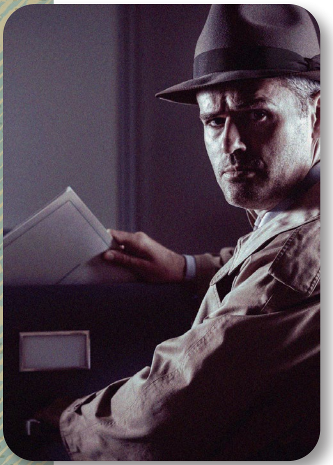
Insider **Threats**

what **you** need to **know**

Office of Information Technology
Division of Information Security
JANUARY 2023

What is an Insider Threat?



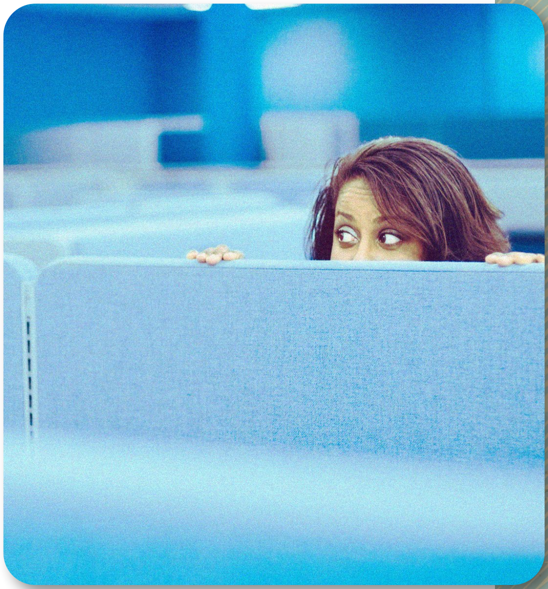
While we often think of an insider threat as someone who maliciously harms the organization, there is more to it than that. It turns out that any person with past or present authorization to access or learn about IHS operations is an insider and poses a threat, either intentionally, accidentally, or negligently.

This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.

Let's define an insider in greater detail before we talk about threats.

What is an Insider?

An insider is any person with prior or current authorized access or knowledge of IHS facilities, data, or any other organizational asset, including personnel. Initially, IHS uses background check procedures to establish trust with insiders. Once onboarded and even after separation, insiders maintain that trust by adhering to IHS data, infrastructure, and facility security policies.

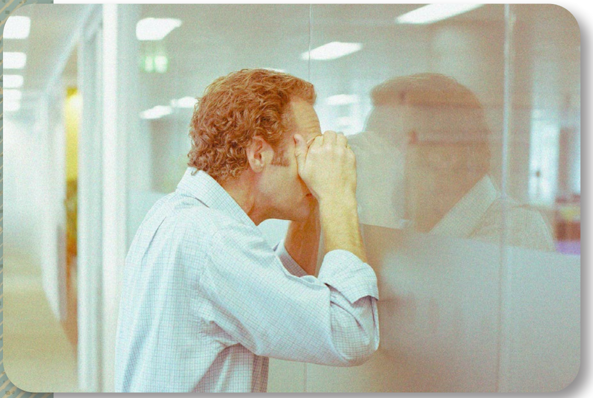


Insiders include the following:

- Employees, business partners, vendors, and those to whom the organization has given sensitive information and access
- Any person with a PIV card authorizing regular or continuous access
- A person with an IHS-owned device or IHS network access
- An employee with knowledge about IHS inner workings, including strategies, strengths, and weaknesses
- IHS employees with access to sensitive Personally Identifiable Information (PII) or Protected Health Information (PHI). This can include medical care providers, supervisors, or human resources staff

What is an Insider Threat?

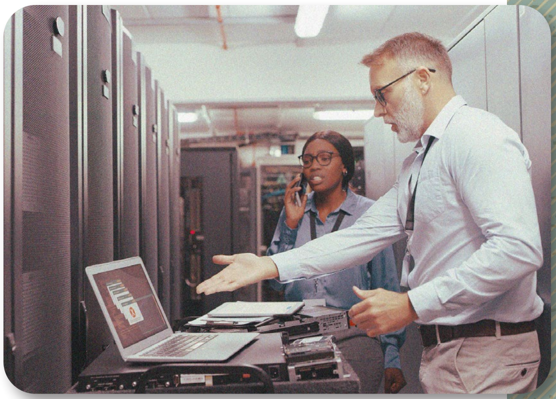
An insider threat is the potential for an authorized person to use their knowledge and access to harm the organization. It is a common misconception that an insider threat is an employee with a personal motive to take malicious action. In reality, every single person with knowledge and access poses a threat to the agency either wittingly or unwittingly.



Types of Insider Threats

An insider threat can manifest in unintentional or intentional action resulting in harm to people, data, or other assets. Harm does not necessarily mean that something noticeably impactful has happened. Instead, harm is any violation of data confidentiality, integrity, or availability. Let's take a look at both kinds of threats.

Unintentional Threats



Unintentional threats fall under one of two categories: negligent or accidental. The difference is subtle, but important.

Negligent insider threats are aware of security policies but intentionally ignore them, increasing agency risk; accidental insider threats mistakenly increase agency risk, usually through inattentiveness. Some examples of negligence include not completing required security training; failing to secure government-furnished equipment; a vendor not complying with security agreements; or sharing access credentials with others.

Examples of accidental insider threats include sending sensitive information to the wrong recipient; falling victim to a social engineering attack; poor password management; or forgetting to lock your computer when away from your desk. These users unwittingly expose enterprise systems to attack. These accidental or careless insiders are sometimes called pawns.

Pawns are authorized users manipulated into unintentionally acting maliciously, often through social engineering techniques such as spear phishing. These unintentional acts could include downloading malware to their computer or disclosing sensitive information to an impostor.

Intentional Threats

Intentional threats are the ones we usually think of when we hear ‘insider threat.’ This threat is determined to cause harm, which may be measurable in dollars or data lost; or the damage may be impossible to compute like resulting negative publicity or diminished employee morale. Intentional insiders can also collude with external threat actors to hurt IHS.

One especially dangerous intentional threat is the lone wolf. Lone wolves operate entirely independently and act without external manipulation or influence. They can be especially dangerous because they often have privileged system access such as database administrators.

Another is the mole. A mole is an outsider but one who has gained insider access to the organization’s systems. They may pose as a vendor, partner, contractor, or employee, thereby obtaining privileged, but unqualified, authorization.

Not Just a Computer Threat

Insider threats are not only a computer or espionage issue; they can cause physical harm to others through acts of violence, sabotage, or theft. Identifying suspicious behaviors can limit the damage these persons can do, or keep them from doing harm at all. Such behaviors can include:

- Repeated violations of security policies and procedures
- Interest in Agency operations outside the scope of responsibility
- Attempts to access data without authorization or send data to unauthorized persons
- Veiled or blatant remarks about attacking the Agency or Agency personnel

Our Responsibility

We are responsible for protecting the populations we serve and their information, so it is important to report any suspicions that someone will use, or has used, their knowledge or access to affect IHS facilities, data, infrastructure, or people negatively. To report a possible Insider Threat, email the Insider Threat Lead at IHSInsiderThreat@ihs.gov. You can report cybersecurity incidents to the IHS Cybersecurity Incident Response Team at incident@ihs.gov. You may also discuss concerns with your supervisor or someone else in your chain of command.

In case of a threat to human safety, please call 911.

Please contact cybersecurity@ihs.gov with any questions or comments about this newsletter.