proofpoint.

WHITE PAPER

Insider Threat Management in Federal Government

The federal government needs Insider Threat Management now more than ever

Introduction

The United States Computer Emergency Response Team (US-CERT), defines "insider threat" as "a current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems." In plain English, the insider threat is a person with malicious intentions who steals information with the intent to do harm to the organization.

Beyond the US-CERT definition, the scope of insider threat expands much further to include any "potential for an individual who has or had authorized access to an organization's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization." A 2016 study by Carnegie Mellon University's (CMU) Software Engineering Institute (SEI) identified that the causal factors are not only similar for both insider cyber sabotage as well as workplace violence, but they progress in much the same pathway.

The Department of Homeland Security (DHS) also notes that insider threats can arise from employee carelessness or policy violations that allow system access to malicious outsiders. A malicious actor can become a credentialed and malicious insider with little more than an ill-advised or ill-intentioned mouse click. Email Account Compromise (EAC) is a common method by which malicious outsiders can masquerade as credentialed insiders.

Table of Contents

The Age of Cyber

Before the Cyber Age, insider threat in the federal context was most commonly manifested as criminal espionage. The names of Jonathan Pollard, Aldrich Ames, and Robert Hanssen notoriously are carved into the annals of federal espionage history. These individuals, and dozens of others, provided information that was sensitive or classified to foreign governments for personal gain and probably a perverse sense of duty. In the specific case of espionage, the intent of the act is to do harm to the United States while benefitting a political or military adversary.

As the Age of Cyber arrived and matured, the insider threat picture changed accordingly. Bradley (now known as Chelsea) Manning downloaded classified information and provided it to WikiLeaks. Edward Snowden, a Central Intelligence Agency employee and subcontractor, grew disillusioned with National Security Agency surveillance programs and leaked the details to journalists for publication. In both of these cases, the actor perceived a wrong that he felt compelled to expose, and the Internet enabled the damage to be widespread.

Cyber-based insider threats now dominate the concerns of many federal agencies. Effective technologies to thwart insider threat have lagged behind the attackers' advanced techniques. Defensive technologies to track and alert on anomalous user behavior, as well as technologies to prevent malicious outsiders from gaining credentialed access, have been slow to emerge and even slower to be adopted.

Use Cases

Understanding the human condition is a foundational element of understanding insider threat. Understanding the human condition in the Federal environment is important to understanding how and why managing insider threat is so important to the well-being of Federal systems and networks, and the protection of sensitive information contained in those systems and networks. While the exfiltration of sensitive data is the underlying concern of Insider Threat Management, in the Federal context it is more about the exfiltration of classified information.

The Employee

Most security professionals are familiar with the basic use cases surrounding the employee as the insider threat. By far the most publicized examples involve a disgruntled inside employee who perceives a greater good from his or her malicious actions. Some examples of the employee use cases are:

Accidental Data Leakage can occur when an employee:

- Misconfigures a system, thus allowing data to be accessed without permission;
- Applies for (or has) excessive privileges to data they should not be authorized to access; or
- Commits human error in transmitting information to the wrong parties. This use case can also be classified as data spillage.

Malicious Activity is the purposeful compromise of internal resources by disgruntled employees or associates looking to take advantage of proprietary data for outside purposes and personal gain.

Social Engineering is the compromise of internal individuals by external actors, which qualifies as both insider and external threat. Social engineering can start with pretexting through the phone (vishing) or email (business email compromise) to get an insider to perform an ill-advised act. Sometimes the social engineering is passive, such as providing malicious links or otherwise obtaining credentials, and other times more aggressive, such as Remote Access Trojans (RATs) and ransomware, which freezes the employee's productivity.

Email Account Compromise is the actual account takeover of an insider account by an external entity, which also qualifies as both insider and external threat. With a compromised account, a malicious actor can access and exfiltrate authorized confidential data, thus bypassing data loss prevention (DLP) alerts.

The Supply Chain

With the advent of recent regulatory changes, the threat landscape must now include robust vendor management reviews – going beyond just 3rd party to even 4th party requirements. These new standards and guidelines apply to two fundamental areas of usage:

3rd-Party Access to internal systems requires enforcement of "least privilege" through role-based access controls, fine-grained entitlement or privilege definitions, robust logging and monitoring of data movement, and logging of all system activities.

Internal access to 3rd-party systems is an exponentially growing area of concern, especially as more organizations outsource their support functions to service providers under the auspices of cloud-based Software-as-a-Service (SaaS) applications. SaaS providers are in effect 3rd parties and must adhere to the same, or better, security rigor required by the organization's internal security controls.

The Remote Worker

With the pandemic crisis of 2020, and its aftermath, organizations within the federal government have been required to refocus their technology and security efforts on a mostly remote workforce. Not only have financial firms had to postpone or abandon infrastructure efforts, quite a few new issues have also emerged:

Virtual Private Networking (VPN): Access to many legacy-based internal applications requires direct private connectivity to the corporate network. The use of VPN as a remote access capability in the past was relegated to simple business continuity and disaster recovery (BC/DR) use cases. However, the recent pandemic has stressed VPN technologies and configurations far beyond their original scope and scale. Because of this increased load, the level of event activity and triggers must be tuned for effective auditing and optimization of the Security Operations Center (SOC) analyst's signal to noise ratio.

Teleconferencing: The ability to communicate with peers and clients is an important part of maintaining good working relationships. Use of this communication medium remotely creates multiple security issues:

- Recording and screen shots from unmitigated sources via smart phones or other devices;
- Lack of control for non-registered, unwanted or hidden participants;
- Lack of control over file- and/or screen-sharing of confidential data.

Telemedicine: Protecting personal information is important. The rise in healthcare costs and organizations' response to keep costs manageable have resulted in an uptick of telemedicine applications. While the merits of telemedicine can be debated, the issue with insider threat is the employee using his or her work computer for engaging in telemedicine, thus possibly storing personal medical information on the agency's endpoint, which inevitably gets backed up to an agency's archive. And although all agencies must comply with the Healthcare Information Portability and Accountability Act (HIPAA), the local storage of an employee's medical information is not something normally in scope for the HR department, and rarely scanned for.

Bring Your Own Device (BYOD): On the flip side of storing personal information on agency resources, is the storage of agency information on personal devices. Many commercial organizations use the BYOD model to keep infrastructure costs low, but most federal agencies do not permit the use of BYOD. However, this does not preclude the use of cloud-based file sharing services. This may be known by many nicknames: "Bring your own …" cloud / data / file system / file share / drop box …. While agencies are required to exercise high levels of scrutiny over cloud-based accounts, having that same level of scrutiny with remote workers is difficult at best.

Home Networks: Although remote workers are connecting securely to their agency's networks via VPN, the actual home network itself may not be secure. Malicious actors may be able to sit on the home network and use man-in-the-middle (MitM) attacks. A 2020 Bitsight study stated that a home network is 3.5 times more likely to have at least one family of malware than a corporate network, and over 25% of home networks have exposed at least one or more services to the internet.[1] This unmitigated attack surface summons an accidental insider threat.

Home Printers: For remote workers, most endpoints have agents that prevent data from being copied to external storage devices, but only prevent access to local printers when the VPN is active. Thus, an insider could theoretically send a confidential document to a printer while connected to VPN knowing the document won't print until the VPN is disconnected. An even smarter insider would be able to access their local printer's storage and pull the document from the print queue.

1 BitSight (2020), *"Identifying Unique Risks of Work from Home Remote Office Networks"*

2 Cummings, Lewellen, McIntire, Moore & Trzeciak (2012), *"Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector,"* CMU SEI, DHS S&T, USSS and CERT Insider Threat Center

Federal-Specific Concerns

Essential Federal Employees

Essential employees are those whose job functions are critical to the mission of an agency, and therefore are not eligible to work from home. Each agency has the discretion to determine which of its employees are essential to the performance of the mission of the agency. In general, law enforcement officials, healthcare providers, safety personnel, and all manner of national security, both military and civilian, are considered essential. Those employees whose work involves the use of classified systems are not eligible to work from home.

Constituency Support Representatives

For example, veterans supported by the Department of Veterans Affairs, or small businesses supported by the Small Business Administration, or federal retirees supported by the Office of Personnel Management, such employees have direct access to client Personally Identifiable Information (PII). The Centers for Medicare and Medicaid Services (CMS) and the Social Security Administration (SSA) are providing much-needed entitlements to eligible citizens. By most standards, this information must be protected according to federal law, such as HIPAA or the Federal Information Security Modernization Act (FISMA).

Healthcare Providers

The Department of Veterans Affairs operates the largest hospital system in the nation. The National Institutes of Health (NIH) is deeply involved in the pandemic crisis, as is the Center for Disease Control (CDC). The Military Health System provides medical care to military personnel and dependents.

Security and Alert Center Operations

Vigilance at 24x7 operations centers is all the more important during a pandemic requiring remote workforce dispersal.

Effectively Managing the Insider Threat

The US-CERT, in collaboration with DHS, researched insider incidents between 2005 and 2012 to answer the question: "What are the observable technical and behavioral precursors of insider fraud and what mitigation strategies should be considered as a result?" Among their top findings were:

1. **The "low and slow" approach accomplished more damage and escaped detection for longer.**
    - Anomaly-driven technology solutions were not only ineffective, but counterproductive, because these long-term bad activities became part of the user baseline.
2. **Insiders' means were not very technically sophisticated.**
    - The lack of sophistication means that existing sensor data could feed into an insider threat program; the magic, of course, is in the behavioral analysis.
3. **Fraud by managers differs substantially from fraud by non-managers by damage and duration.**
    - Managers have the ability to alter business processes, sometimes by manipulating subordinate employees.
    - Non-managers might be customer service representatives who alter accounts or steal customer PII to their benefit.
4. **Most incidents were detected through an audit, customer complaint, or coworker suspicion.**
    - This is an important finding: whereas an external breach has a trail of anomalous breadcrumbs, the insider threat is fueled by sentiment, motivations and mindset – factors not easily detected by technology.

Identification and prevention of insider threats is a relatively new focus for security teams because it requires a different perspective and approach to the problem; hence a skillset not traditionally used in security operations.

Much of the traditional security operations is focused around identifying and mitigating the external threat: from the hacktivist to the nation state. The spending on security tools mostly focuses on intelligence gathering – IoCs (Indicators of Compromise) and identifying the nefarious actor's TTPs (Tactics, Techniques, and Procedures) – and rule-based permissions.

The market for insider threat management tools is sparse and disconnected: managing data loss prevention (DLP), identity and access management (IAM), and user behavior analytics (UBA) are three disparate data points.

Effective management of insider threats requires a focus on a holistic people-centric approach to cybersecurity. The holistic people-centric approach uses technology but frames it in a way to allow orchestrated analysis and dynamic actions.

Sensors collect data points for specific areas, automation coalesces the bulk of sensor data, machine learning analyzes the data against past experiences, artificial intelligence provides a list of possible scenarios based on the analysis and external intel; but in the end, it needs to be a human that makes the final decision for any non-trivial set of possibilities presented.

The human reviewer provides a level of sentiment analysis and context that current AL/ML technologies cannot easily assess (without learning). The human decision maker applies this context to decisions in a way that may not be easily programmable, but which feeds back into the AI/ML components for better future results.

In short, the ideal insider threat management (ITM) program takes input from a variety of technologies, and builds a larger orchestration of the user, their actions and their potential risks.

Executive Order 13587 and the Insider Threat Program Maturity Framework

In October 2011, the President signed Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and Responsible Sharing and Safeguarding of Classified Information." Among its mandates were the creation of an Interagency Insider Threat Task Force to "develop a Government-wide program (insider threat program) for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure, taking into account risk levels, as well as the distinct needs, missions, and system of the individual agencies." A year later, a presidential memorandum established the "National Insider Threat Policy" directed that a program be established for deterring, detecting, and mitigating insider threat; an integrated capability be created to monitor and audit information for insider threat detection and mitigation; that a senior official be designated at each agency to manage and oversee the insider threat program; and that independent assessments be enabled in accordance with E.O. 13587. It also established the charter for the National Insider Threat Task Force (NITTF), co-chaired by the Attorney General and the Director of National Intelligence.

The NITTF published an Insider Threat Program Maturity Framework in November of 2018. The Framework is an aid for advancing Federal agencies' programs beyond minimum standards, and helps agencies' insider threat programs become more proactive, comprehensive, and better postured to deter, detect, and mitigate insider threat risk. The Framework consists of 19 maturity elements, each of which identifies a capability or attribute of an effective insider threat program and provides amplifying information to assist agencies in strengthening their programs. The 19 elements are grouped into the categories of senior official/leadership, program personnel, employee training and awareness, access to information, monitoring user activity, and information integration, analysis, and response. By adopting the Framework, agencies are better equipped to manage and oversee the challenges associated with insider threat on classified systems.

E.O. 13587 and the NITTF deal exclusively with classified systems and information, which is where the Federal government has been harmed by insider threats and where the Federal government has chosen to focus its attention on the magnitude of harm associated with classifies systems and formation. After all, Chelsea Manning, Robert Hanssen, Edward Snowden, and numerous other malicious actors have inflicted harm on the nation as insider threats. However, other Federal agencies in possession of sensitive information, from personally identifiable information (PII) to acquisition sensitive information to internal investigations to policy formulation and many other categories of sensitive information are just as susceptible to insider threats, and just as likely to cause harm to the agency.

Proofpoint ITM

As the leading people-centric ITM solution, Proofpoint's ObserveIT ITM protects against data loss and brand damage involving insiders acting maliciously, negligently, or unknowingly. ObserveIT correlates activity and data movement, empowering security teams to identify user risk, detect insider-led data breaches, and accelerate security incident response.

The primary benefits of a purpose-built ITM platform like ObserveIT include:

1. **Reduce the mean time to detect** (MTTD) of insider breaches by applying threat detection techniques to cross-channel visibility of user activity across endpoint, cloud, and email. Specifically, Proofpoint leverages a Threat Scenario Library of pre-defined risky activity patterns developed in part based on research from US-CERT.
2. **Make insider risk teams more efficient** by enabling analysts to rapidly understand the context around alerts in order to judge whether credible to pursue. Classic UBA solutions are prone to delivering a large number of false positive alerts which consume resources and can result in alert fatigue
3. **Reduce mean time to respond** (MTTR) of insider threats by accelerating and streamlining incident response. With insider incident response including cross functional teams including security, HR, legal, compliance, and line of business managers, teams benefit from the workflow and information sharing utilities within the platform.

In addition to the ObserveIT ITM platform, Proofpoint's people-centric security offerings including information protection, security awareness training, and email account protection provide a powerful toolset to support a holistic insider threat program.

LEARN MORE

For more information, visit **proofpoint.com**.