WHITE PAPER
OCTOBER 2015

IT@INTEL

A Field Guide to Insider Threat

Intel IT hopes enterprises can use our Insider Threat Field Guide to understand and prioritize insider threats to further improve enterprise security strategies.

Executive Overview

One of the most serious security challenges facing enterprises today is that of insider threat. However, many enterprises do not fully understand the scope of the problem and until recently, there has been a lack of tools to respond to this challenge.

Using the Threat Agent Library developed by Intel IT, study of published material, and discussions with other enterprises, we have created an Insider Threat Field Guide that identifies 60 most likely insider threat attack vectors. In particular, the guide does the following:

- Facilitates clear and consistent sharing of information, both internally and externally.
- Enables more effective security strategies and faster responses by risk managers, policymakers, auditors, and security specialists.

We believe enterprises can use our field guide to better understand insider threats and take steps to minimize the associated risks.

Tim Casey
Cyber Risk Systems Architect
Intel IT, Information Security Group

Contents

Contributors

Bjoern Almgren
Privacy Analyst, Intel IT

Martin Martinez
Mergers and Acquisition Senior Security Manager, Intel IT

Matthew Rosenquist
Cybersecurity Strategist, Intel IT

David Ulmer
Manufacturing Information Security Manager, Intel IT

Business Challenge

Most enterprise security teams are aware of "insider threats." However, they often use a narrow definition of the term, which can result in inadequate security for the enterprise. For example, if the enterprise focuses only on a few types of insider threats, such as fraud and damage caused by disgruntled workers, they may overlook other more significant types of threats that present bigger consequences.

Many enterprises also do not differentiate between an "insider threat," which is a potential for harm, and an "insider event," which is the occurrence of a malicious or harmful activity. Such confusion complicates an enterprise's ability to assess and communicate the actual risks.

While no enterprise can protect against every possible scenario, it is possible to prioritize, in order to proactively protect against the most likely or most damaging threats in a given environment. To do this, an enterprise needs standard definitions of terms and an appropriate analysis of insider threat agents and activities.

Solution

To address the problem of insider threats, Intel IT recently used our Threat Agent Library and internally developed threat analysis methods to create the Insider Threat Field Guide (see Figure 1). We complemented our internal resources with information from leading research organizations such as the CERT's Insider Threat Center[1]. We then further researched data from a wide array of case histories, insider event databases, and law enforcement records to identify the most common insider threat agents along with their primary means of attack.

[1] See www.cert.org/insider-threat.

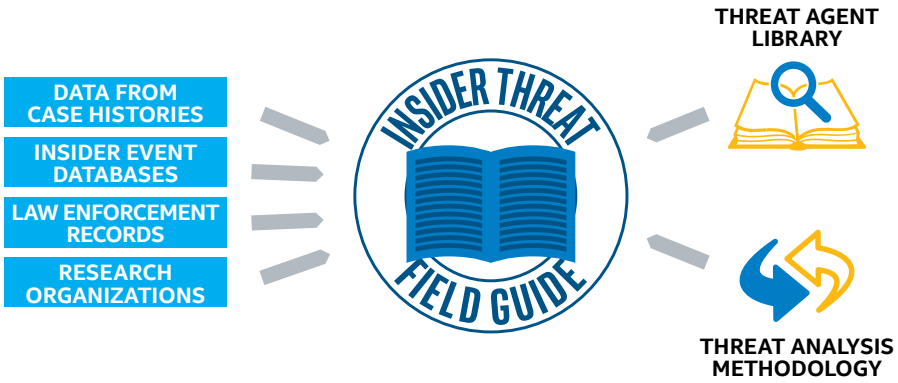

Figure 1. The Insider Threat Field Guide is a unique security asset that can help identify the most common insider threat agents along with their primary means of attack. We based the information in the field guide on information from many internal and external sources.

"When you say insider threat in the financial sector, people typically think of fraud or theft of customer data. In other sectors, they tend to think of theft of trade secrets or confidential information, and often they think that those threats are mitigated by the Data Loss Prevention group.

I love the Insider Threat Field Guide because it illustrates how complex insider threat really is. It drives home the point that insider threat is about people, not just technology. This guide can be used by any organization to prioritize its own insider threats and to develop a corresponding roadmap for creating and maturing its own program for managing insider risk."

Dawn Cappelli, *Director, Insider Risk Management, Rockwell Automation*

We developed threat agent "caricatures" to help describe threats in a more relatable language. For example, "A Spy can electronically impersonate a coworker to access her controlled information" is more easily understood than a technical description like "The threat moves laterally through the network until admin privileges are established."

Additionally, we used a formal vocabulary to define insider threat, insider event, and insider risk. This vocabulary again draws on the important foundational work of CERT and other organizations, and intersects with the National Institute of Standards and Technology's emerging cyber risk management guidance.[2] Our definitions cover all dimensions of threat—cyber and physical, accidental and intentional, benign and malicious. These definitions are as follows:

- **Insider threat.** The *potential* for a current or former employee, contractor, or business partner to accidentally or maliciously misuse their trusted insider access to harm the organization's employees and customers, assets, partners, or reputation.
- **Insider event.** The *realization* of an insider threat, encompassing any activity from the first deliberate act through the final outcome.
- **Insider risk.** The *level of exposure* to harm from insiders, factoring in insider threat, the vulnerability to that threat, and the consequences of any resulting event.

Just as a field guide for birds helps narrow down the species by identifying characteristics, location, and so on, our Insider Threat Field Guide helps identify the insider threat agents an enterprise is most likely to encounter. Enterprises can use that identification to do the following (see Figure 2):

- Refine security controls to focus on the most likely threat scenarios.
- Educate management about insider threats to improve awareness and support.
- Identify security gaps that should be addressed.
- Optimize their limited resources, such as people, time, and money.

[2] For more information on the National Institute of Standards and Technology's Cybersecurity Framework, visit www.nist.gov/cyberframework.

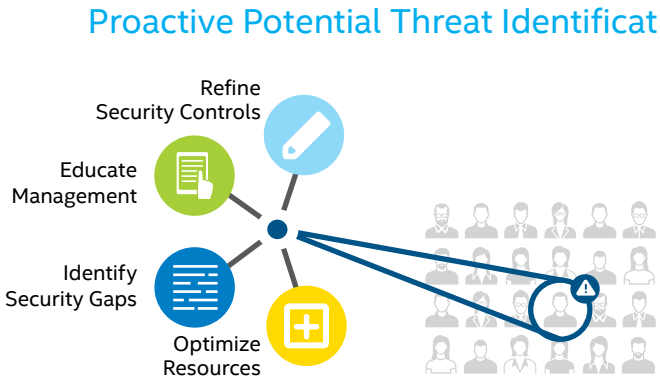

Figure 2. The Insider Threat Field Guide helps identify the insider threat agents an enterprise is most likely to encounter. Using this information, enterprises can bolster their defenses against insider attack.

"The Insider Threat Field Guide is a foundational element of Intel's insider risk management strategy. The Guide enables a common understanding of insider threat across the internal security community. In addition, the Guide enables defenders to have a structured dialogue with management and decision makers regarding the insider threat."

Brian Willis, *Manager, Threat Intelligence and Infrastructure Protection, Intel IT Information Security, Intel Corporation*

Insider Threat Field Guide Matrix

The Insider Threat Field Guide takes the form of a matrix, shown in Table 1. It maps the major insider threat agents (people) to the ways in which insiders can negatively impact an organization (event types). A definition of each insider threat agent is given in Table 2. More information about event types, which can take various forms and have varied types and levels of impact on the enterprise, is provided in the Insider Event Types section.

Insider threat agents can also include individuals who at one time worked for the enterprise and may have sold or given insider information to hostile entities. For this type of agent, we categorized the individual by the organization to whom they gave the information. For example, an insider who left the enterprise and sold proprietary information to a competitor would be classified as a Competitor threat agent in this model.

The field guide includes the following types of intent:

- **Nonhostile agents** have no ill will toward the enterprise; the harm they do is accidental or incidental. While nonhostile agents may have benign intentions, their actions may still cause harm to the enterprise, so it is equally important to understand and manage these issues.
- **Hostile agents** do have ill will toward the enterprise and intend to do harm.
- **Agents with "unknown" intent** can be either hostile or nonhostile, depending on the individual agent and the circumstances.

While any individual could potentially perform any event type shown in the matrix, our extensive research has identified the 60 most likely activities that may be performed by each class of insider threat agent, as indicated by the X's in Table 1. In addition to the field guide, we create personas to help our security team better understand the threat and further improve our defenses. These personas are examples of how each event type might happen for a particular insider threat agent (examples are provided in the Using Personas section).

No model can completely predict human behavior. Therefore, it is possible that actual individuals who pose a threat to the enterprise may not fall neatly into any one of these categories. Similarly, individuals who appear to fit a particular category may act in ways that this model does not predict. However, we believe our field guide provides significant benefit by providing a useful framework from which to view and help manage the entire insider threat landscape.

Table 1. Insider Threat Field Guide Matrix

		EVENT TYPE								
		ACCIDENTAL LEAK	ESPIONAGE	FINANCIAL FRAUD	MISUSE	OPPORTUNISTIC DATA THEFT	PHYSICAL THEFT	PRODUCT ALTERATION	SABOTAGE	VIOLENCE
INTENT	**Nonhostile**									
	Reckless Insider	X			X			X		
	Untrained/Distracted Insider	X			X			X		
	Outward Sympathizer	X			X					
	Unknown (nonhostile or hostile)									
	Supplier	X	X	X	X	X		X		
	Partner	X	X	X	X	X		X		
	Hostile									
	Irrational Individual	X			X		X		X	X
	Thief		X	X		X	X			
	Disgruntled Insider	X	X	X	X	X	X	X	X	X
	Activist		X		X	X	X	X	X	
	Terrorist						X		X	X
	Organized Crime		X	X		X	X	X		
	Competitor		X			X		X	X	
	Nation State		X			X		X	X	

Table 2. Threat Agent Definitions

THREAT AGENT TYPE	DEFINITION
Reckless Insider	Person who knowingly and deliberately circumvents safeguards for expediency but does not intend harm or serious consequences
Untrained/Distracted Insider	Person with harmless intent who inadvertently misuses systems or safeguards
Outward Sympathizer	Person who knowingly misuses the enterprise's systems to attack others in support of a cause external to the enterprise, but with harmless intent to the enterprise itself
Supplier	Business partner who seeks inside information for business advantage over its own competitors (that is, other suppliers)
Partner	Business partner with whom the enterprise has voluntarily shared sensitive data for collaborative efforts and who may either accidentally or deliberately expose that information
Irrational Individual	Person acting with illogical purpose and behavior
Thief	Opportunistic person with profit motive
Disgruntled Insider	Unhappy current or former insider with intent to harm the enterprise, industry, or fellow insider
Activist	Highly motivated supporter of a cause who does not engage in physical violence
Terrorist	Person who relies on physical violence or extreme acts to support a socio-political agenda
Organized Crime	Crime syndicate with significant resources and attack skills
Competitor	Business adversary who competes for customers, revenues, public exposure, or resources
Nation State	State-sponsored attacker with significant resources, and able to affect a major disruption to even national scale

Insider Event Types

Our research helped us identify the nine primary categories of harmful insider activity for inclusion in the field guide. These are described below.

Accidental Leak

Unintentional leakage of intellectual property or data on the part of the insider; however, it still harms the enterprise. Leaks may be caused by carelessness or unfamiliarity with or circumvention of information security protocols. Examples include:

- Unwittingly providing information in a phishing attack
- Talking about sensitive matters to persons without appropriate clearance
- Leaving sensitive documents or computing devices accessible to others
- Posting confidential details to social media sites

Misuse

Broadly encompasses any insider use of enterprise resources in ways that bypass or ignore safety or security protocols; violate enterprise policies; are unrelated to the insider's job; are illegal; or otherwise potentially harm the enterprise, intentionally or unintentionally. Examples include:

- Using an enterprise server inappropriately for personal gain
- Using the enterprise printer to print hundreds of wedding invitations
- Downloading pirated movies onto an enterprise laptop

Fraud

Using insider access to divert enterprise financial resources to one's self. In short, stealing money from the company. Examples include:

- Influencing others to use a supplier with whom the insider has an existing financial relationship
- Expense report fraud
- Use of controlled, non-public information for insider trading

Physical Theft

Stealing physical property, as opposed to intangibles such as money (see Fraud) or intellectual property (see Opportunistic Data Theft and Espionage). Examples include:

- Stealing valuable inventory
- "Borrowing" a laptop or office projector

Violence

Physical harm to others. This category ranges from minor incidents to more serious scenarios. Examples include:

- Violence or the threat of violence used to coerce employees
- Angry employee punching his/her supervisor

The Evolution of Intel's Threat Agent Analysis Methods

In 2007, Intel IT published a unique standardized Threat Agent Library—a reference document describing the types of human agents that pose threats to organizational assets. The Threat Agent Library helps risk managers identify relevant threat agents quickly and accurately, and to understand their importance.

Originally, the library consisted of 22 archetypes defined using eight descriptive parameters. The archetypes represent external and internal threat agents ranging from industrial spies to untrained employees. The library standardizes threat agent definitions and presents information objectively.

A few years later, we developed a Threat Agent Risk Assessment methodology that distills the immense number of possible information security events into a digest of only those exposures most likely to occur. This methodology identifies threat agents that are pursuing objectives which are reasonably attainable and could cause harm to Intel.

Because information security is an ever-changing field, we recently refined the Threat Agent Library by adding the Motivation parameter, which identifies the driver—be it an emotion or the pursuit of supremacy or material gain—that causes the threat agent to commit harmful acts. Understanding these drivers is important to help qualify the nature of the expected harmful action.

Nine Primary Insider Event Type Categories

- Accidental Leak
- Misuse
- Fraud
- Physical Theft
- Violence
- Sabotage
- Product Alteration
- Opportunistic Data Theft
- Espionage

Sabotage

Intentional destruction of enterprise resources so they can't be used. Sabotage can include both physical and logical damage. Examples include:

- Breaking a component in a critical machine
- Contaminating a clean room
- Installing a logic bomb in enterprise software

Product Alteration

The accidental or deliberate introduction of malware or a cybersecurity vulnerability into a product an enterprise develops. It may be installed in either hardware or software. Examples include:

- Misconfiguring products to cause failure
- Inserting malware in software drivers downloadable from the company website

Opportunistic Data Theft

Stealing information or intellectual property, such as software or business data. The threat agent takes unprotected information and copies it (the enterprise retains access to the data) or physically retains it (the enterprise loses access to the data). This is similar to espionage, but the scope, sophistication, and motivation are different. Examples include:

- Prior to leaving the enterprise, an employee downloads design files to take to a new employer

Espionage

Systematic and targeted extraction of corporate information by a trusted insider that gives the attacker a strategic economic, military, or public relations advantage. Espionage may bring to mind sophisticated government spies, but most of the people who engage in corporate espionage are average insiders who are engaged by an outside organization to complete a relatively specific task. Examples include:

- An employee sells photographs of a product prototype to an industry magazine
- A person routinely sends specific, confidential personnel files to a nation state handler

Insider Threat Agent Profiles

When developing insider threat agent profiles, we first defined each class of agent, including associated characteristics. To help our security team understand the personality types, each profile is typically a brief dossier that describes the agent's motivation, followed by a list of event types the agent is likely to perform. After completing the profiles, security teams can concentrate on protecting against the higher risk profiles likely to affect a particular asset. Figure 3 gives three examples of insider threat agent profiles we have developed.

Using Personas

We often use personas—like the three shown here—to help us easily envision and communicate about insider threats. These personas transform abstract concepts into realistic scenarios, which security professionals can then use to help describe potential insider events better and improve their defenses. The following sample personas merely provide concrete illustrations of insider threat scenarios by combining the threat agent type with a specific situation that leads to an insider event; they are not part of the field guide itself. Enterprises using the Insider Threat Field Guide should develop their own, tailored set of personas.

- **Scenario 1:** Accidental leak by a Distracted Insider. Anya's department has been hit hard with layoffs, and the remaining employees are now scrambling to take on new duties, sometimes without adequate preparation or training. Overwhelmed by the new tasks, Anya posts internal specification documents to her employer's supplier information web site, hoping to preemptively answer supplier questions, not realizing the site is publicly accessible. Now, enterprise intellectual property is widely exposed and can be indexed by Internet search engines.
- **Scenario 2:** Misuse by an Outward Sympathizer. Jon is an immigrant from a region experiencing frequent violent conflicts. His family still lives in this region. When a large conflict flares up, he wants to protect his family, but the distance prevents direct involvement. Instead, he installs a hacker toolkit onto an enterprise server and uses it to attack the opposing country. That country detects the attack and not only retaliates with its own cyberattack but also seizes Jon's employer's local offices.
- **Scenario 3:** Physical theft by a member of Organized Crime. Tom has run up large gambling debts with a local crime syndicate and cannot pay them back. To erase the debt, he agrees to help the syndicate steal shipments of his employer's secret, high-value hardware prototypes. He uses his manager-level network access to find the manifests and shipping schedules, and relays the information to the syndicate, which then easily hijacks the shipments during transport.

Three Sample Insider Threat Agent Profiles

Organized Crime

Intent: Hostile
Description: A large, organized, lawless entity may target the enterprise with hostile action. Typically, the goal of organized crime groups is to steal any information or data that can be easily monetized, such as personal, financial, or operational data, as well as intellectual property. Rather than operating as a few individuals, organized crime groups are large and can conduct systematic, aggressive theft of data. This type of insider event tends to involve a local group that targets the enterprise in the region where the group is based.

Potential Event Types:
- Fraud
- Violence
- Product alteration
- Opportunistic data theft
- Espionage

Reckless Insider

Intent: Nonhostile
Description: Not hostile to the enterprise, but does deliberately ignore or circumvent security processes, believing nothing bad will happen. This is often motivated by the desire to finish tasks more quickly. The enterprise may be harmed by this person's carelessness, possibly including being exposed to hostile outside action.

Potential Event Types:
- Accidental leak
- Misuse
- Product alteration

Supplier

Intent: Unknown
Description: A nonhostile supplier, accidentally leaks sensitive information through ordinary human interaction (such as talking with a Distracted Insider).

Alternatively, a hostile supplier may intentionally steal information, not necessarily to harm the enterprise, but with the intent to gain an unfair advantage over other suppliers. In this case, while the supplier's intended target is not the enterprise itself, it is nonetheless a harmful action.

Potential Event Types:
- Accidental leak
- Misuse
- Opportunistic data theft

Figure 3. Threat agent profiles describe characteristics associated with a particular threat agent type. These dossiers help our security team understand the personality types, the agent's motivation, and the event types the agent is likely to perform.

Conclusion

The full spectrum of insider threat is far greater than most have yet recognized. Intel IT's Insider Threat Field Guide aggregates and distills data from various sources into a comprehensive view of the most likely threat agent types and ways an organization may be impacted by an insider threat.

This new tool can help risk managers identify and prioritize insider threats, communicate the risk of these threats, and optimize the use of information security resources to develop an effective defense strategy.

For more information on Intel IT best practices, visit **www.intel.com/IT**.

Receive objective and personalized advice from unbiased professionals at **advisors.intel.com**. Fill out a simple form and one of our experienced experts will contact you within 5 business days.

IT@Intel

We connect IT professionals with their IT peers inside Intel. Our IT department solves some of today's most demanding and complex technology issues, and we want to share these lessons directly with our fellow IT professionals in an open peer-to-peer forum.

Our goal is simple: improve efficiency throughout the organization and enhance the business value of IT investments.

Follow us and join the conversation:

- Twitter
- #IntelIT
- LinkedIn
- IT Center Community

Visit us today at **intel.com/IT** or contact your local Intel representative if you would like to learn more.

Related Content

Visit **intel.com/IT** to find content on related topics:

- Threat Agent Library Helps Identify Information Security Risks paper
- Prioritizing Information Security Risks with Threat Agent Risk Assessment paper
- Understanding Cyberthreat Motivations to Improve Defense paper

Printed in USA Please Recycle 1015/JGLU/KC/PDF