


THE INCREASING THREAT FROM INSIDE

A PROACTIVE AND TARGETED APPROACH
TO MANAGING INSIDER RISK



AUTHORS

Paul Mee
Rico Brandenburg
Matthew Gruber
James Cummings

INTRODUCTION

Insider threat represents a growing contribution to an organization's overall cyber risk exposure. A significant number of executives fall victim to common misconceptions about insider risk and, therefore, they typically do not believe that their organization's own workers pose a significant threat. Even those who do, find it challenging to make significant headway, as doing so requires tackling a host of thorny legal and HR issues. As a result, many organizations have underinvested in this area.

Applying data loss prevention technology, monitoring software, or compliance surveillance tools is not enough. Organizations need to scale their diligence and defenses appropriately to identify, detect and mitigate risks before they materialize or cause harm. The leaders in this area:

- Have the right level of senior stakeholder engagement,
- Use a risk-based prioritization of what to monitor and protect, and most importantly,
- Have implemented joined-up procedural arrangements with clear and tested roles and responsibilities to enable the right response when unusual behavior is identified.

Given the growing threat of insiders, it is crucial for organizations to develop an effective insider risk program. The way to success is to start small, with a focus on the highest-risk areas, and start now, as organizations simply cannot afford to ignore the threat any longer.

Insider

Insiders generally refer to people (employees, former employees, contractors, business associates) who have or had authorized access to the organization's data, information systems, or facilities. Their intentional or even non-intentional acts (i.e., negligence, carelessness, or compromised credentials) can pose a significant threat to the organization. Insider threat can take many different forms, including destruction and manipulation of organizational assets (digital/physical); espionage; fraud; insider trading; and theft of intellectual property (IP), trade secrets, or personal information.

THE THREAT IS REAL

In 2018, of the 5 billion records stolen/compromised, over 2 billion were a result of insider circumstances.¹

Insider threat is one of the greatest drivers of security risks that organizations face. Typically, a malicious insider utilizes their (or other employee's) credentials to gain access to a given organization's critical assets. Many organizations are challenged to detect internal nefarious acts, often due to limited access controls and the ability to detect unusual activity once someone is already inside their network. Security functions have traditionally invested much more heavily in combating external threats ("securing the perimeter") than in combating the risk posed by employees, contractors, or business partners.

But organizations are waking up to the fact that insider threat can pose considerable harm to their operational resilience, financial status, and reputation. Across industries, regulators, government agencies, and industry groups have signaled that organizations need to take insider threat seriously (e.g., New York State Department of Financial Services (NYDFS) Cybersecurity Regulation, National Infrastructure Advisory Council (NIAC), National Insider Threat Task Force (NITTF), Department of Energy (DoE), International Air Transport Association (IATA)).

Nearly 75% of companies believe they have appropriate controls to mitigate insider threat – but more than 50% of companies had a confirmed insider attack in the past 12 months.²

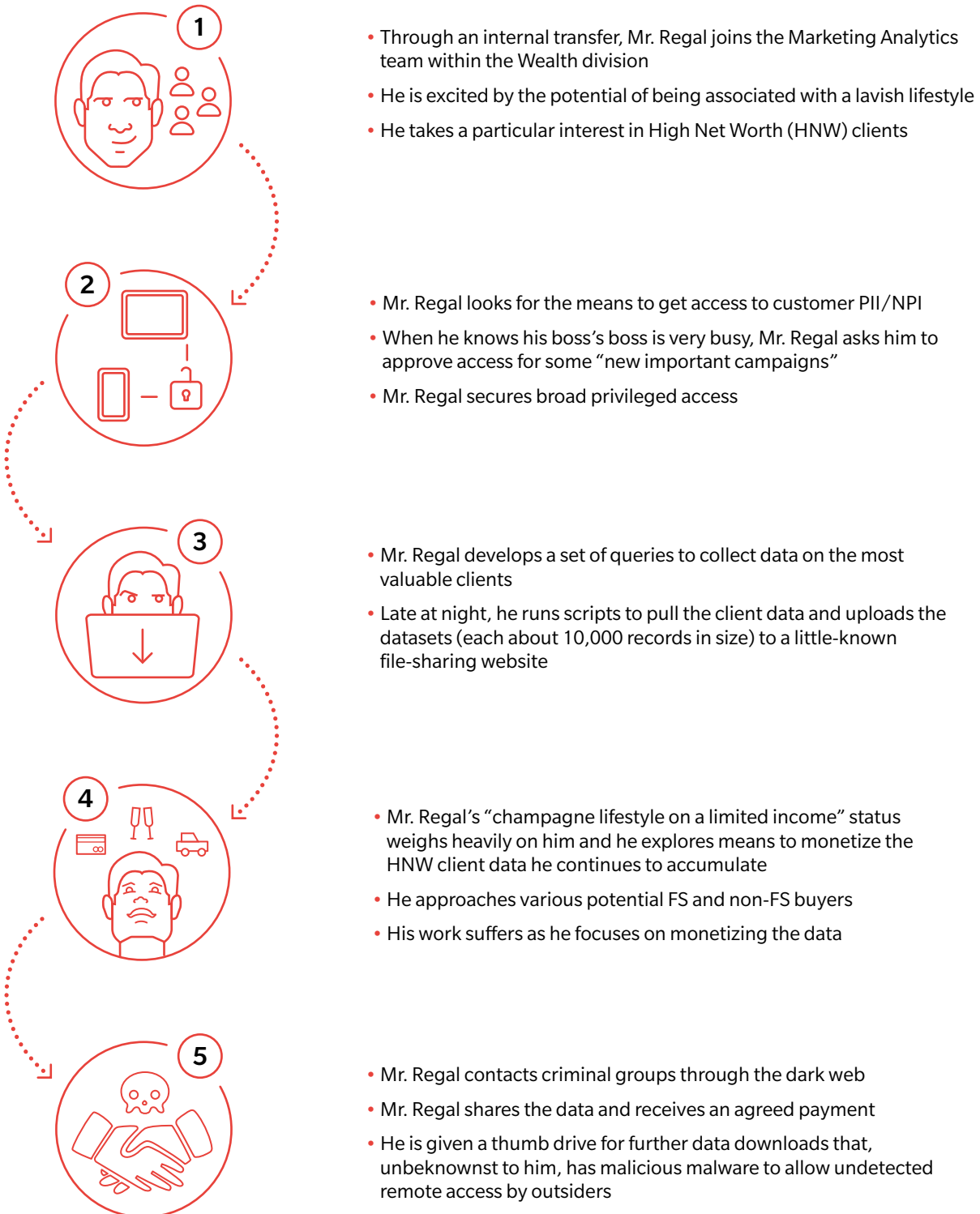
Because they are often familiar with the organization and typically have the "keys to the castle," insiders can more easily identify where the organization is exposed and are well-placed to exploit vulnerabilities or cultural norms, (e.g., trust-based access). Exhibit 1 provides an example of how a malicious insider can take advantage of a data analytics function in a financial institution. The example demonstrates that an insider can perform activities that by themselves may not be considered suspicious. But considering the series of activities reveals the malicious intent and begs the question: "Why could this pattern of behavior not have been detected?"

1. Risk Based Security, Inc. Data Breach QuickView Report, Year End 2018 - Data Breach Trends. Includes malicious and accidental circumstances

2. Crowd Research Partners: 2018 Insider Threat Report

A SERIES OF SUSPICIOUS ACTIVITIES

by the talented Mr. Regal



Despite the growing consensus that insiders represent a considerable threat with potentially severe consequences, some organizations remain in denial. They fall victim to generally accepted myths that make them believe that “this won’t happen to us” (Exhibit 2).

More than 30% of companies consider themselves slightly or not at all vulnerable to insider threats.³

The threat is not only pervasive; it is also challenging to detect. Frequently, malicious acts perpetrated by insiders blend into daily behaviors and will circumvent organizational controls. While malicious insiders often demonstrate common personal patterns, many of these behavioral triggers are stove-piped within an organization and do not in isolation result in an alert. If viewed collectively, these behaviors could highlight malicious intent, but all too often, organizations only aggregate these behaviors into a pattern after an incident has occurred, damage has been done, and the culprit has been identified.

We urge boards of directors and executives to think carefully about their company’s risk profile and control environment before declaring themselves safe. Ultimately, it only takes one person with access to the organization’s most sensitive and critical information, systems, or facilities to carry out an attack that can cause lasting damage to business operations, reputation, and regulatory standing.

It only takes one person to carry out an attack that can cause lasting damage.

Common personal patterns

Declines in performance, dissatisfaction with the organization, heavy use of personal devices at work, extensive communication with external contacts, activity at unusual hours, and attempts to gain access to restricted assets (digital/physical), and financial hardship have all been observed in malicious insiders. Companies are also increasingly concerned about workers adopting more extreme political or social positions that could lead them to carry out malicious acts, which can be evident in their social media and internet browsing activity.

3. Crowd Research Partners: 2018 Insider Threat Report

Exhibit 2: Myth busters
Common misconceptions about insider threats

MYTH	TRUTH
A GOOD COMPANY CULTURE IS ENOUGH TO PROTECT AGAINST INSIDERS	A good company culture reduces the likelihood of disgruntled employees. But the motivation of malicious insiders can be driven by a variety of factors unrelated to the company’s culture, e.g., financial gain, ideology, desire for recognition. Over 50 percent of companies confirmed insider attacks in the past 12 months. ⁴
INSIDER THREAT COMES FROM CONTRACTORS	Permanent staff are typically with an organization longer and accumulate more access over time, so they represent a bigger threat. 56 percent of companies identified regular employees as the greatest security risk to organizations. ⁴
INSIDER RISK IS MITIGATED THROUGH THE GENERAL CONTROL ENVIRONMENT	Controls designed for other purposes may not be as effective against insiders (e.g., requiring people to have valid credentials to enter a building or log in), but they can be leveraged in an effective program.
MALICIOUS INSIDER ACTIVITY CAN BE SPOTTED RIGHT AWAY	Many organizations have rules-based monitoring that will detect basic insider activity (e.g., an employee emailing large files to her personal email). But few organizations will detect more sophisticated insider activities (e.g., exploiting access they rightfully have, sending confidential information in the body of an email to a seemingly legitimate email address). On average, it takes organizations 72 days to contain an insider incident, with only 16 percent of such incidents contained in less than 30 days. ⁵
DATA LOSS PREVENTION (DLP) IS AN EFFECTIVE INSIDER RISK PROGRAM	DLP is a component of, but not the same as, an insider risk program. DLP can help prevent exfiltration of data by an insider. But it provides little protection against other malicious acts (e.g., destruction of assets, fraud).
INSIDER THREAT IS ONLY AN ISSUE FOR STRATEGIC INDUSTRIES	Many of the highest-profile events have been in “strategic industries” with leading-edge innovation or R&D, national defense capabilities, or highly valuable data (e.g., medical records). However, companies in all industries ⁵ and all sorts of government bodies have had material events caused by an insider.
RECRUITING HAS A GOOD PROCESS TO FILTER OUT POTENTIALLY MALICIOUS EMPLOYEES	People do not need to have malicious intentions from the start. Changes in personal or economic circumstances may create incentives for malicious activity over time.

4. Crowd Research Partners: 2018 Insider Threat Report

5. Ponemon Institute 2018 Cost of Insider Threats: Global. Includes accidental insiders, malicious insiders, and credential thieves

DOES YOUR INSIDER RISK PROGRAM NEED A RESET?

Establishing and operationalizing an effective insider risk program is not easy. Compared to more traditional cyber defense activities, addressing insider threat requires significantly more coordination, touches more closely on privacy and related ethical issues, and has more potential to cause lasting damage to a company's culture and reputation if not done correctly.

In our experience, many organizations think they are effectively addressing the threat, but fall victim to common pitfalls that undermine their efforts. If your organization demonstrates one or more symptoms related to these pitfalls (Exhibit 3), your insider risk program may need a hard reset.

Case study: A program gone wild

Recently, the media highlighted the case of a large financial services firm that retained a data mining company for its insider risk program. The data collection was limitless and there were few guardrails on how the insider risk program could use that information. Ultimately, the experiment collapsed when bank executives realized that the degree of surveillance was tantamount to invasive spying, did not belong in a corporate environment, and was damaging the company's culture. This case illustrates some of the potentially severe consequences of an insider risk program gone awry, which can also include higher attrition, difficulties attracting talent, legal challenges, and reputational damage.

PITFALL 1: NOT OBTAINING ORGANIZATIONAL COMMITMENT

- Senior executives are skeptical of the danger posed by insiders
- The board and senior management did not have input into the design of the program

PITFALL 2: NEGLECTING THE BASICS

- “Crown jewel” assets and high-risk areas have not been identified
- Insider risk training is absent or patchy at best
- Identity and access management is under-developed or variable
- No or limited employee screening/vetting (often none after initial recruitment)

PITFALL 3: HAVING A PROGRAM IN NAME ONLY

- No playbooks for responding to potential insider threats
- Limited, siloed, or poor articulation of the components of the program and how to measure success
- Response and escalation processes are not drilled and tested

PITFALL 4: HAVING INITIATIVES BUT NO HOLISTIC PROGRAM

- Existing capabilities and processes are not effectively leveraged (e.g., DLP program, compliance surveillance, physical security)
- Critical functions (HR, Legal, and Audit/Compliance) are not consistently coordinating and communicating with regards to insider risks
- No single executive or group with authority to decide whether to initiate an insider investigation

PITFALL 5: BITING OFF MORE THAN YOU CAN CHEW

- Program is “one-size-fits-all” and attempts to monitor the entire organization
- Not enough resources to effectively cover insider-related scope and processes

PITFALL 6: IGNORING THE CULTURAL RAMIFICATIONS AND PRIVACY CONCERNS

- Little consideration of how the program can exist in and adapt to different country, regulatory, and societal/cultural regimes
- Key functions like HR, Compliance, Legal, and Privacy not involved in the design of the program
- Program is perceived as “Big Brother-like,” excessively monitoring employee behavior and communications

TAKING A PRACTICAL APPROACH TO INSIDER RISK



Let's revisit the example of Mr. Regal, the employee in the Wealth division of a bank who managed to successfully sell sensitive customer information over the dark web. Exhibit 4 describes how an effective insider risk program might have detected the threat and prevented Mr. Regal from executing his attack. The set of detective and protective controls and monitoring capabilities allow the organization to identify individuals who pose higher risk to the organization and introduce additional monitoring to ensure that malicious activities can be identified and stopped.

A SERIES OF SUSPICIOUS ACTIVITIES

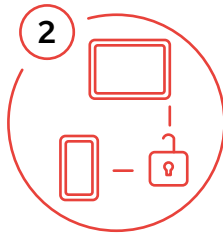
by the talented Mr. Regal



- Through an internal transfer, Mr. Regal joins the Marketing Analytics team within the Wealth division
- He is excited by the potential of being associated with a lavish lifestyle
- He takes a particular interest in High Net Worth (HNW) clients



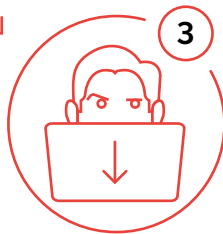
Background and financial checks initiated on Mr. Regal due to the transfer indicate some concern based his previous credit history and high debt.



- Mr. Regal looks for the means to get access to customer PII/NPI
- When he knows his boss's boss is very busy, Mr. Regal asks him to approve access for some "new important campaigns"
- Mr. Regal secures broad privileged access



Elevation of privileges raises Mr. Regal's risk rating to "high." Mr. Regal is put on a "watch list" to be monitored more closely.



- Mr. Regal develops a set of queries to collect data on the most valuable clients
- Late at night, he runs scripts to pull the client data and uploads the datasets (each about 10,000 records in size) to a little-known file-sharing website



An alert is generated because behavioral analysis on members of the "watch list" indicates that it is unusual for Mr. Regal to be downloading sensitive client data late at night.



- Mr. Regal's "champagne lifestyle on a limited income" status weighs heavily on him and he explores means to monetize the HNW client data he continues to accumulate
- He approaches various potential FS and non-FS buyers
- His work suffers as he focuses on monetizing the data



The insider risk program sees that Mr. Regal, already on the "watch list," receives a poor performance review and coordinates with HR to further investigate.



- Mr. Regal contacts criminal groups through the dark web
- Mr. Regal shares the data and receives an agreed payment
- He is given a thumb drive for further data downloads that, unbeknownst to him, has malicious malware to allow undetected remote access by outsiders



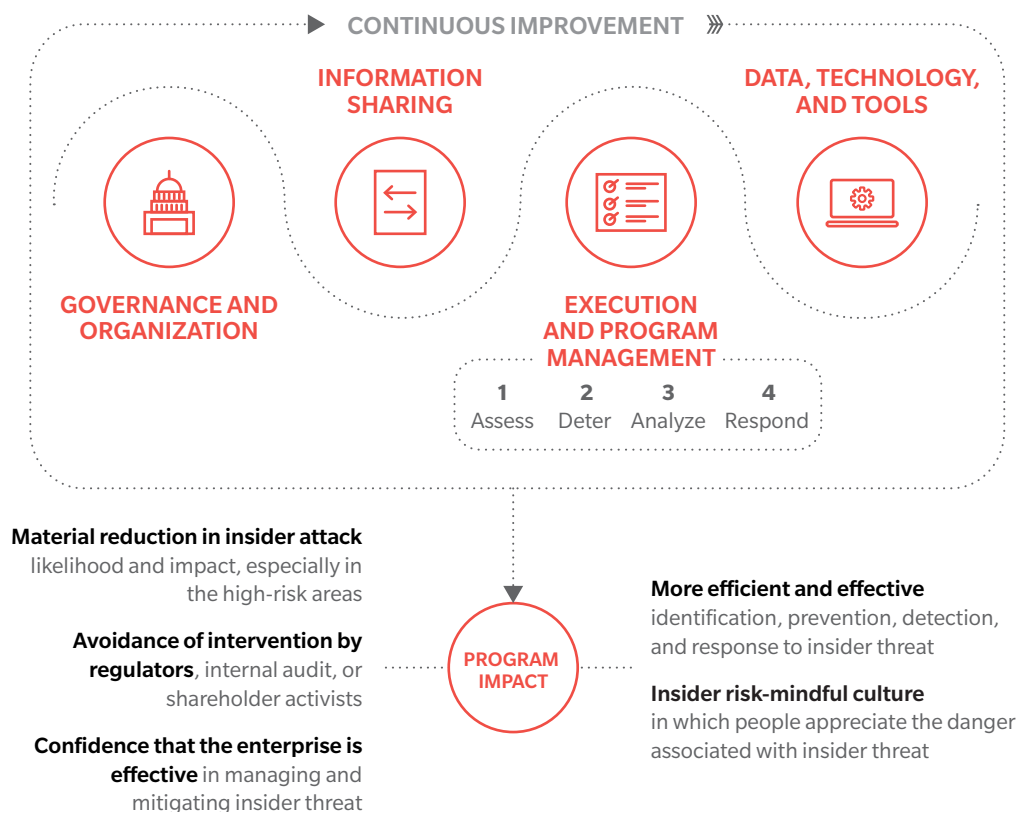
Dark web analysis reveals that there has been a data breach before the breach is made public.

An effective insider risk program is designed to identify potential threats and prevent bad actors from carrying out malicious acts, but a program is more than just a set of controls. Exhibit 5 describes the five key elements for an effective program:

- **Governance and organization:** Clear articulation of the oversight and operating model
- **Information sharing:** Effective cross-functional interaction model to address legal, ethical, cultural, and privacy concerns, and understand what is required to “get to yes”
- **Execution and program management:** Processes and controls that cover the end-to-end lifecycle of insider risk management in line with the organization’s risk appetite
- **Data, technology, and tools:** Foundational capabilities that support the management of insider risk
- **Continuous improvement:** Mechanisms to integrate learnings from past events and to evolve the program in line with the changing risk exposure

As highlighted in Exhibit 5, an effective insider risk program not only reduces the risk associated with insiders, but it also delivers important tangential benefits for the organization. For example, collecting badge-in/badge-out data to identify suspicious activity can assist in workplace availability studies or safety during a building emergency.

Exhibit 5: Oliver Wyman insider risk program framework⁶



6. Reflects industry-wide frameworks and best practices, including the NITTF Insider Threat Program Maturity Framework.

Most organizations that exhibit some of the pitfalls highlighted in Exhibit 3 will require a review and a reset of their insider risk program. This means refocusing the organization's efforts on practical use cases that support the development of a data-driven, risk-focused, and proactive insider risk program. Based on our experience, we have identified key practices that will help make an insider risk program as effective as possible.



GOVERNANCE AND ORGANIZATION

Define the insider risk program. Define and document an “insider risk program” with a clear mandate and vision that includes representatives from different, key functions across the organization (e.g., Cyber/Information Security, Physical Security, HR, Privacy, Legal, Compliance). Everyone involved in the program should have defined roles and responsibilities. Whether the organization creates a dedicated team for insider threat or not, a specified group should be responsible for formulating policy related to insider threat and operationalizing the program.

Engage senior leadership. Ensure executive leadership provides oversight of and input on the direction of the program. One global firm found that presenting a small number of illustrative use cases to the board of directors and executive management helped leadership provide clear guidance on the tolerance for tracking, recording, and analyzing worker behavior.

Integrate existing efforts. Identify other existing, related efforts and integrate them under the umbrella of insider threat, either directly folding them into the insider risk program or empowering the insider risk program to provide requirements to other efforts. For example, the compliance surveillance program may continue to be owned by Compliance but be required to scan for additional use cases or escalate certain incidents to the insider risk program.



INFORMATION SHARING

Monitor, measure, and communicate success. Define what success means and develop a set of metrics to provide insight into the program's effectiveness over time. Best-in-class organizations compile these metrics in a senior executive dashboard that is regularly updated, with drill-down capabilities to assist program leadership. Metrics encompass traditional measures of success, like outcomes of insider threat cases, and more non-traditional measures of success, like how well different functions coordinate or awareness of insider threat.

Overcome barriers to information sharing. Providing the insider risk program with access to the information needed to identify and investigate suspicious behavior usually involves overcoming a variety of legal, ethical, cultural, and privacy barriers. Organizations should define clear guidelines on the information that can be collected/shared and maintain anonymity until there is enough certainty to unmask the individual.



EXECUTION AND PROGRAM MANAGEMENT

Focus the program. Understand the organization's highest-risk areas ("crown jewels"), identify the potential insiders (people with access), and create a set of use cases to inform prevention and monitoring based on historical events and actors' likely motivations. One organization embarked on an enterprise-wide effort to identify the critical systems that exposed the organization to the most damage if a malicious insider had access.

Don't neglect prevention. Focus on proactively preventing or minimizing insider threat, rather than simply detecting rogue employees. Some organizations actively modify roles across the high-risk population to limit the potential damage that any one employee could do. Organizations should also raise awareness on insider threat and encourage people to come forward if they observe unusual behavior.

Rigorously document and test processes and playbooks. Document a clear set of steps and criteria to determine if further investigation or action is warranted when a potential threat or malicious act is detected. The potential consequences of malicious acts (e.g., reductions in compensation, termination, change of access privileges) should be documented and standards should be in place to guide management on when to employ them. Processes should be drilled and tested, even outside of insider threat response. For example, Security and HR should regularly test processes to remove access for employees who are terminated (forced or voluntary).



DATA, TECHNOLOGY, AND TOOLS

Ingest relevant data. Gain access to a wide variety of data that can shed light on suspicious behavior. Data can be internal (e.g., badge-in/badge-out, log-in times), the result of periodic background / financial checks, or even external (e.g., social media), to the extent allowed by law.

Leverage technological solutions. Employ a data analytics platform to ingest the myriad of data being collected and identify suspicious behavior based on defined use cases. The platform should prioritize the alerts for investigation by the relevant personnel. Use a case management system to manage alerts and investigations and ensure that only the right individuals can gain access to sensitive insider threat-related information.



CONTINUOUS IMPROVEMENT

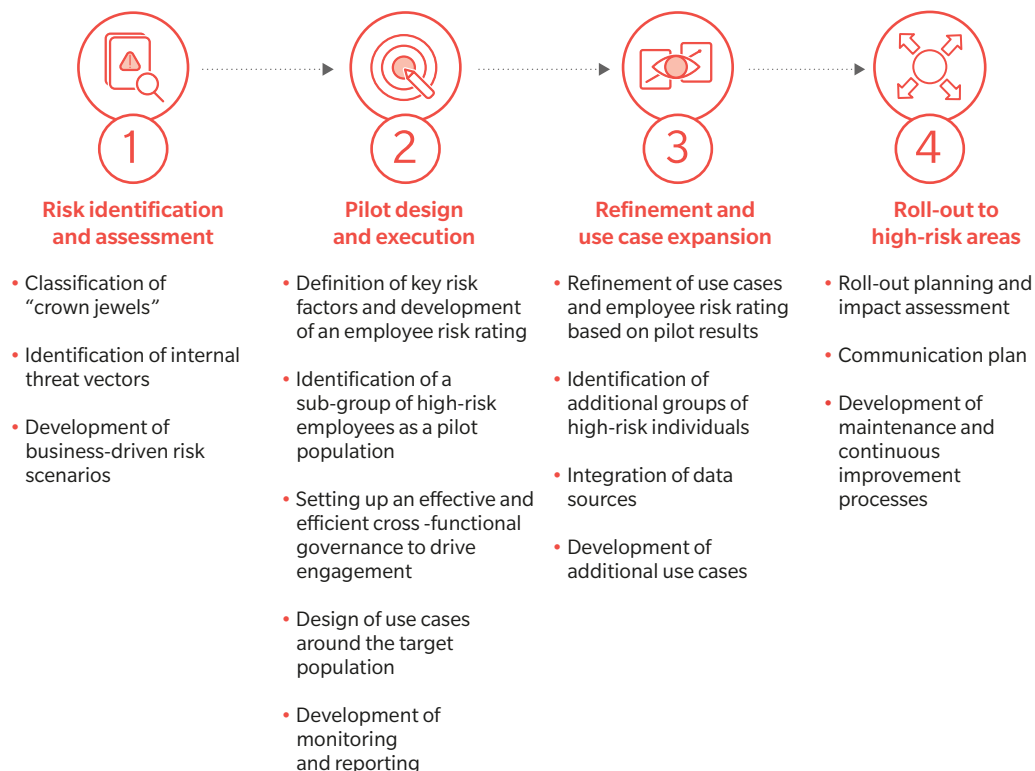
Test the effectiveness of the program. Have workers mimic insiders in a form of "red teaming" to see if detection mechanisms would identify the threat. Employ threat hunting, focusing on critical assets and starting from the hypothesis that an insider has compromised those assets in some way. Team members should be responsible for capturing and cataloging the learnings from these activities and suggesting corresponding enhancements to the program.

START SMALL AND FOCUSED

Implementing an effective insider risk program requires a design tailored to the specific culture, processes, and risks of the organization. Exhibit 6 describes the approach to designing and implementing a successful insider risk program. It starts with the identification of the risk exposure and the business impact of the risk. Once the “crown jewels” and associated insider risks are identified, a pilot can be designed to mitigate these risks. It’s important to start small and focus on a clearly defined high-risk employee sub-group to work through the organizational issues that need to be solved. Most importantly, the pilot needs to help the program stakeholders understand what it takes to “get to yes” (know when to act on a suspected malicious insider). After the pilot learnings are communicated to senior executives and incorporated into the program design, the organization can decide how to further roll out the insider risk program (Exhibit 6).

Designing and implementing an effective insider risk program is crucial for any organization. With insider threat only increasing in prominence, organizations simply cannot afford to ignore the threat. Getting it right will deliver clear benefits, but delays could be costly. Take a proactive approach to managing insider risk – start small, but start now.

Exhibit 6: Successful design and implementation of an insider risk program



Oliver Wyman is a global leader in management consulting that combines deep industry knowledge with specialized expertise in strategy, operations, risk management, and organization transformation.

For more information please contact the marketing department by email at info-FS@oliverwyman.com or by phone at one of the following locations:

AMERICAS

+1 212 541 8100

EMEA

+44 20 7333 8333

ASIA PACIFIC

+65 65 10 9700

Paul Mee

Partner, Digital and Financial Services, Cyber Platform Lead
paul.mee@oliverwyman.com

Rico Brandenburg

Partner in the Risk & Public Policy and Digital practices
rico.brandenburg@oliverwyman.com

Matthew Gruber

Engagement Manager in the Risk & Public Policy and Digital practices
matthew.gruber@oliverwyman.com

James Cummings

Senior Advisor on Cyber Risk Management and Cyber Defense
james.cummings@oliverwyman.com

www.oliverwyman.com

Copyright © 2019 Oliver Wyman

All rights reserved. This report may not be reproduced or redistributed, in whole or in part, without the written permission of Oliver Wyman and Oliver Wyman accepts no liability whatsoever for the actions of third parties in this respect.

The information and opinions in this report were prepared by Oliver Wyman. This report is not investment advice and should not be relied on for such advice or as a substitute for consultation with professional accountants, tax, legal or financial advisors. Oliver Wyman has made every effort to use reliable, up-to-date and comprehensive information and analysis, but all information is provided without warranty of any kind, express or implied. Oliver Wyman disclaims any responsibility to update the information or conclusions in this report. Oliver Wyman accepts no liability for any loss arising from any action taken or refrained from as a result of information contained in this report or any reports or sources of information referred to herein, or for any consequential, special or similar damages even if advised of the possibility of such damages. The report is not an offer to buy or sell securities or a solicitation of an offer to buy or sell securities. This report may not be sold without the written consent of Oliver Wyman.