OPTIV

INSIDER THREAT

Solution Primer

Heath Nieddu
Senior Analyst, Solutions Research
Office of the CISO, Optiv

Introduction

Mitigating insider threats presents a unique problem for information security leaders. Authorized users are carrying out harmful actions by performing tasks that may appear to be part of their day-to-day work. This is the salient detail that keeps insider threat activity under the radar of so many of our traditional alerting solutions, processes and strategies. Insider threats represent special problems for security leaders because of their motivations, methods and obscurity.

For the security leader providing protection of the enterprise's most valuable resources, it is crucial to understand the insider threat problem. This involves creating a plan that allows for proactive management of the threat, ensuring enhanced processes, and paving the way for full utilization of technology solutions.

Meeting Business Needs

Many security leaders have concluded that insider threats represent a sufficiently high level of risk that deserves dedicated management because of a growing body of statistics, executive interest and high profile events.

Insider threats put both routine operations and innovation activities at risk

The low frequency-high impact events (such as Edward Snowden) occupy our attention and the news cycles. It is important to prepare for these, but it is also important to understand the long-term trends and focus on the high frequency-lower impact events (such as fraud) that can eventually put strategic objectives at risk through death by a thousand cuts.

- Verizon and the U.S. Secret Service found in 2009 that 48 percent of data breaches were attributed to the work of insiders. Of these, 90 percent were the result of deliberate, malicious acts. Over the years since then, this average has moderated to a still-healthy average of 20 percent. [i]

- The average impact suffered by a firm was $1.7 million, with a range of $1,000 to $87 million, and over half the population suffering less than $50,000, according to a CERT database of 123 insider threat cases from 2012. [ii]

- An influential study from 2005 found nearly all of the organizations experienced financial loss as a result of the insiders' actions (91 percent). Losses ranged from a low of $168.00 to over $691 million. In 30 percent of the cases, the financial loss was in excess of $500,000.

- Insider threat fraud is an expensive problem because it is even harder to identify, incidents last for long periods of time, and these insiders are motivated primarily by financial gain. [iii]

› The median loss from occupational fraud cases was $145,000, according to the Association of Certified Fraud Examiners. [iv]

› Fraud cases involving more than one person are much more expensive, with a 66 percent jump when the number involved moves from one person to two, according to the same study.

› A 2004 study by SEI focusing on the financial sector found that IT fraud becomes more expensive the longer an insider operates. It took on average 32 months to detect an insider committing fraud, with the longer duration events costing 25 percent more to companies.

Insider Threat Defined

While insider threat has been defined in many different ways, Optiv defines **insider threat** as:

"An insider threat is an employee, contractor or other trusted party of an organization with legitimate access to systems, data and applications who uses that access to intentionally harm the organization's finances, reputation, mission or clientele, or takes actions that are contrary to policy, regulation or law"

This definition aligns with the mainstream view that insider threat discussions and research are focused on malicious actors. Interestingly, many advanced external threats appear as insiders during their attacks. **This means some of the controls resulting from an insider threat mitigation plan will also identify external threats acting suspiciously. This is a bonus. For the purposes of focusing the discussion in this research, these non-malicious insiders are outside of our scope.**

Insider threat is as much a people problem as it is a technology problem.

Insider threat is as much a people problem as it is a technology problem.

Insider threat is as much a people problem as it is a technology problem. The key is to focus on the people and understand what drives them. This will help tailor training and awareness campaigns, as well as technology implementations.

Exploring the Actors that Comprise Insider Threats

Contractual employees pose a significant problem in terms of their dynamic need for privileged access, the difficulty in monitoring their actions, and the trouble in creating processes to investigate parties that may be outside of normal HR parties.

While contractual employees are by definition a limited time-frame relationship, **trusted third parties** include suppliers and customers that may have more long-term access to systems, such as inventory or customer-facing systems. *For more information, see Optiv's research on Third-Party Risk.*

It's important to recognize that different organizations will invest in insider threat mitigation in different ways and to various extents based on their mission. An **organization** can include a private enterprise running for profit or not-for-profit, as well as a non-governmental or governmental organization. Enterprises may be primarily concerned for their stakeholders, their mission or their reputation, which results in different needs.

Insider threats put operations and innovation at risk

Insider threats emerge from a combination of trigger events and personal characteristics. There is a menu of consistent trigger events that set insider threat actors into motion, including: personal psychological change, professional stressors or prompting by an external party. For example:

- A company threatens to lay off a large portion of the workforce;
- An external company attempts to recruit an insider to work for them for an enticing sum of money; or,
- Unmet salary expectations. [v]

Once a trigger event has occurred, a variety of attributes play a part in determining how the insider will interpret and act upon the trigger event. For example, a triggering event of reducing the workforce may cause each employees to behave in different ways. A disgruntled IT worker predisposed to feeling defensive towards management's lack of awareness about the difficulty of their job may decide to conduct IT sabotage. A low-level bank teller receiving the same news, possessing an attribute of feeling overly self-centered may justify committing fraud in small amounts in fear of being fired. A mid-level manager with the same fear of upcoming plans by senior leadership may decide to convince other workers to gather intellectual property and provide it to the competition in exchange for future employment.

How a malicious insider acts out against the enterprise is based on the trigger events, their skill level, access and time constraints. Regardless of the probable attack paths based on evidence from the past, insider threats will evolve their actions to meet their future goals. Given that, how do we address this issue?

The answer to mitigating insider threat is a combination of people, process technology and measurement of the threat, risk and program.

Exploring the Actors that Comprise Insider Threats

Program Drivers

Program drivers guide the development of the overall program. These are the elements that propel security programs to the point of taking action on insider threats.

- Situational awareness of extent of insider threat
- Major transformation in business
- Changes in the workforce

As high impact insider threat-based incidents make main stream news, business leaders are asking more questions about the state of their security programs and demanding higher levels of accountability. Security leaders must demonstrate that they can define the problem and explain to what extent it is an issue internally. This is often the first step in approaching insider threat mitigation – to define the problem and understand the current state.

The five-year strategy cycle is only for the most disciplined; even a three-year strategy must be built with an ever-increasing amount of agility baked in. Change is occurring at an unprecedented rate. Most industries are under pressure to transform quickly in order to compete.

These transformations ripple through the enterprise, and IT infrastructure is not immune. Domains are smashed together without enough due diligence, and large parts of an acquisition workforce are quickly integrated, while others are let go. Transformations are triggering events for insider threats, catalyzing their resolve to take action. At the same time, these transformations create vulnerabilities as change governance is overtaxed, leading prudent security leaders to think more critically about insider threat.

Changes in the workforce require security leaders to collaborate with other business units to manage an employee base with less average tenure, and who generally have a different understanding of loyalty to the enterprise.

The traditional social contract between an enterprise and an employee is different and less rigid. The benefits in innovation and cost management are obvious, with subtle costs including less cultural loyalty by employees to a single firm. Predictably, this makes insider threats more of a concern.

Business Requirements

While the program drivers help guide the development of the overall program, business requirements help define the initial deliverables. Operating a successful program means effectively meeting the requirements from the business stakeholders in a timely manner.

Optiv solutions research and development focused research into developing a strong program built on stakeholder input, and gathered a list of commonly identified business requirements for insider threat programs and strategies across a representative sample of industry verticals, maturity and company size. As CISOs build their insider threat strategy, consider these business requirements:

- Insider threat strategy protects key business functions at acceptable costs
- Insider threat strategy is coordinated with other business units
- Security leaders communicate to organization value strategy

For business leaders, there is usually a key function, process or initiative that needs to be protected above all others. This could be the key revenue generating process, or selected from the top of key risks created by an enterprise risk management program. The need to support this function should be easily understood and agreed upon by a large portion of management and is therefore an obvious topic to rally around.

The coordination of activities is just as important as deciding what activities to undertake (porter, strategy). This is especially true with insider threat because so many of the mitigations could already exist in the security program, but need tuning. With so many other large implementations most likely going on in a security program, insider threat efforts will need to demonstrate frugal use of already existing resources.

As with all security issues, the ability to describe the problem, and convincingly report on progress is what will ensure the longevity of efforts past the initial interest. This will require a combination of quantitative indicators and narrative explanations, with reporting tailored to the target audience.

There are generally three levels of audience that must be considered: **senior management**, **director-level management** and the **front line employees** actually making the changes. Each of these groups will require unique reporting.

Leveraging a Third-Party Risk Program

Mitigating insider threats happens over time, with a plan, and with incremental increases in maturity. The basic steps forward resemble those needed for any security strategy: assess, plan, implement and adjust approach based on results and new inputs from stakeholders.

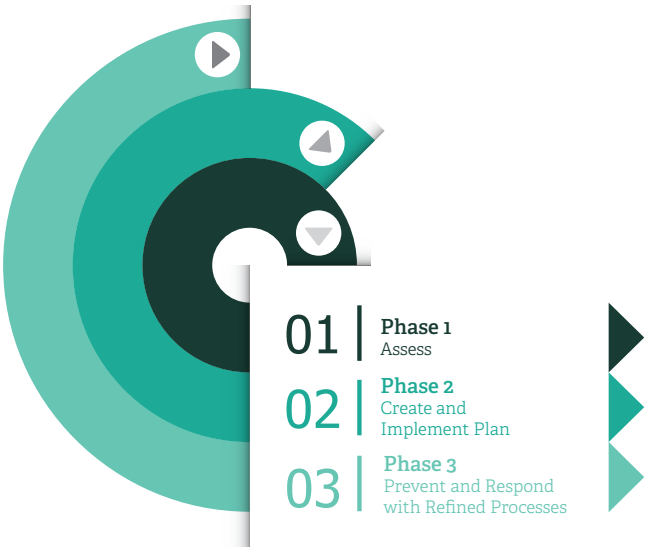
The challenges will arise around establishing a strong foundation in identity and access management, monitoring and data protection, before moving quickly into refining those processes for insider threat and pursuing anomaly detection. This will most likely be a decision made by security leadership.

Ensure that adequate time is spent listening to senior management and other stakeholders. Insider threat mitigation is a broad and chronic problem that will require all hands on deck. Avoid insider threat reporting fatigue by ensuring that all communication is impactful, focused and intentional.

Mitigating insider threats happens over time, with a plan, and with incremental increases in maturity.

Developing a Program Strategy Approach

The foundation of any well-orchestrated security program or strategy is rooted through business alignment and supported by an appropriate balance of personnel, process and tools. Without an appropriate alignment to business objectives and available resources, the program will be unbalanced and may produce irrelevant results. Inconsistent results are the antithesis of what CISOs want to achieve, thus the need to start by developing a strategy.



Developing a strategy with multiple and distinct phases to naturally lead teams to assess, act upon and refine tactics to mitigate insider threat will create a resilient framework for remediating issues. A principles-based strategy can provide that resiliency and sustain efforts over time. [vi]

Below is a three-phased approach to planning, defining and beginning to operationalize an insider threat program or strategy that is **outcome-based and capability-driven**. This is not meant to be a complete framework, but outlines a high-level strategy that plots a course and provides research-backed guidance to the first few critical steps. We'll discuss setting goals, defining the resources necessary to achieve those goals, and provide high-level advice on achieving those goals. This three-phase approach is an aggregate of the in-depth five-step maturity model that is outlined more completely in the **Insider Threat Solutions Blueprint**.

Phase 1 – Assess

Drivers

The critical step to addressing insider threat is to evaluate existing processes within the organization so that the team designs appropriate enhancements.

Assess current efforts by determining what processes are more important to the business, evaluating incident response and user life-cycle management, reviewing relevant risk assessments, reaching out to HR teams, assessing DLP capability, reviewing SIEM capabilities and gathering any current reporting.

Components

- **People**
  - **External support:** Communicate with senior management, legal, privacy and HR teams about their efforts to mitigate insider threats and gauge their interest in participating in a coordinated effort.
  - **RACI:** Use all of the input above to develop a RACI model (Responsible, Accountable, Consulted, Informed) of the pertinent stakeholders in any insider threat mitigation plan.
- **Process**
  - **Business needs analysis:** Consider what the overall business needs, rather than relying on stale assumptions about what business leaders should be requesting from security teams. This is related to insider threat because it will help you prioritize which processes to analyze and protect.

    For example, if a healthcare system is investing heavily in an electronic healthcare record (EHR) system, then it may be most beneficial for the security team to analyze the insider threats that are related to the processes surrounding the EHR implementation. Different parts of the business will focus resources toward initiatives at different times, and

helping the business deliver on those initiatives should be the highest priority.

› **Risk management:** Gather any previous risk assessments, audits or analysis related to insider threats.

› **User life-cycle management:** Make a diagram of all the key steps in the life-cycle of a technology user, from vetting to post-off boarding.

› **Incident response:** Collect incident process documents and search for special sub-routines for handling insider threats.

• **Technology**

› **DLP:** Assess the maturity of the DLP program. Pay attention to how long it takes to craft new DLP rules and how effective the current set of rules are at limiting the impact of insider misuse.

› **SIEM:** Request use cases that relate to alerting on insider threats. Determine the compatibility of other tools with your SIEM.

› **Log Aggregation:** Assess the maturity of any existing log aggregation tools. Expect individual efforts to exist throughout the enterprise.

› **IAM:** Assess the maturity of the IAM program. Pay attention to pre-boarding vetting and integration with HR and operational managers. What inputs does the IAM team receive that tell them what access to grant? Also note the off-boarding processes: how does the team ensure that all access is terminated after an insider no longer has a relationship with the enterprise?

• **Measurement**

› Determine how many incidents are originated by an insider threat.

Capabilities

› **Core program fundamentals:** incident response, log management, patch management

› Basic SIEM in place if not fully used.

› Basic DLP in place if not yet in prevent mode.

› Basic channels developed for delivering training and awareness material.

› Basic understanding of current risk management practices both in security functions and in the larger enterprise.

Operational Advice

› Start using effective insider threat stories and data to convey the need for tight cooperation within the broad workforce.

› Develop awareness for the true efficacy of the current tool set for solving insider threats by asking for reporting about the topic from each tool administrator.

› Review key business level strategies and speak with key business stakeholders to ensure strategy development will be relevant to current thinking.

Phase 2 – Create and Implement Plan

Drivers

This is the stage where strong governance, communication and transparency are required. Measure progress toward goals and do the groundwork to ensure implementation follows principles of strategy. This stage will require driving the details of strategy to completion.

Components

- **People**

› **Employee training and awareness:** Build a tightly knit ethos around protecting the core mission of the business. Attain this through a variety of delivery mediums.

› **User life-cycle management:** HR and IAM functions help reduce gaps and inform the broader mitigation effort on progress.

- **Process**

› **Program Governance:** Create and implement an insider threat mitigation RACI, highlighting and re-designing key processes, and illustrating the reference architecture required for technology enhancements and investments. Make sure that the plan is underpinned by a handful of explicit, guiding principles. These principles will be used by a broad workforce to help determine the best path of action when new or emerging events arise.

› **Risk Management:** Identify key risk by prioritizing crucial business processes, identifying key vulnerabilities, assessing relevant insider threats and suggesting mitigations.

› **Incident Response:** Ensure incident responders are prepared to deal with an insider threat incident. The impact will likely be higher than normal, so extra speed and discretion is of the essence in managing the attack.

- **Technology**

› **Privileged identity, access and user management:** The information security leadership team should develop a privileged identity management (PIM), privileged account management (PAM) and a privileged user management (PUM) gap analysis in conjunction with IT engineers. This work creates an investment plan that is designed to ensure elevated access is provided only when necessary.

› **Anomaly detection capability:** The information security leadership team should set proper expectations with all stakeholders about the steep learning curve and potential benefits of enhanced user anomaly detection. If this effort is part of a broader anomaly detection effort within security, then requirements such as target data and alerting threshold should be communicated with that project team. Current solutions are continually improved using the identified use cases found in the user anomaly detection solutions.

- **Measurement**

› **Reporting:** Reporting should consist of both narrative commentary and any measures of progress. Key performance indicators, (KPIs) largely focus on mitigation plan completion and are comprised of base measures. Be sure that reporting speaks to three levels of customers, including: senior management, security and technology leadership, as well as those responsible for actually implementing changes. All three groups will need unique reporting to perform roles.

Capabilities

› The ability to recruit and maintain sponsors and stakeholders is vital, as well as identifying early successes to share with the implementation team.

› Ensure ability to inform and empower multiple parties across enterprise to execute insider threat mitigation plan through guiding principles.

› Measures, metrics and KPIs can be designed to effectively communicate across multiple layers of the enterprise.

› Conduct account audits in order to hunt down rogue backdoor accounts for employees who have already left.

› Perform proper vetting of employees before onboarding.

Operational Advice

› Decide if the insider threat mitigation plan will be broad-based, or linked to key business projects.

› Decide if the insider threat mitigation plan should primarily be about cost avoidance or business enablement.

› Understand that tools are necessary but not sufficient for tackling the insider threat problem.

› Recognize successes in order to get over the initial implementation hurdles.

› Be prepared to dedicate human resources to UBA implementation efforts to help ensure success.

› Ensure that anomaly detection tools are user-centric rather than data-centric. This will make investigations easier to pursue and the tool easier to use.

Phase 3 – Prevent and Respond with Refined Processes

Drivers

Shift from an implementation stage to a refinement focus that emphasizes sustainable maturity and provides early warning, incident prevention and reduced incident impacts.

Demonstrate support for overall business and a higher state of cultural cohesion around insider threats using a refined mitigation effort.

Components

- **People**

› **Employee training and awareness:** Training includes developing the broad management team and all employees to be the human sensor that detects suspicious behavior early. This training is coupled with clear reporting processes.

› **User life-cycle management:** Information security, HR and IAM teams utilize a standard user life-cycle process. User access tools are integrated with other security functions when needed.

•Process

› **Program Governance:** Defend plan with results related to reduced insider incident impacts and demonstrate broad completion of plan milestones.

› **Risk Management:** Senior management and information security leadership refine risk tolerance levels for key processes and information security leadership ensures enforcement.

› **Incident Response:** IR team is fully integrated with HR, legal and privacy, and processes are established to closely limit details related to managing an insider incident.

•Technology

› **Privileged identity, access and user management:** Administrators develop reporting and use cases showing the benefit of their work and where extra attention is needed. This reporting is directed to information security leadership so that plan can be adjusted if needed.

› **Anomaly detection capability:** Custom baselines developed and thresholds refined to eliminate false positives with the aid of a dedicated analyst. The primary analyst matures the anomaly detection capability to the point that it can be taken out of visibility-only mode and can be used to prevent certain actions.

•Measurement

› **Reporting:** Base measures are formed into more complex metrics, contextualizing numbers by relating them to business drivers in percent and fractions.

Capabilities

› Creation and maintenance of customized behavioral baselines.

› Leveraging the human sensor in the workforce through training and reporting processes.

› Integration of UBA alerting into SIEM or other reporting tools and processes.

Operational Advice

› Empower individuals to make appropriate adjustments to plan.

› Shift from monitor to prevent whenever possible.

› Create mechanisms to report suspicious behavior.

Call to Action

Third parties simultaneously pose one of the greatest business advantages and risks to your organization. In order to manage risk effectively across the business, CISOs are implementing third-party risk programs that are closely aligned with their enterprise risk management, legal and vendor management organizations. As a result, the role of the CISO has been elevated to one of a corporate risk leader, rather than a technologist – and board-level visibility and accountability is both tremendously powerful and incredibly complicated.

The CISO will have one chance to scope, define, design and implement a strong third-party risk program aligned to business strategy. Adopting a program strategy approach provides the structure and rigor to demonstrate necessary due-diligence, goals-attainment, and ultimately define success or failure. The program structure should allow for discovery, identification, assessment and treatment of those third parties in a uniform manner to drive down the unknown risk to the business.

[i]Verizon and the U.S. Secret Service, 2010 Data Breach Investigations Report, 2010, p. 17

[ii]Cappelli, Dawn M., Moore, Andrew P., and Trzeciak, Randall F., The CERT Guide to Insider Threats: How to Prevent, Detect and Respond to Information Technology Crimes (Theft Sabotage, Fraud), SEI Series in Software Engineering, Upper Saddle River, NJ, 2012, Chapter 2

[iii]Randazzo, Marisa R., Keeney, Michelle, National Threat Assessment Center, United States Secret Service, Cappelli, Dawn M., Moore, Andrew P.. Insider Threat Study: Illicity Cyber Activity in the Banking and Finance Sector, CMU/SEI, June 2005, p.19

[iv]Association of Certified Fraud Examiners. Report to the Nations on Occupational Fruad and Abuse. 2014, pp.19,4.

[v]Cappelli, Dawn M., Moore, Andrew P., and Trzeciak, Randall F., The CERT Guide to Insider Threats: How to Prevent, Detect and Respond to Information Technology Crimes (Theft Sabotage, Fraud), SEI Series in Software Engineering, Upper Saddle River, NJ, 2012, Chapter 2

[vi]Product of five focus groups conducted across the country with enterprise security leaders, as well as internal and external subject matter experts.

1125 17th Street, Suite 1700
Denver, CO 80202
800.574.0896
www.optiv.com

Optiv is the largest holistic pure-play cyber security solutions provider in North America. The company's diverse and talented employees are committed to helping businesses, governments and educational institutions plan, build and run successful security programs through the right combination of products, services and solutions related to security program strategy, enterprise risk and consulting, threat and vulnerability management, enterprise incident management, security architecture and implementation, training, identity and access management, and managed security. Created in 2015 as a result of the Accuvant and FishNet Security merger, Optiv is a Blackstone (NYSE: BX) portfolio company that has served more than 12,000 clients of various sizes across multiple industries, offers an extensive geographic footprint, and has premium partnerships with more than 300 of the leading security product manufacturers. For more information, please visit www.optiv.com.

1.16 | F1