PLATINUM
BUSINESS SERVICES, LLC

The Threat Within

Platinum Business Services, LLC

Jody Venkatesan, CISA, CISM, CGEIT, CRISC, CDPSE
President & CEO

Email: jvenkatesan@weareplatinum.net
Phone: 301-651-1297
Fax: 301-483-0104
Website: weareplatinum.net

SBA Certified 8(a) HUBZone, Service-Disabled Veteran Owned Small Business (SDVOSB), Veteran-Owned Small Business (VOSB), Small Business (SB), Small Disadvantaged Business (SDB)
TIN/EIN: 26-3462811
Cage Code: 59N47
DUNS: 828491410
UEI: PCNMDK3FLJB9
CIOSP3 NIH CIOSP3 SDVO
(Contract #HHSN316201800030W)
GSA MAS Professional Services #GS00F344CA
GSA MAS IT #GS-35F-0067Y
GSA 8(a) STARS 3 #47QTCB21D0108

The Threat Within

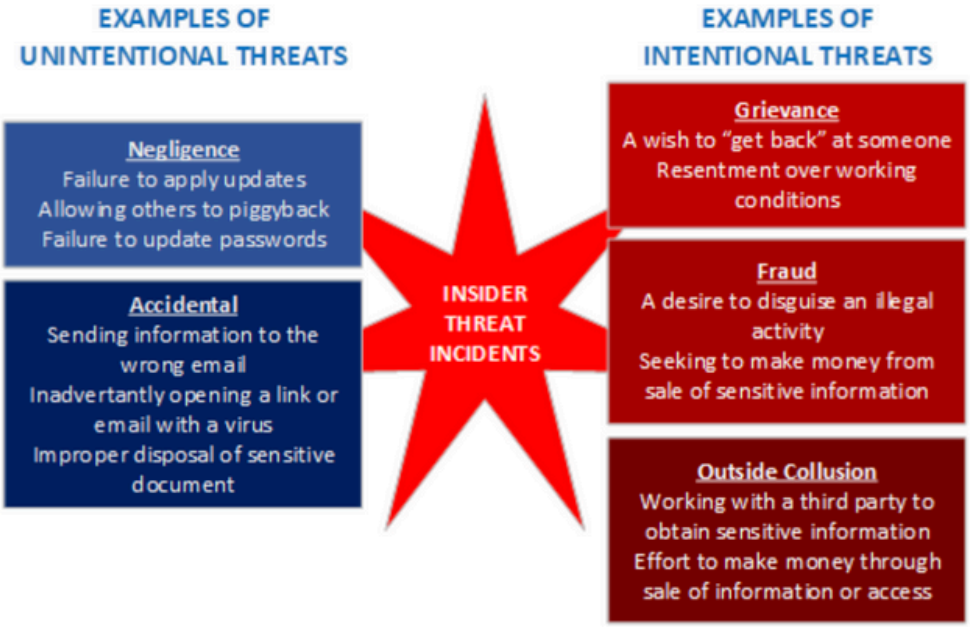
Introduction

Our IT systems are constantly under attack, either intentionally or through carelessness, which results in the creation of open vulnerabilities. Over the past few years, the attacks have increased exponentially. Between 2021 and 2022, attacks increased by 48% worldwide, according to Check Point Research. Government agencies have faced even more assaults, with the US Government cyber-attacks increasing by 57% in the same period. The only government with a more alarming record is the United Kingdom, with an increase of 77%, according to CrowdStrike.

In 2022, the US Government, including the military, experienced an average of 1,661 attacks per organization every week. Fortunately, the majority of these attacks are unsuccessful; however, when one is successful, it can create havoc.

One must consider that ID Watchdog, IBM, and the Cybersecurity and Infrastructure Security Agency (CISA) all estimate that approximately 60% of attacks result from internal threats. Verizon says as much as 82% of attacks result from insiders, at least partly. Effectively addressing and managing internal threats is critical to maintaining the security and integrity of valuable Government data. Regardless of the source, insider threats are real and very costly.

CISA defines an insider threat as an insider with authorized access who, wittingly or not, harms the Information System. These threats happen for various reasons, each requiring a different approach to defend against. Detecting insider threats is not as simple as it may seem at first. To do so, we must look at information cybersecurity people don't typically investigate. But we could pay heavily if we don't look for these symptoms.



The Threat Within

There are several sources for planning and structuring insider threat policies and processes, including:

- Executive Order 13587 – Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information
- DoD Directive 5205.16 – The DoD Insider Threat Program
- Committee on National Security Directive 504 (CNSSD 504) Directive on Protecting National Security Systems from Insider Threat, Annex B,
- CISA Insider Threat Mitigation Guide

What they all have in common is a recognition that insider threat is fundamentally different from outsider threat, particularly in the need to consider, understand, and respond to human factors. Many insider threats result from human conditions, such as stress, negligence, or carelessness. The most important method for dealing with these causes is to provide a robust management approach that creates a safe environment, attends to people's emotional needs, protects individuals' privacy, and creates an environment of awareness of individuals and the importance of security.

Analysis of the environment and organizational structure is our starting point for developing an Insider Threat Strategy. Platinum reviews, documents, and prioritizes all potential insider threat situations. We recognize that awareness of a threat situation may come from a wide variety of sources, including but not limited to allegations from other staff members, attempts to perform unauthorized access within the IT system, or attempts to insert unauthorized code into the IT system, as typical examples of the types of threshold events. Our approach is designed to identify all potential sources of internal threats within the organization and take steps to minimize the threats.

Unintentional Threats

The successful Insider Threat Strategy begins with a sound, robust staff management approach that establishes a clear understanding of the policies, processes, and standards implemented to avoid unintentional insider risks from either negligence or accidents. There are also some steps that the IT and cybersecurity teams can take to further protect from unintentional threats. The implementation and enforcement of Zero-Based Architecture, with its rigorous approach to granting access permissions, can prevent people from accessing information for which they have no permission. Furthermore, enforced time-outs protect against the unauthorized use of a machine. Based on the environment, other steps may be taken to maintain staff awareness and prevent unintentional harm.

Platinum looks for symptoms of carelessness and works to take steps to prevent them. Simple examples of carelessness include:

- Leaving doors unlocked
- Leaving computers on without password-protected screen savers
- Introducing unauthorized software to the system, such as games or music videos.

The Threat Within

These are just examples of the clues our team looks for when developing a comprehensive strategy. We look for means to automate detection/protection where possible. And we keep looking for other risks or threats and ways to prevent them.

Intentional Threats

Staff and management must also look for signs that may indicate intentional threats. This may include various indicators, such as a perceived grievance, financial pressure or distress, or unrestrained ambition. Some may even think they are taking action to protect the public interest, such as the security leaks that Edward Snowden created at the NSA.

The intentional insider is often synonymously referenced as a "malicious insider." Intentional threats are actions to harm an organization for personal benefit or to act on a grievance. For example, many insiders are motivated to "get even" due to a perceived lack of recognition (e.g., promotion, bonuses, desirable travel) or termination. Their actions can include leaking sensitive information, harassing associates, sabotaging equipment, perpetrating violence, or stealing proprietary data or intellectual property in the false hope of advancing their careers. They include:

- Espionage
- Terrorism
- Unauthorized disclosure of information
- Corruption, including participation in transnational organized crime
- Sabotage
- Workplace violence
- Intentional or unintentional loss or degradation of departmental resources or capabilities

We also look for:

- **Collusive Threats** – A subset of malicious insider threats is called collusive threats, where one or more insiders collaborate with an external threat actor to compromise an organization. These incidents frequently involve cybercriminals recruiting an insider or several insiders to enable fraud, intellectual property theft, espionage, or a combination of the three.
- **Third-Party Threats** – Additionally, third-party threats are typically contractors or vendors who are not formal members of an organization but have been granted some level of access to facilities, systems, networks, or people to complete their work. These threats may be direct or indirect.

We use the CISA Framework (Defining the Threat, Detecting and Identifying the Threat, Assessing the Threat, and Managing the Threat) coupled with Zero Trust Architecture to address the multiple possible sources of threats.

So first, Platinum looks for symptoms of carelessness, such as:

- Leaving doors unlocked
- Leaving computers on without password-protected screen savers
- Introducing unauthorized software to the system, such as games or music videos.

Preventing Incidents and Responding When They Do Happen

We then look for signs of intent, indicators of possible malicious attack, such as:

- Attempting to enter into areas they don't have a reason to be in
- Carrying or leaving with unusual packages or items
- Attempting to access programs or data outside their user group permissions.

Insider threat prevention requires training and modifying human behavior as much or more than looking at IT information. The Platinum team includes individuals with the skills to provide training and awareness for your personnel so they are trained not to be careless and taught to look for and report suspicious behavior – and are reminded regularly.

We also use existing IT tools, analyzed for different information, to detect potential insider threat behavior – and, in some cases, prevent it. In addition to taking suspicious activity reports from peoples' peers and supervisors seriously, we use system tools to look for indicators. This includes activities such as:

- Reviews of physical access logs to identify individuals attempting to enter areas where they have no logical reason to visit
- Reviews of IT system access logs to determine if they are attempting to access systems or data they do not usually use
- Review of configuration management validation scans to ensure no unauthorized software has been introduced to the system
- Review of internal firewall reports to look for attempts to access unauthorized data
- Review of personal communications (e.g., email) with keyword indicators for risks to identify attempts to pass unauthorized information
- Review of personal communications with key IP addresses for suspicious actors to determine if the users have communicated with a known source of phishing or if they are communicating with a known hacker.

These are just a few steps Platinum takes to monitor and prevent insider threats from affecting the integrity of your systems. Platinum works collaboratively with your staff to define all key areas that may be used to detect inappropriate activity, conduct forensics to identify the suspicious actor and implement methods for monitoring trends in physical behaviors and IT system indicators. As we develop manual and automated processes customized to your environment to capture this data and identify potential weaknesses within the environment, we will also share this information with other cybersecurity groups working on this critical issue. In this way, we stay current on the ever-evolving methods used by malicious actors and the practical steps to detect them and prevent an unfortunate event.

Analysis of the RIGHT user activities is critical. As an IT organization, it is natural to look at what can be done using the tools within the IT system. We are cognizant of the need to turn these tools to analysis of the CORRECT data to be effective. For example, we will work with your staff to evaluate the viability of conducting analytics (e.g., trend analysis, variance analysis) of data such as entry logs, electronic key access records, and other indicators of behavior-related physical access variations.

Preventing Incidents and Responding When They Do Happen

Similarly, we will evaluate the viability of assessing a variety of other data sets, whether it is transaction logs for evidence of suspicious IP addresses or attempts to access unauthorized data, emails for keywords, or scans for unauthorized applications, codes, or devices within the network.

Our team brings the capabilities of IT systems, database analysis, and analytics to evaluate insider threats that various IT and behavioral issues may indicate. Our team will look at methods for tracking and assessing information from threat reports, from non-traditionally IT databases (e.g., door access logs), and analysis of traditional IT sources. We have staff with analytics and IT/data analysis skills to support this three-pronged approach to insider threat analysis. Let us help you protect the integrity of your systems.