both technical and psychological challenges that increase the risk of insider threat. The significant rise in electronic communication increased the likelihood that sensitive data would be mishandled, stored improperly, or exfiltrated without the agency's knowledge. Job security concerns meant that organizations found it more difficult to secure sensitive data and prevent data hoarding by employees. Psychological stressors caused by the pandemic and increased interpersonal tensions are also less noticeable in a remote environment, and traditional insider threat guidance, which often relies on person-to-person interactions to notice anomalous activity or behavior, is not as reliable.[10]

Mitigating the Threat

Many agencies' insider threat programs have protocols for how to detect and defend against the possibility of intentional or unintentional data exfiltration. NIST lays out the essential framework:

Identify: Using tools like network access control can help give IT leadership a sense of who and what are on the network, and where they are.

Protect: Focusing on identity management and control as a means of reducing risk, including increasing zero-trust models in government agencies, can limit or contain the impact of data exfiltration.

Detect: Continuously monitoring networks can quickly detect instances of anomalous activities or cybersecurity events.

Respond: Immediately moving to mitigate, contain, and communicate the data breach can rapidly determine the impact of the attack and begin mitigation with the appropriate stakeholders.

Recover: Building resilience with the organization includes implementing lessons learned and restoring systems affected.

As the federal workforce works in a more dispersed environment, working to mitigate these risks through technology and training is key to detecting and preventing insider threats and data exfiltration before they happen.

Protection Within and Without

A 2021 survey found that 50% of government cybersecurity experts believe that there will be a “Cyber 9/11” in the next decade.[11] This alarming statistic shows just how much the cyber world has become the new battlefield. Government agencies are shoring up their protection against external threats. They must also ensure that the threat isn’t working against them internally as well.

FORCEPOINT’S PERSPECTIVE: Forcepoint offers a variety of solutions to safeguard your data and your organization against insider threats.

Data Protection is a first point of capability to stop information from walking out of your organization.

Forcepoint DLP can provide visibility and control to stop data from leaving your organization across endpoints, 3rd party devices, and applications, from the 9x Gartner Magic quandrant leader.

Forcepoint Data First SASE – is the industry’s only solution uniformly protecting data from the endpoint to cloud, for your organization’s multi-cloud hybrid workforce.

Find Risk at the earliest point of detection, and pivot to investigation with the industry leader in Insider Threat capabilities.

Forcepoint Behavioral Analytics – Combines visibility, analytics and automated control to detect and block anomalous user activity.

Forcepoint Insider Threat Solutions – Collect, analyze, and mitigate against high-risk user behavior, with industry leading visibility into user activities.

Forcepoint User Activity Monitoring – Proactively detects high-risk behaviors and compromised access in the most stringent security environments in the world.

Forcepoint can fortify your existing security solutions to protect your critical data and intellectual property. As your organization pursues Zero Trust methodologies or seeks to strengthen security, the unique offerings can connect siloed systems, establish baselining critical to anomalous behavior detection, rapidly enable security teams, and stop breaches.

About GBC

As GovExec's research division, Government Business Council (GBC) is dedicated to advancing the business of government through analysis, insight, and analytical independence. An extension of GovExec's 50 years of exemplary editorial standards and commitment to the highest ethical values, GBC studies influential decision makers from across government to produce intelligence-based research and analysis.

About Forcepoint

Forcepoint is the human-centric cybersecurity company that understands behavior and adapts security response and enforcement to risk. The Forcepoint Human Point platform delivers Risk-Adaptive Protection to continuously ensure trusted use of critical data and systems. Based in Austin, Texas, Forcepoint protects data and identities for thousands of enterprise and government customers in more than 150 countries.

Endnotes

1. https://www.nextgov.com/ideas/2021/07/state-data-security-federal-government/183869/
2. https://www.dhs.gov/science-and-technology/cybersecurity-insider-threat
3. https://www.reuters.com/article/us-usa-manning/u-s-judge-orders-wikileaks-source-chelsea-manning-released-from-prison-idUSKBN20Z3OT
4. https://www.npr.org/2019/09/19/761918152/exiled-nsa-contractor-edward-snowden-i-haven-t-and-i-won-t-cooperate-with-russia
5. https://www.odni.gov/index.php/ncsc-what-we-do/ncsc-insider-threat
6. https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/control?version=4.0&number=PM-12
7. https://www.cisa.gov/insider-threat-cyber
8. https://www.cisa.gov/insider-threat-cyber
9. https://www.cdse.edu/Portals/124/Documents/student-guides/INT260-guide.pdf
10. https://www.insaonline.org/new-paper-addresses-insider-threat-and-remote-work/
11. https://www.nextgov.com/ideas/2021/09/prioritizing-breach-prevention-secure-government/185766/