DATAPATROL

USE CASE

Insider Threats in Government: A Real-World Use Case Analysis

Every day, government entities manage vast amounts of sensitive metadata, including citizen records, internal memos, investigation files, case evidence, and infrastructure data. This makes the public sector one of the most frequently targeted domains globally, with organizations facing persistent cyber threats, attempts to obtain or disclose restricted information, and sophisticated attacks designed to compromise national security and public trust.

This use case document examines the critical security challenge posed by insider threats within the government sector, specifically focusing on unauthorized data exfiltration methods that bypass traditional security controls.

By examining these incidents, government organizations can identify systemic vulnerabilities, strengthen operational resilience, and stay aligned with national cybersecurity requirements.

Incident Reports Overview

The following section details three real-world security incidents, each involving an insider leveraging physical or digital capture methods to exfiltrate sensitive data.

1

U.S. Airman Leak Through Screenshots and Mobile Phone Photos (Jack Teixeira)

In 2023, a U.S. Air National Guard airman named Jack Teixeira accessed highly classified military intelligence reports and secretly took screenshots and mobile phone photos of the information displayed on his workstation. He later posted these images on Discord, exposing sensitive military assessments to the public. The leak was discovered after the images circulated online, and investigators traced the timestamps and access patterns back to his workstation. In this situation, DataPatrol's dynamic on-screen watermarking would have visibly shown Teixeira's name, device ID, and timestamp on every screen he viewed, making any photographed image immediately traceable.

DataPatrol's anti-screenshot technology would also have blocked attempts to capture the screen using built-in or third-party tools. The incident demonstrates how easily screenshots and mobile photos can bypass traditional security, and how visible watermarks and capture controls serve as powerful deterrents.

2

UK Government Staffer Photographed Confidential COVID Documents

In 2021, a staff member at the UK Cabinet Office secretly took photos of restricted COVID-response briefing slides during an internal meeting. The staffer used a personal mobile phone to capture the content directly from the screen. The leak came to light only because another employee noticed the phone being held up toward the presentation. If the screens had DataPatrol screen watermark on, every slide and document shown during the meeting would have carried a clear, user-linked watermark with the presenter's name, date, and time.

Even if a photo was taken, the image would immediately reveal who captured the content. This incident highlights the importance of visual deterrence in environments where mobile phones cannot always be fully controlled.

3

Pentagon Analyst Leaked Classified Documents Through Unauthorized Printing

In 2018, a Pentagon analyst printed several classified documents and physically removed them from the secure facility. These printed documents were later shared with unauthorized individuals, creating a serious national security breach. The leak was not identified immediately; it was detected only after an internal audit revealed unusual printing activity tied to the employee. In such a case, DataPatrol's print watermarking would have embedded, visible identifiers, such as username, machine name, and timestamp on every printed page, making it impossible to share the documents anonymously. This incident shows how dangerous uncontrolled printing can be inside government organizations.

Comparative Analysis

Similarities Across Incidents

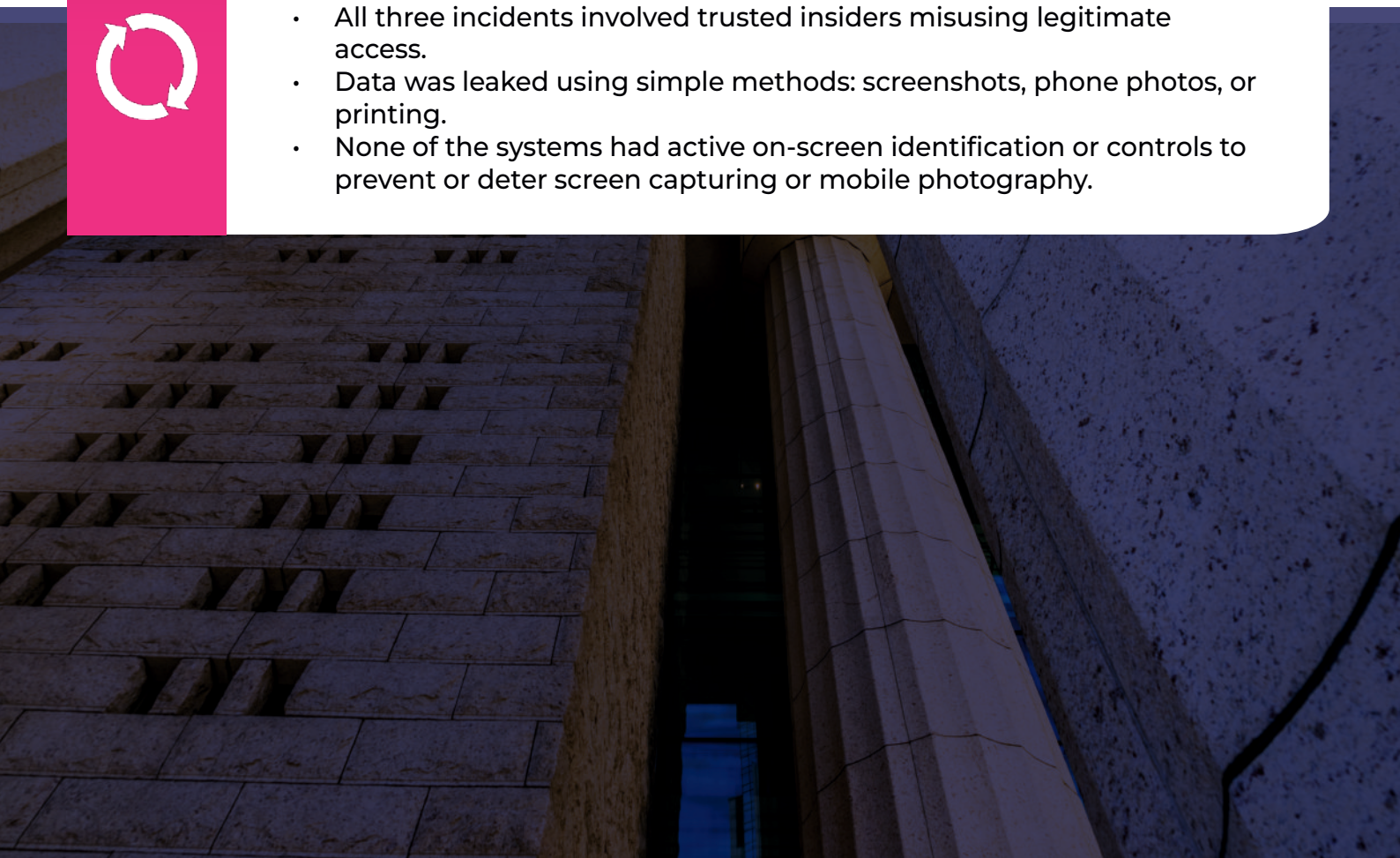
- All three incidents involved trusted insiders misusing legitimate access.
- Data was leaked using simple methods: screenshots, phone photos, or printing.
- None of the systems had active on-screen identification or controls to prevent or deter screen capturing or mobile photography.

Differences Between Incidents

- Two incidents involved digital screen capture: one involved physical printing.
- The UK Government leakage case was observed by a colleague, while the others were discovered only after public leaks.
- Motivations and access methods varied, but the weakness in controls was consistent.

Recurring Vulnerabilities

- All three incidents involved trusted insiders misusing legitimate access.
- Data was leaked using simple methods: screenshots, phone photos, or printing.
- None of the systems had active on-screen identification or controls to prevent or deter screen capturing or mobile photography.



Recommendations & Preventive Measures

To reduce the risk of insider threats and improve data protection across government environments, organizations should consider the following actions:

Use Visible Deterrents

Apply dynamic screen watermark that clearly display the user's identity, device, time, and access details. This discourages mobile phone photography and unauthorized screen captures and ensures any leaked image can be traced immediately.

Secure Document Printing

Add visible watermarks to all printed materials so that sensitive documents remain traceable even after they leave the digital environment. Enforce strict print permissions to limit who can print sensitive content.

Restrict Copy and Capture Functions

Disable screenshot tools, snipping utilities, and clipboard copying. These controls block the most common extraction methods used by insiders.

Monitor Web-Based Access

For internal portals and classified systems accessed through browsers, display user identifiers through WebMark feature. This strengthens accountability and deters sharing of sensitive data.

Strengthen Access Controls

Implement strict role-based access and ensure that users, contractors, and third-party personnel only see information relevant to their responsibilities. Regular access audits help identify risky permissions before they lead to misuse.

Ongoing Training & Awareness

Continuously train staff and contractors on secure handling of sensitive information, insider threat indicators, and the legal consequences of unauthorized disclosure. Clear expectations reduce accidental misuse and discourage intentional violations.

Conclusion

Insider threats in government environments are especially dangerous because they come from individuals who already have legitimate access to sensitive systems. The three real incidents presented here show how easily critical information can be leaked through screenshots, mobile photography, or unauthorized printing, methods that bypass traditional cybersecurity controls. With DataPatrol's dynamic screen watermark, PrtSc prevention and logging and print watermark, governmental organizations can proactively prevent these types of leaks, strengthen accountability, and significantly enhance their overall security posture. DataPatrol not only helps identify leaks after they happen, it makes them far less likely to happen at all.