

INSIDER RISK MANAGEMENT PROGRAM BUILDING: RESULTS FROM A SURVEY OF PRACTITIONERS

Andrew P. Moore

Sarah Miller

Angela Horneman

May 2021

Introduction

A recent survey of insider risk management practitioners illuminates the deep complexity of insider risk management and the broad range of realized insider threats faced by organizations across industry sectors.¹ Some decision makers may resist considering their employees as a potential threat. While it certainly makes sense to be sensitive regarding *how* to frame insider risk programs to best serve the organization, practitioner experience shows that simply ignoring insider risk is problematic. Nevertheless, the complexity and potential scope of the problem can be daunting to organizations. Practitioners recommend an incremental approach to navigate this complexity and practically deal with the insider risk scenarios that an organization considers important. In addition, a well-balanced insider risk program can become known as an advocate for employee well-being and a means for a more productive, engaged, connected, and committed workforce.

Using the collected survey data, this paper describes and contextualizes practitioner recommendations for organizations building and/or extending their insider risk programs. We expect the results to be useful for organizations at earlier stages of building or extending their insider risk management capability. For the purposes of this study, we define an *insider* of an organization as an employee, contractor, or other business partner that has or had authorized access to the organization's assets. Access includes both physical and virtual (cyber) access; assets include information, processes, systems, and facilities. Insider *risk* for an organization is the potential for an insider to use their authorized access to the organization's assets, either maliciously or unintentionally, in a way that negatively affects the organization. We further had a flexible notion of an insider risk program: an *insider risk program* exists

^{p1} This work was funded by Carnegie Mellon University CyLab, with generous support from Microsoft. For their help in survey design, the authors would also like to thank Dan Costa, Carrie Gardner, Bob Ditmore, Michael Theis, David Evans, Raman Kalyan, and Khetiwe Chitewere.

when an organization has staffing, policies, practices, and procedures in place to address any aspect of insider risk, such as prevention, detection, mitigation, or response.²

This paper contains detailed survey analysis results, which is a longer version of the summary paper titled “Insider Risk Program Building: Summary of Insights from Practitioners.”

A Brief History of Insider Threat Guidance

The insider threat problem in organizations has been studied for decades, with many incident analyses and surveys (too numerous to mention) documenting the extent of the problem. Guidelines for helping organizations mitigate the insider threat started coming out in the 2000’s. One of the earliest and most persistent through time is the Common Sense Guide to Prevention and Detection of Insider Threats, the first version of which was published by Carnegie Mellon University’s CyLab in 2005 and is now in its sixth edition.³ Insider threat became more prominently recognized when, by U.S. Presidential Executive Order, insider threat mitigation was mandated in the form of a set of minimum standards in 2011, first for U.S. Government organizations and later its contractors.⁴ Best practices for these minimum standards soon followed developed by an organization set up by the Executive Order, the National Insider Threat Task Force (NITTF).⁵

Gradually, insider threat program building became a central focus for NITTF and other government organizations. Complementing CERT’s training in the area,⁶ the NITTF developed a framework for maturing insider threat programs.⁷ Although DHS recently published an insider threat mitigation guide that applies to both the public and private sector,⁸ most of the NITTF guidance is targeted primarily at U.S. Government organizations and their contractors, and is steeped in that perspective and language. There is a fair amount of commonality in guidance for the public and private sectors, however the priorities may be significantly different. The study described in this paper focuses primarily on industry’s perspective on building insider risk programs.

² We fully acknowledge that organizations use different terms for their programs, such as insider threat programs, internal risk programs, or insider risk capability. We suggested that respondents interpret references to insider risk program in whatever terms made most sense for their organization.

³ Theis, M.C., R.F. Trzeciak, D.L. Costa, A.P. Moore, S. Miller, T. Cassidy, and W.R. Claycomb. "Common sense guide to mitigating insider threats, Sixth Edition." (2019).

⁴ The White House. (2012). Presidential Memorandum—National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs. November 21, 2012.

⁵ National Insider Threat Task Force (NITTF). (2017). Insider Threat Guide: A Compendium of Best Practices to Accompany the National Insider Threat Minimum Standards.

⁶ CERT National Insider Threat Center, Training on Building an Insider Threat Program; Insider Threat Program Manager: Implementation and Operations, 2018-2021.

⁷ National Insider Threat Task Force (NITTF). (2018). Insider Threat Program Maturity Framework.

⁸ DHS Cybersecurity Infrastructure and Security Agency (2020) Insider Threat Mitigation Guide, August 2020.

Complexity of Insider Risk Management

Insider threat is unique in the realm of organizational security and resilience in that the potential threat agents (the organization's trusted personnel) play fundamental roles in accomplishing the organization's mission. Insider goodwill is essential to both keeping intentional insider risk to a minimum and ensuring organizational success generally. Research from the CERT® Division's National Insider Threat Center at Carnegie Mellon University's Software Engineering Institute (SEI) shows that the organization's practices and managerial processes can create a working environment conducive to insider threats by undermining insiders' goodwill. In particular, workforce management practices that damage insiders' perceptions of organizational support are correlated with increased intentional insider misbehaviors.⁹ Such damage may occur when employees feel undervalued, unsupported, or treated unfairly.

Insider risk management activities typically focus almost exclusively on individual behaviors rather than also considering the context in which that behavior occurs. Social exchange theory, and associated research on employee-employer relationships, shows that individuals reciprocate their experience of their employer's treatment of them, whether that treatment is perceived as good or bad.¹⁰ Without due attention to the organizational context, insider misbehaviors can be repeated as a natural response to counterproductive management practices. Fortunately, threat-conducive organizational behaviors can be prevented, detected, and responded to as a means to reduce risk, just as insider misbehaviors can. And as an organization's insider risk program becomes known as a source of advocacy for the workforce and a means for improving employee work life, organizations can expect a reduction of insider risk and the associated investigative costs.

Figure 1 depicts the complexity of the insider risk management problem, which involves people, management, and organizational dimensions. Employees must balance their work (professional) and life (personal) stress with the supports they have to reduce, or otherwise manage, that stress. Both personal and professional stressors are a common factor in turning otherwise committed and loyal employees into insider threats. While a well-known cognitive attribution bias documents the tendency of managers to blame workers, and for workers to blame their environment, for problems that arise, overcoming these tendencies is essential to effective program function.

In addition, although the organization has a mission to accomplish, exclusive focus on the mission while sacrificing necessary infrastructure is counterproductive in the longer term. One essential piece of the organizational infrastructure is a well-oriented insider risk program, but remediation of insider incidents can be more complex than for outsider incidents. The way that the organization handles insider risk and responds to employee concerns may be deeply ingrained in its culture. However, an insider risk program can mitigate potential cultural issues by striking the right balance of policies, practices, and resources to support employees through work/life stressors, minimize attribution bias, and

⁹ A.P. Moore, T.M. Cassidy, M.C. Theis, D. Bauer, D.M. Rousseau, S.B. Moore, "Balancing Organizational Incentives to Counter Insider Threat," IEEE Workshop on Research in Insider Threat, May 2018.

¹⁰ We do not intend to imply that the victim organization is at fault in malicious insider attacks; most such insider incidents are violations of law or agreements with the organization that are prosecutable in court.

reasonably invest in organization infrastructure.

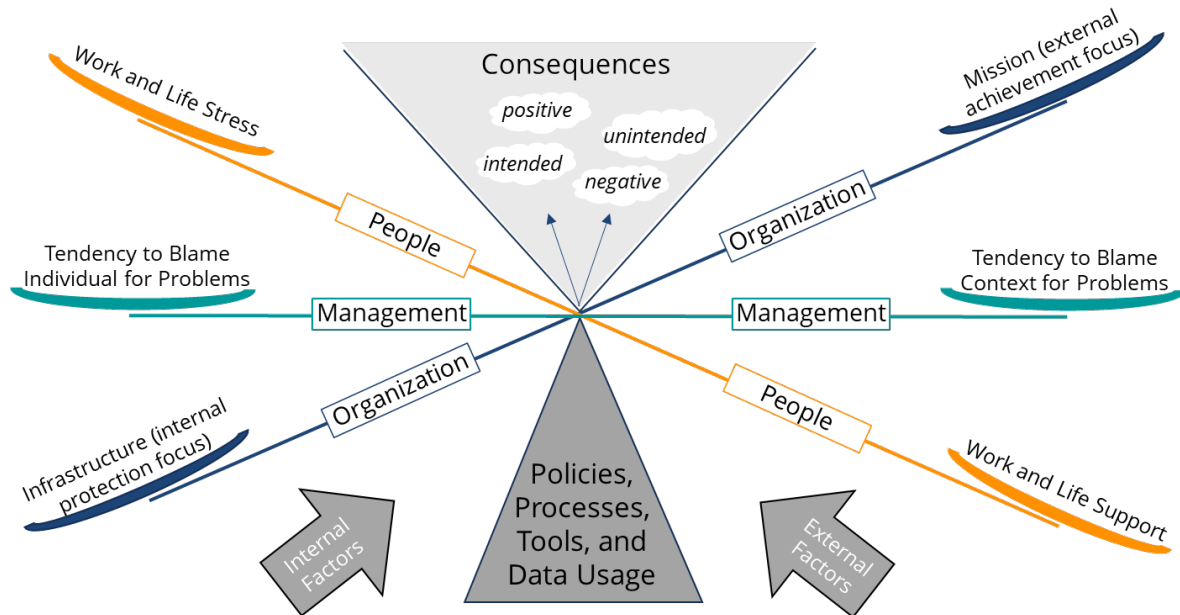


Figure 1: Complexity of Insider Risk Management

Insider risk management program policies, processes, tools, and data used to manage insider risk form the fulcrum by which balance can be promoted or undermined within an organization. Consequences arise as a result of the way an organization decides to manage its workforce. Consequences can be positive or negative, intended or unintended. Positive consequences are of course always desirable whether they are intended or not. Negative intended consequences can be thought of as realized risks that were understood and accepted as a part of doing business. Negative unintended consequences, on the other hand, are those that are most undesired, perhaps not understood or even identified, and thus possibly a surprise to the organization. Previous work has attempted to brainstorm potential negative unintended consequences of insider risk program policies and practices,¹¹ but we are unaware of efforts to elicit such consequences more systematically from practitioners.

Finally, a diverse set of internal factors (such as an organizational culture that can promote insider disaffection) and external factors (such as industry competition that can promote insider theft) varies greatly from organization to organization. While this variation makes it impossible to find a one-size-fits-all solution to these complexities, there are principles that apply to organizations in general.

¹¹ A. P. Moore, W.E. Novak, M.L. Collins, R.F. Trzeciak, and M.C. Theis. "Effective Insider Threat Programs: Understanding and Avoiding Potential Pitfalls," In SEI Digital Library. Pittsburgh, PA: Software Engineering Institute, 2015.

Primary Findings

The following identifies the primary findings from the analysis of the survey data. These findings will be elaborated in the subsequent sections of the report.

- Organizational Dimension
 - Institutionalization of insider risk programs within organizations is central to organizations' success. This includes ensuring the executive support for the program is consistent and communicated, funding for the program is sufficient, benefits of insider risk program are understood across the organization, and collaboration among the departments to share data takes place.
 - Respondents emphasized the need for incremental implementation, resisting "boiling the ocean" and promoting "start small, and build as you go" - an issue that will be explored in more depth in later sections of this paper. In addition, many advise new organizations to leverage existing processes and resources where possible, presumably from other risk management and cybersecurity related activities. Respondents also commonly advised establishing risk tolerances of what is the organization is willing to accept or not accept, and identifying and protecting the organization's "crown jewels."
- People Dimensions
 - Broad consensus and high levels of concern are indicated for a broad range of different insider threats, including both malicious acts involving disgruntled insiders or nation state actors, and unintentional threats involving reckless, untrained, or distracted actors. Although with less consensus, thieves and sympathizers to external influences were rated medium-high to high. Rated at a high level of concern were acts of insider financial fraud, sabotage, information/data theft, and workplace violence.
 - Respondents clearly indicated that many insider risks translate into quantifiable insider incidents. Organizational concern is justified by almost all respondents having experienced actual incidents over the last year, some in the hundreds of incidents. The detailed analysis shows that all of the event types were relevant for some organizations and, all sectors were negatively affected. While it is true that larger organizations (in terms of workforce size) have a greater potential for insider incidents, it is noteworthy that some large organizations had fairly few incidents and some small organization had many incidents in the last year.
- Management Dimension
 - Respondents most commonly rated negative consequences of insider risk controls as high for infringement of employee rights and civil liberties, as medium high for inhibiting productivity, and medium for undermining trust in the workforce and reducing retention of good employees.

- Recommendations for mitigating negative consequences included training and awareness, communication of program goals to employees, clear policies, alignment and collaboration across stakeholders (e.g., Legal, HR, Privacy, Security, and Physical Security), privacy-informed governance and controls, business-informed access controls, program audit and oversight, evidence-based and confidential investigations, and program performance management.
- Analytical Tools, Processes, and Data Sources
 - Most respondents indicated that the deployment of User and Entity Behavioral Analysis (UBA/UEBA) tools should be delayed until 2 to 3 years after the initial launch of the program. They most commonly indicated that the deployment of other tools they were questioned about are appropriate for initial launch, including User Activity Monitoring (UAM), Data Loss Prevention (DLP), Security and Information Event Management (SIEM), and Incident Case Management (IM). For DLP and SIEM, respondents with extensive experience are twice as likely as less experienced respondents to indicate delaying deployment.
 - A majority of respondents indicated that implementation of the following processes should be delayed until 2 to 3 years after the initial launch of the program: external source intelligence analysis, periodic/continuous employee threat evaluation, behavioral science methods to identify indicators, and evaluation of employee perceptions of working conditions. A majority felt that the focus of initial launch should include monitoring and analysis of select user activity and pre-employment screening. While not the most common response, over a third of respondents indicated that analysis of employee complaints and grievances should also come at initial launch.
 - There was a relatively even split on data sources recommended for initial launch and full rollout. The majority of the data sources that were recommended for full rollout are those that would have a greater complexity of implementation than those identified for initial launch. The most common response was to wait until 2 to 3 years after initial launch to use the following data sources (starred items indicate reaching a majority):
 - Administrative: Configuration change data*, Mobile device manager data, permission change monitor data*
 - Communication: Help desk ticket system data, telephone records data*
 - Network: Network packet tags, Wireless spectrum monitor data
 - Personnel: Corporate credit card records*, Performance evaluations*, Other personnel records
 - Security: Conflict of interest reports, Foreign contacts reports*, Travel reports*
 - Violation Reporting: Disciplinary records

Survey Design and Participation

Figure 1 provides a rough overview of the design of the survey used in our study, and the structure of the remainder of this paper. The next three sections reports on the people, management, and organizational dimensions of the results. We then develop a contextual model of the results thus far reported. The sections after that reports results associated with the insider risk program processes, tools, and data usage. To inform the incremental build of an insider risk program for organizations at various stages of progress, we asked survey participants to place the processes, tools, and data sources at the stage of development where they are most appropriately considered. Where insightful, we also distinguish the responses of more experienced practitioners from those with less experience to assess where results may be most insightful for emerging insider risk programs.

The survey questions are elaborated in the appendix. The primary targets of the survey are practitioners within organizational insider risk programs.¹² To reach these targets we surveyed organizations from the Open Source Insider Threat Information Sharing Group—a group moderated by the CERT that meets regularly to discuss operational issues related to insider risk programs in their organizations. As a means to compare the perspectives of the insider risk management practitioner with that of other business executives not necessarily focused on insider risk concerns, we also invited alumni of the Heinz Executive Education program to participate in the survey. Because we were primarily interested in the individual practitioner’s viewpoints, rather than the organizational perspective, multiple people from the same organization could respond to the survey.

While the survey responses of 73 individuals were used in our analysis, not all individuals responded to every question. Responding individuals held a variety of job positions in cybersecurity, HR, and legal professions. These individuals could be analysts, chief information security officers (CISOs), chief information officers (CIOs), chief human resources officers (CHROs), or legal counsel. As shown in Figure 2, respondents were generally knowledgeable and experienced with insider risk management, with well over half having fair to extensive and experience. Over 80% had been involved with creating an insider risk program within an organization.

¹² This population is hard to reach making it difficult to identify a representative random sample for the purposes of generalizing to the larger population. We therefore chose to survey the described convenience sample. While this non-probabilistic sample can introduce bias into the results, this is a reasonable approach for our current study as a means to explore the space of practitioner perspectives and provide a basis for generalizable research in the future.

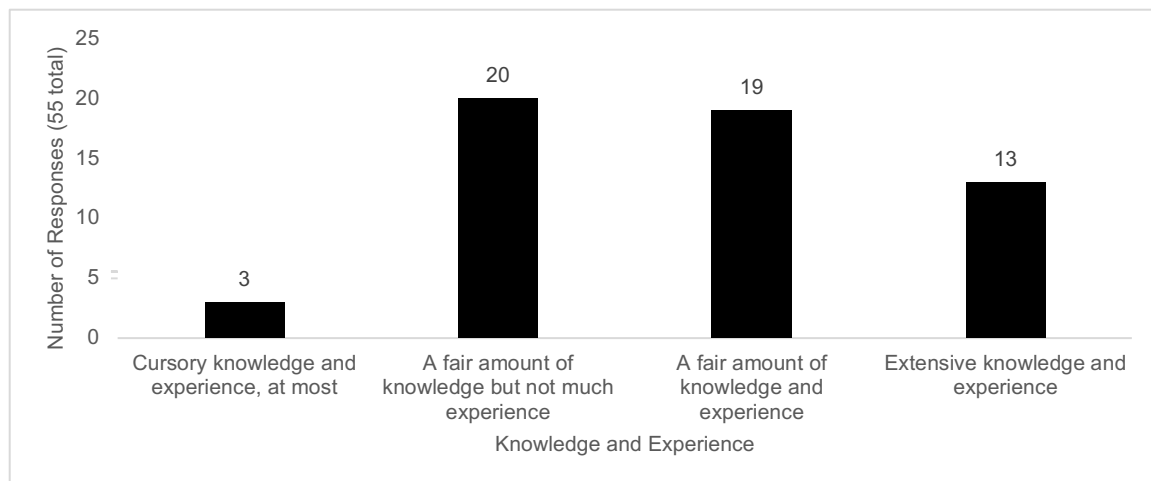


Figure 2: Knowledge and Experience of Survey Respondents

As shown in Figure 3, the respondents' current employer belonged to a wide range of industry sectors, with the Financial Services sector most represented by far. Over half of the respondents' organizations have over 10 thousand employees and only 2 of the organizations have over 100 thousand employees. In addition, over 90% of these organizations have active insider risk programs, with staffing indicated in Figure 4. Over half of the respondents monitor almost all of their employees as part of their program, with about 10% monitoring between 75% and 90%, and another 10% less than 75%.

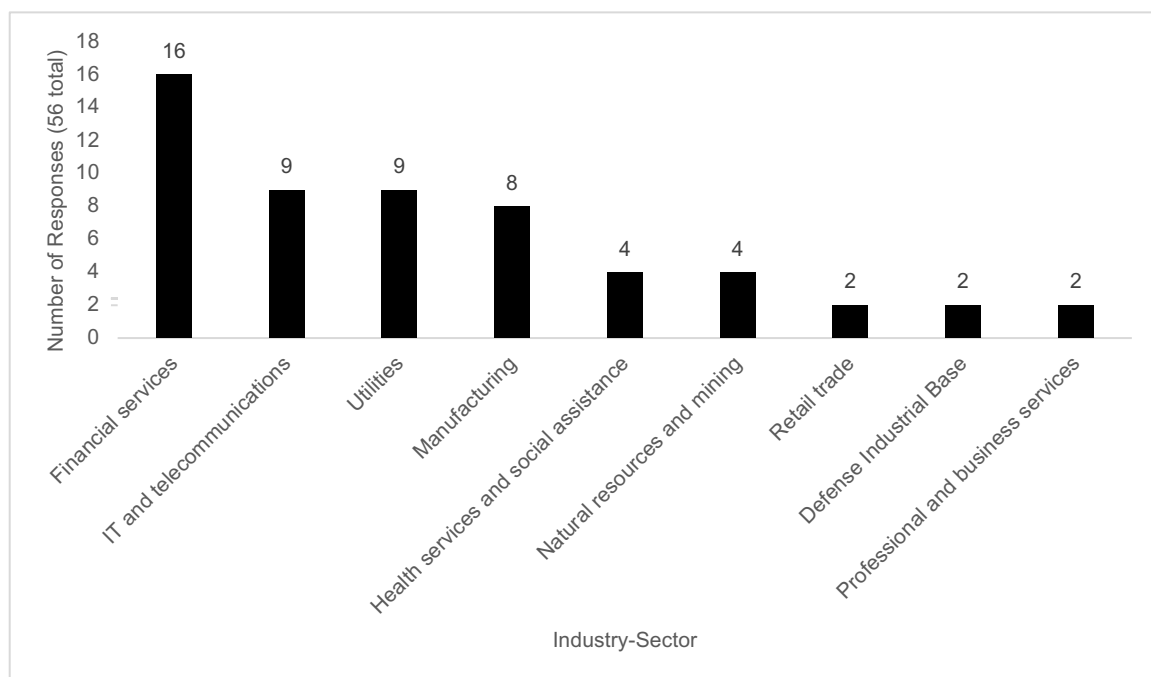


Figure 3: Industry Sector of Respondent's Organization

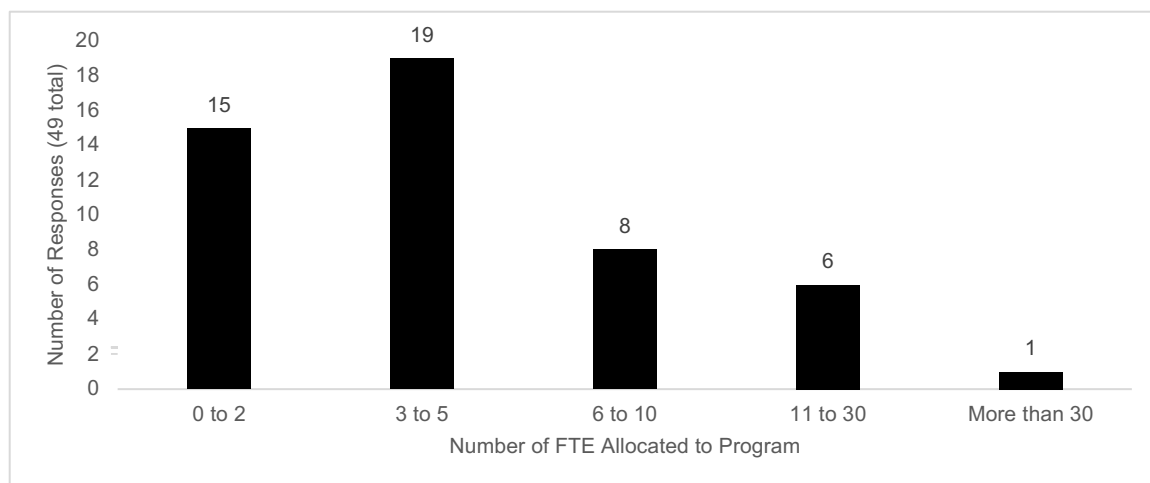


Figure 4: Staffing of Insider Risk Programs

The People Dimension

Respondents clearly indicated that many insider risks are realized operationally. While a well-balanced set of organizational policies and practices can optimize insider threat defense, it does not eliminate insider risk. External factors, such as an economic downturn or the value of an organization's intellectual property to competitors, can influence an insiders' decision to act counter to the organization's interests despite the strongest, most well-balanced defense. The range and frequency of insider incidents that organizations faced were inquired about in questions Q12 through Q16.

As summarized in Figure 5, survey respondents indicated broad consensus and high levels of concern for a wide range of different insider threats including both malicious acts involving disgruntled insiders or nation state actors, and unintentional threats involving reckless, untrained, or distracted actors. Although with less consensus, thieves and sympathizers to external influences were rated as a medium-high to high level of concern. Rated at a high level of concern were acts of insider financial fraud, sabotage, information/physical theft, and workplace violence. Less egregious and unintentional insider acts were rated of moderate concern as shown.

THREAT TYPE	THREAT EVENT	INCIDENT COUNT IN LAST YEAR
HIGH CONCERN • Thief • Disgruntled insider • Nation State • Reckless insider • Untrained/distracted insider	HIGH CONCERN • Financial fraud • Sabotage of capability • Information/data theft • Workplace violence	MALICIOUS • Over 5 incidents • 69% respondents • Over 10 incidents • 44% respondents • Over 100 incidents • 11% respondents
MODERATE CONCERN • Sympathizer to external influence • Irrational individual • Competitor	MODERATE CONCERN • Misuse of resources • Workplace harassment • Insiders tricked by outsider • Other accidental leakage • Physical theft	OTHER • Over 5 incidents • 84% respondents • Over 10 incidents • 58% respondents • Over 100 incidents • 13% respondents

Figure 5: Summary of Concerning Threats and Incident Frequencies over Last Year

Respondents clearly indicated that many insider risks translate into quantifiable insider incidents. Organizational concern is justified by almost all respondents having experienced actual incidents over the last year - some in the hundreds of incidents. The detailed analysis shows that all of the event types were relevant for some organizations and all sectors were negatively affected.

We adapted Intel's categorization of insider threats, splitting threats into those that are primarily malicious in question Q12 - Irrational Individual, Thief, Disgruntled Insider, Activist, Terrorist, Organized Crime Member, Competitor, Nation-State - and those that may be non-malicious in question Q13 - Reckless Insider, Untrained / Distracted Insider, Sympathizer to External Influences.¹³ Table 1 shows the current priority level within organizations for each insider threat type. While there was relatively low concern about activists, terrorists, and organized crime members, there was high concern over a broad range of other threat actors. There was also fairly high consensus over high levels of concern of two malicious threat types – disgruntled insiders and nation states – and two accidental insider threats – reckless insiders and untrained/distracted insiders.¹⁴

¹³ Intel Corporation, A Field Guide to Insider Threat, IT@Intel, White Paper, October 2015.

¹⁴ Reckless refers to "without thinking or caring about the consequences of an action" which is distinct from distractedness.

Table 1: Insider Threat Type Priority for Organizations

Indicate the current priority level for each of the following insider threats to your organization.						
Threat	Respondent Count	Low	Medium Low	Medium	Medium High	High
Irrational Individual	50				✓	
Thief	50					✓
Disgruntled Insider	51					✓
Activist	51	✓				
Terrorist	50	✓				
Organized Crime Member	49	✓				
Competitor	50			✓		
Nation-State	51					✓
Reckless Insider	53					✓
Untrained / Distracted Insider	52					✓
Sympathizer to External Influences	52				✓	

Legend
 ✓ Most common rating
 At least 40% respondents

Figure 6 shows that organizational concern is justified by almost all respondents with actual incidents over the last year, many in the tens and hundreds of incidents (questions Q15 and Q16).

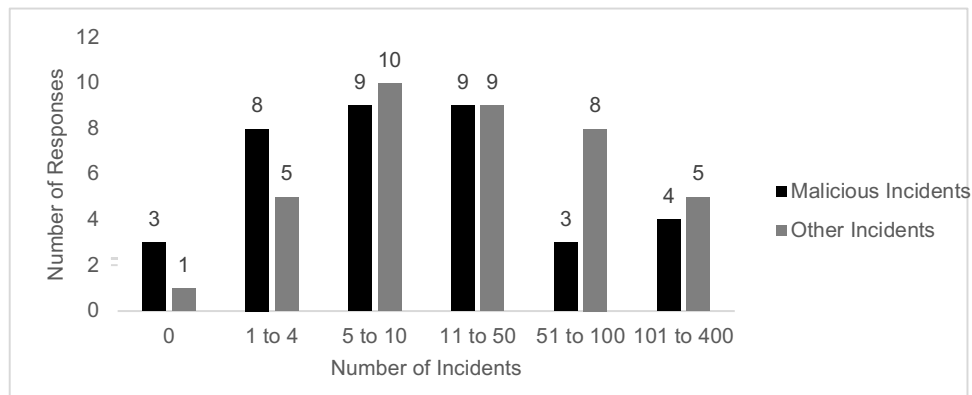


Figure 6: Incident Counts for Malicious and Other Types

Table 2 show the types of insider event types included in these estimates (when tracked by the organization) and their assessed priority level by the respondent (question Q14). Of note is that for no event type was the most commonly rated priority level below medium, and some of the event types – both malicious and accidental – had broad consensus of high priority for the respondent’s organization. The detailed analysis shows that all of the event types were relevant for some organizations and all sectors were negatively affected. While it is true that larger organizations (in terms of workforce size) have a

greater potential for insider incidents, it is noteworthy that some large organizations had fairly few incidents and some relatively small organization had many incidents in the last year.

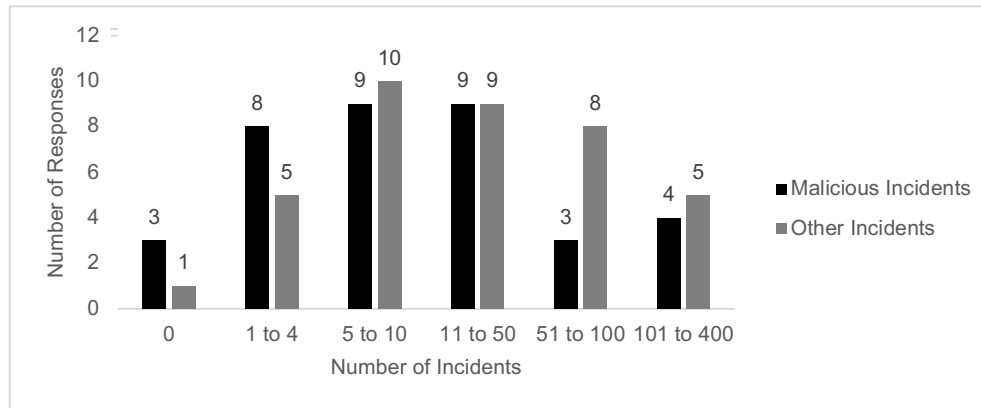


Figure 6: Incident Counts for Malicious and Other Types

Table 2: Priority Levels for Insider Event Types

Indicate the current priority level for each of the following insider event types for your organization.						
Threat	Respondent Count	Low	Medium Low	Medium	Medium High	High
Insider financial fraud	50					✓
Insider sabotage of operational capability	51					✓
Insider theft of information / data	51					✓
Insider physical theft	52			✓		
Insider workplace violence	49					✓
Insider misuse of organizational resources	51				✓	
Insider harassment in the workplace	51				✓	
Insiders tricked by outsiders	52				✓	
Other accidental leaks of information / data by an insider	52					✓

Legend

- ✓ Most common rating
- At least 40% respondents
- At least 60% respondents

The Organizational Dimension

An effective organization must balance the goals associated with achieving its mission with the needs of building an organizational infrastructure that can ensure resilience in the face of diverse threats. Institutionalization of insider risk programs within organizations is central to the program's success. Institutionalization as commonly defined in organizational maturity models promotes a way of doing business that is followed routinely as part of an organization's corporate culture. For insider risk programs,

as the survey results are summarized in the center of the Figure 7, predominant advice includes ensuring that the executive support for the program is consistent and communicated, funding for the program is sufficient, benefits of and commitment to the insider risk program are understood across the organization through workforce training and awareness, and collaboration among the departments to share data takes place.

Other advice by experienced insider risk practitioners is also shown in the figure. *Predominant* advice includes those recommendations that were most commonly cited by respondents. *Frequent* advice includes recommendations cited by at least five different respondents. While advice identified as *Key* was cited less commonly by respondents, organizations establishing an insider risk program should consider that advice carefully. For example, a continuous improvement perspective suggests a culture of learning, whereby an organization learns and adapts to what works best for the organization and its employees based on experience gained through incremental advances.



Figure 7: Summary of Survey Respondent Advice to Insider Risk Program Builders

The rest of this section describes these results in more detail.

Challenges and Barriers

Insider risk management programs are established to manage the insider risks to the organizational mission. Success depends on both individual and collaborative efforts. The above dynamics comes into play in establishing and refining insider risk management programs. While respondents were in broad agreement that many departmental stakeholders should be involved in insider risk decision making activities leading up to the initial program launch (question Q30), they also indicated a high level of agreement that collaboration is among the top challenges for organizations (question Q19). Table 3 shows at least 60% agreement that coordinating, communicating, and sharing information across the organization's business units is among the top agreed-upon challenges for insider risk programs. Specifically included in the need to be involved in insider decision making early on are Human

Resources, Information Technology, Physical Security, Executive Leadership, Enterprise Risk, Legal, and Privacy.

Table 3: Challenges of Insider Risk Management Programs

How extensive is the challenge of achieving each of the following for insider risk programs?						
Challenge	Respondent Count	Low	Medium Low	Medium	Medium High	High
Coordinating and communicating across business / operational units	50				✓	
Establishing the insider risk program scope and organizational structure	50			✓		
Ensuring compliance with all applicable legal requirements	50			✓		
Developing policy and formalizing the program	50			✓		
Incorporating insider risk controls for trusted business partners	49				✓	
Obtaining adequate funding for program operation	50					✓
Developing and administering insider threat awareness training	50			✓		
Hiring and retaining qualified insider risk program personnel	48				✓	
Sharing information across the organization's departments / units, including Human Resources (HR)	50				✓	

Legend	
✓	Most common rating
	At least 40% respondents
	At least 60% respondents

Table 3 also shows high (or medium high) ratings for the challenge of obtaining adequate funding for program operation and incorporating insider risk controls for trusted business partners. The most common answer associated with all of the challenges identified as part of question Q19 were given a medium or above rating of challenge priority.

As shown in Figure 8, an open-ended question regarding the biggest barrier to insider risk mitigation today (question Q33) shows agreement in the importance of socio-cultural issues regarding training, awareness, and culture presumably at both an individual and departmental level.

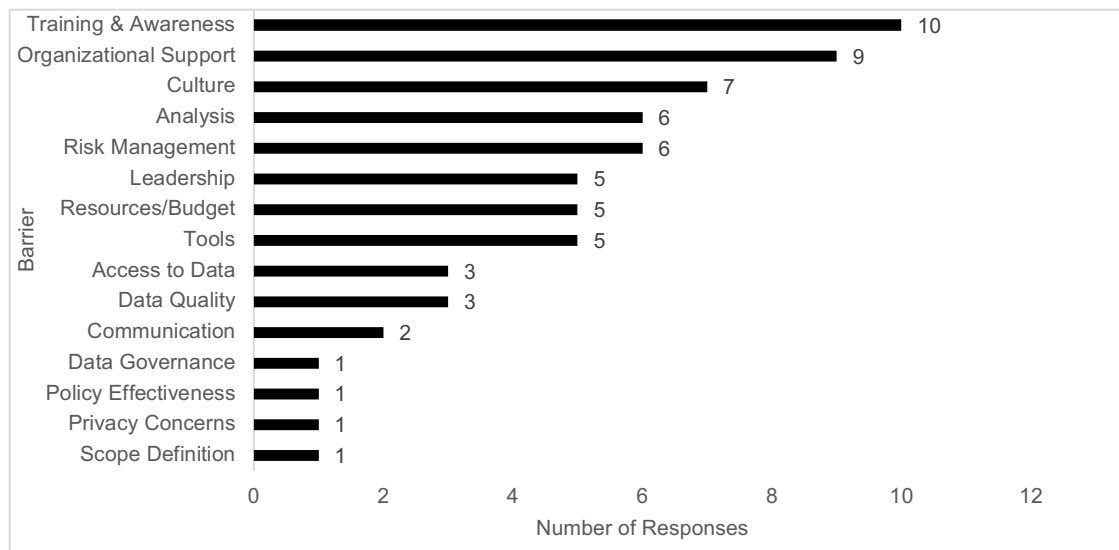


Figure 8: Barriers to Establishing Insider Risk Programs

Barriers to organizational support for the insider risk program mission also rated highly, which includes getting stakeholders to buy-in to the program. Cultural issues blended with the barriers to training and awareness in that some stakeholders are not really understanding insider risk as a concept, or seeing it as strictly at odds with employee privacy.

Practitioner Advice to Insider Risk Programs

Figure 9 shows the results associated with an open-ended question (question Q30) regarding the respondent's advice for organizations establishing a new insider risk program. Here again, there is broad agreement that insider risk programs need to focus on obtaining executive sponsorship for the program and ensuring collaboration of stakeholders across the organization, at the department and individual levels. The consistency of these issues, which were seen as major challenges for the organization and a centerpiece of the advice for new programs, suggests that they are fundamental to program success.

A second level of advice is to focus on incremental implementation, resisting “boiling the ocean” and promoting “starting small, and build as you go”: an issue that will be explored in more depth in later sections of this paper. In addition, many advise new organizations to leverage existing processes and resources where possible, presumably from other risk management and cybersecurity related activities. Respondents also commonly advised to establish risk tolerances of what is the organization is willing to accept or not accept, and identifying and protecting the organization's “crown jewels.”

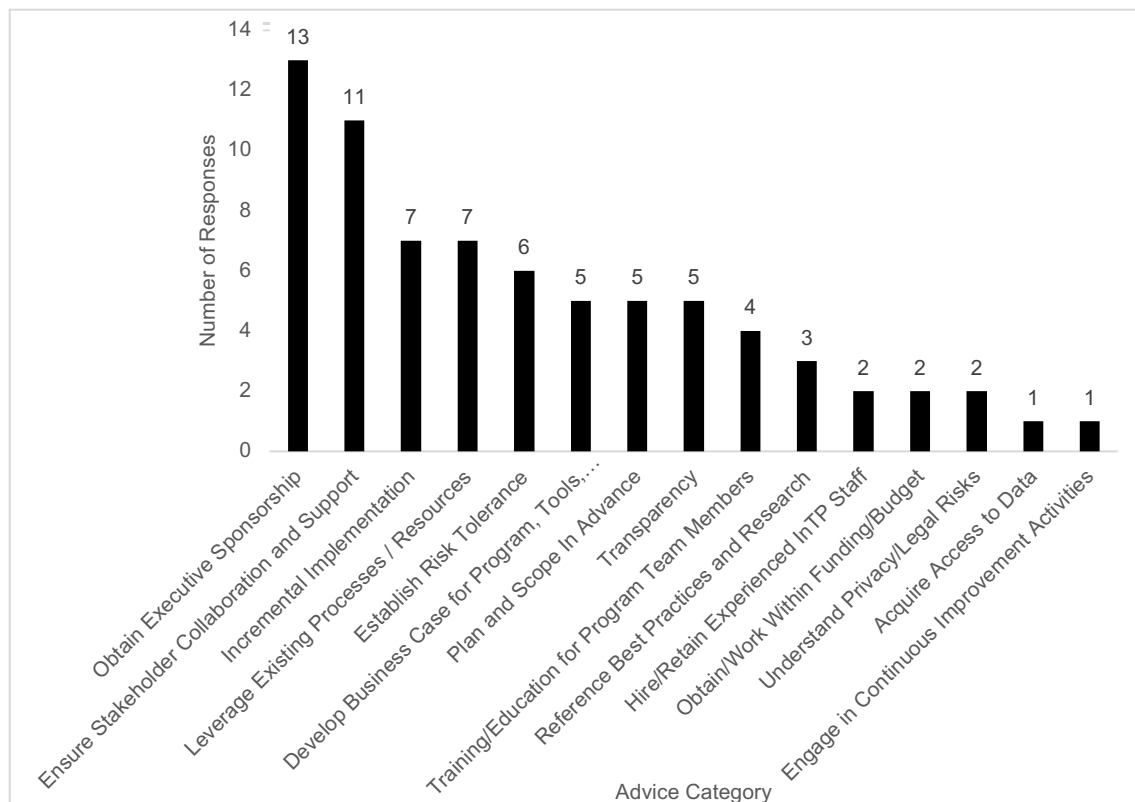


Figure 9: Advice for Organizations Establishing a New Insider Risk Program

The prevalence of institutionalization factors is consistent in question 32 when participants were asked for the one factor or practice that is most important for an organization to get right to mature its insider risk program, as seen in Figure 10. Stakeholder Collaboration and Support emphasized the need for two-way collaboration and support, having the other key partners helping to shape the program, but also the program reaching out for more support when needed. Respondents promoting the need for upfront (or prior) program planning and scoping suggested having a vision in place before you start building the program out or buying tools. Also noteworthy in establishing a Communication/Business case is

- being able to develop and communicate the justification for the program, acquisition of tools, staffing, etc.
- being able to draw out why the program matters in metrics that others in the organization understand.

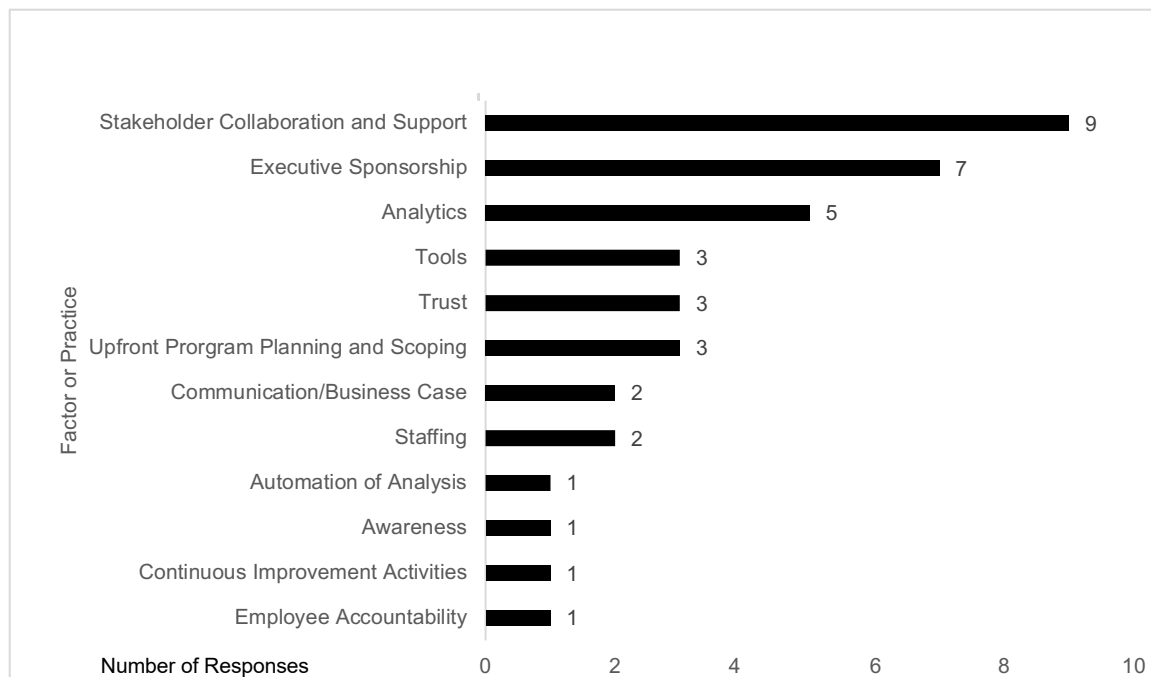


Figure 10: Most Important Factor or Practice According to Respondents

Management-level operational performance measures inquired about had broad consensus of a medium-high level of importance in insider risk management decision making. The measures identified in question 20 include the number of cases, number of monitored employees, number of cases escalated for review, number of findings per year, and number of incidents avoided due to technical controls.

The Management Dimension

As mentioned, an imbalance of organizational policies and practices can add stress to employees' lives, both professionally and personally. The survey questioned the extent of concern associated with potential negative unintended consequences (question Q17) selected from previous research.¹⁵ While there was not broad agreement about the extent of concern in the various categories of negative consequences, Table 4 shows the most common response categories. A high rating of concern is indicated regarding the program infringing on employee privacy rights and civil liberties, justifying the earlier recommendations of having legal and privacy involved with decision making from the very beginning of program establishment. In general, more experienced respondents had higher concern for the negative unintended consequences than less experienced respondents.

¹⁵ A. P. Moore, W.E. Novak, M.L. Collins, R.F. Trzeciak, and M.C. Theis. "Effective Insider Threat Programs: Understanding and Avoiding Potential Pitfalls," In SEI Digital Library. Pittsburgh, PA: Software Engineering Institute, 2015.

Table 4: Concern Over Potential Negative Unintended Consequences

To what extent are you concerned about each of the following potential negative unintended consequences for insider risk programs?						
Negative Unintended Consequence	Respondent Count	Low	Medium Low	Medium	Medium High	High
Insider risk controls inhibiting productivity	51				✓	
Undermining trust between management and other employees	51			✓		
Undermining trust among all employees	51			✓		
Reducing retention of good employees	51			✓		
Undermining goodwill of good employees	51			✓		
Investigations unfairly affecting employee careers	51	✓				
Workplace becoming more confrontational	51	✓				
Infringing on employee privacy rights and civil liberties	51					✓

Insider risk controls inhibiting productivity, e.g., possibly through overly constraining role-based need-to-know controls, are most commonly rated medium-high. The next set of negative consequences commonly rated at medium concern reflect respondents' concern that insider risk programs will undermine good relations among employees and between employees and management, possibly reducing retention of good employees. Despite this concern, low concern was commonly indicated for insider risk programs making the workplace more confrontational or unfairly affecting employee careers, e.g., through indiscreet investigations of suspected but innocent employees.

Forty respondents provided recommendations to mitigate negative unintended consequences. The responses were affinity-grouped and categorized. Several themes emerged in these responses, with respondents offering between one and five recommendations. The most common recommendation was to provide training and awareness opportunities. Within that, some specific training goals included that employees understand what is expected of them (e.g., policies and acceptable behaviors) and how to report potential incidents. Additionally, two of these respondents suggested that unintentional incidents be treated as a coaching or learning opportunity, as opposed to having a purely punitive outcome.

Closely related to training and awareness was the recommendation to clearly communicate insider risk program goals to employees. This recommendation involved clarifying for employees the rationale for having a program, specifically that insider risk programs are intended to protect both the organization and its employees. The intent of communication to employees about the program was two-fold: 1) transparency and 2) supporting a collaborative as opposed to an adversarial relationship between employees and the program. Clear policies were identified as a priority, with Acceptable Use Policy (AUP) and Code of Business Conduct as exemplars. Again, this would be closely related to training and awareness and communication of program goals.

Another highly-recommended practice was ensuring alignment and collaboration across program stakeholders, including other program offices. In particular, respondents highlighted Human Resources (HR) and/or Legal/General Counsel as a part of the organization to coordinate with. Other

stakeholders of mention include security, privacy, cyber, business units, physical security, and risk management. The general practice in this case involves building relationships across the organization in order to support decision-making of the insider risk program.

Respondents recommended privacy-informed governance and controls for programs. Suggested practices included having the privacy office as part of the insider risk governance committee, or at least as a partner; masking or anonymization of subject/employee personal information wherever possible, including in HR or personnel records; and compliance with privacy-related regulations. Conversely, some respondents recommended communicating to employees that they should not have any expectation of privacy on company-owned devices; this was not counted within the training and awareness or communication of program goals recommendations.

Two practices emerged related to investigations: investigations should be 1) evidence-based and 2) handled discreetly and confidentially. Access controls were the subject of several respondents' recommendations. Aside from modifying access controls and audit protocols more generally, the more specific best practice suggested was ensuring that the business is considered and consulted when constructing controls. Several respondents recommended program audit and oversight, which is inclusive of what is more informally known as "watching the watchers," as well as overall program governance by a committee of internal stakeholders. Another two practices emerged related to program performance management, including maintenance and reporting of metrics as well as review of training activities.



Figure 11: Recommendations for Mitigating Negative Unintended Consequences

Unique responses (i.e., those that were offered by only one respondent) included: obtaining executive sponsorship, reminders about an Employee Assistance Program (EAP) as a resource, having a reporting campaign, and ensuring that the program's policies and practices align with the overall organizational culture.

Table 5 demonstrates how the recommendations from respondents may correspond to the negative unintended consequences presented to them. For the sake of clarity, unique responses are omitted.

Mitigations with an asterisk identify those mitigations that were most commonly identified by respondents.

Table 5: Mapping of Negative Unintended Consequence to Potential Mitigations

Negative Unintended Consequence (Prioritized)	Potential Mitigations (most common recs are starred)
Infringing on employee privacy rights and civil liberties	Evidence-based and confidential investigations* Privacy-informed governance and controls
Insider risk controls inhibiting productivity	Business-informed access controls
Undermining trust among employees and between employees and management	Training and awareness* Communication of program goals to employees* Clear policies*
Undermining goodwill of good employees	Training and awareness* Program audit and oversight Communication of program goals to employees*
Reducing retention of good employees	Program performance management
Investigations unfairly affecting employee careers	Evidence-based and confidential investigations*
Workplace becoming more confrontational	Communication of program goals to employees*

Contextual Model of the Insider Risk Management Problem

This section refines the insider risk management problem as illustrated in Figure 1 through the lens of the results in the previous sections as well as previous research. We use a modeling approach called causal loop diagrams to represent this refinement.¹⁶ Previous research found that workforce management practices that damage employees' Perceived Organizational Support (POS) correlate with increased intentional insider misbehaviors.¹⁷ POS involves employee perceptions that their employer values their contributions, cares about their well-being, and treats them fairly. POS-based practices generally fall into the areas of organizational justice, rewards and recognition, organizational communication, and direct supervisor support. These practices promote the insider goodwill essential to both keeping insider risk to a minimum and ensuring organizational success generally.

Workforce management practices that bolster POS serve to improve employees' organizational commitment in a way that complements traditional security practices to provide a more holistic risk management balance. In general, we view *supportive practices* as creating *positive attitudes* in the workforce resulting in *positive deterrence* of insider threat. This contrasts with Deterrence Theory and criminology generally which is usually focused on what we would call *negative deterrence*, attempting to force rather

¹⁶ Causal loop diagrams (known more generally as influence diagrams) map the causal influences between variables important to representing the problem. Causal influences are represented as directed arrows with a polarity symbol (plus or minus) attached to represent pair-wise relationships. A plus sign represents a direct relationship between the variables in that the variables move in the same direction, i.e., as the source variable increases, the destination increases; and as the source variable decreases the destination variable decreases. A minus sign represents an inverse relationship between the variables, i.e., the variables move in opposite directions.

¹⁷ A.P. Moore, T.M. Cassidy, M.C. Theis, D. Bauer, D.M. Rousseau, S.B. Moore, "Balancing Organizational Incentives to Counter Insider Threat," IEEE WRIT, 2018.

than attract individuals to proper behavior. Supportive practices that align the workforce values and attitudes with the organization's objectives form a foundation on which to build security practices that rely on forcing functions. Of course, negative deterrence is always going to be needed since some insiders will act out no matter how supportive the environment due to other factors, but a combination of positive and negative deterrence can improve the effectiveness and efficiency of the insider threat defense over negative deterrence alone.

Figure 12 provides a causal loop diagram that puts the above in perspective. Sustainable mission accomplishment, as shown in the upper right, is the primary objective of most organizations. Insider incidents have the often-realized potential to negatively affect an organization's mission. Most organizations focus on reducing insider risk through a negative deterrence approach to put more effort into hardening systems and detecting suspicious behaviors, as seen in the blue feedback loop. While such efforts are necessary, they should not significantly detract from positive deterrence efforts.

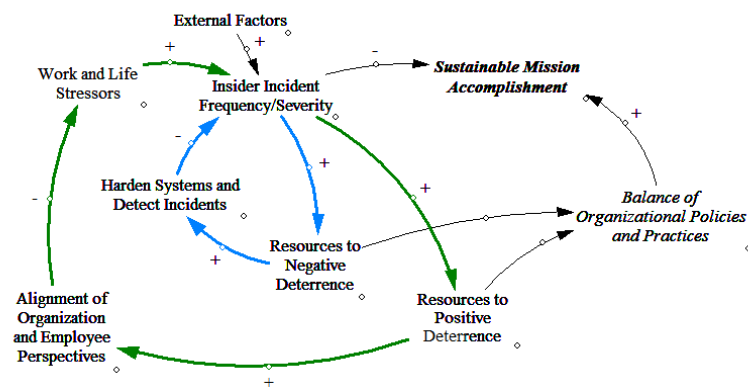


Figure 12: The Basic Organizational Balancing Act

The vast majority of insider incidents are perpetrated by individuals who started out in their organizations as committed and loyal employees. But as professional (work) and/or personal (life) stressors intervened, they found themselves motivated to act counter to their employer's interests.¹⁸ The green feedback loop in Figure 12 shows that positive deterrence can align the organization and employee perspectives in a way that can reduce work/life stressors, and disincentivize insider misbehaviors.

As shown in the middle right of the figure, it is the combination of positive and negative deterrence that determine the balance of organizational policies and practices.¹⁹ Balance does not necessarily mean equal weighting of the two approaches. An appropriate balance depends on the nature of the subject organization. Organizations accustomed to top-down command and control (as in the military) may be perfectly fine with insider threat defense focused primarily on negative deterrence. Organizations that

¹⁸ E. Shaw, L. Sellers, "Application of the Critical-Path Method to Evaluate Insider Risks," *Studies in Intelligence*, Vol. 59, No. 2, June 2015.

¹⁹ Since it is a balance that is the subject of these relationships, no polarity signs are attached to these arrows.

rely on highly skilled workers that are in short supply in a competitive domain may require a balance more weighted on the positive deterrence side.

As mentioned previously along the organizational dimension, an effective organization must balance the push to achieve its mission with the needs of building an organizational infrastructure that can sustainably ensure resilience in the face of myriad threats. Figure 13 extends the model to depict the basic relationships involved. Survey results showed the importance of executive support for the insider risk program and institutionalization of the program to ensure adequate funding and collaboration across the organization, especially for sharing data essential to the program mission. All of this helps to ensure good mission-infrastructure balance, which contribute to appropriate policies and practices and sustainable mission accomplishment.

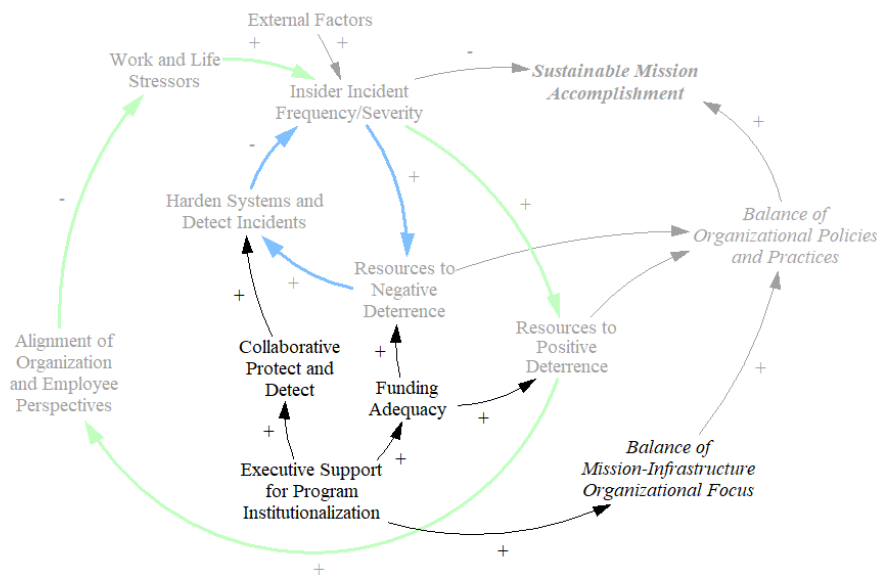


Figure 13: Core Challenges of Achieving Mission-Infrastructure Balance

An imbalance of an organizations mission and infrastructure can occur either as too narrow of a focus on mission or on infrastructure. Such imbalance can occur as an organization hires staff members and forms departments within the organization as a means to accomplish its mission. The organization develops objectives for the department or staff member to ensure mission success. Of course, the organization and its mission also depend on the collaboration of organizational departments and individual staff members to achieve its mission. As time goes on, however, the individual focus can take on a counterproductive life of its own and detract from the collaborative needs of the organization, resulting in undermining the mission. There are many aspects to program institutionalization that are evident in survey responses, but this notion of cross-organization collaboration is central.

Figure 14 extends the model to include the relationships associated with negative unintended consequences of insider risk programs viewed as concerning by survey respondents. Many of the unintended

consequences are shown to arise from negative deterrence approaches to hardening systems and increasing detection capabilities, as seen in the middle-left side of the figure:

- Excessive attempts to harden systems that restrict access, e.g., based on need-to-know, can make doing one's job more cumbersome, possibly even less efficient or effective. Neither employees nor managers will be happy with the reduced productivity that can result
- Attempts to improve detection capabilities, including earlier detection of potentially suspicious behaviors, may involve increased reporting by managers and coworkers – “See Something, Say Something” campaigns are increasingly popular. While such approaches can be valuable there is the potential for them to negatively affect trust in the workplace. Coworker trust is necessary for effective workplace functioning, and can influence workplace stress.
- Trust between management and the workforce is also vital. Overly-aggressive suspicious behavior detection and investigation can lead to false allegations and infringement of employee privacy expectations, negatively affecting employee-manager trust. Attribution bias can exacerbate this situation by having managers tending to blame workers for problems caused by the workplace context, and having workers tending to blame the workplace context for problems of their own making.²⁰

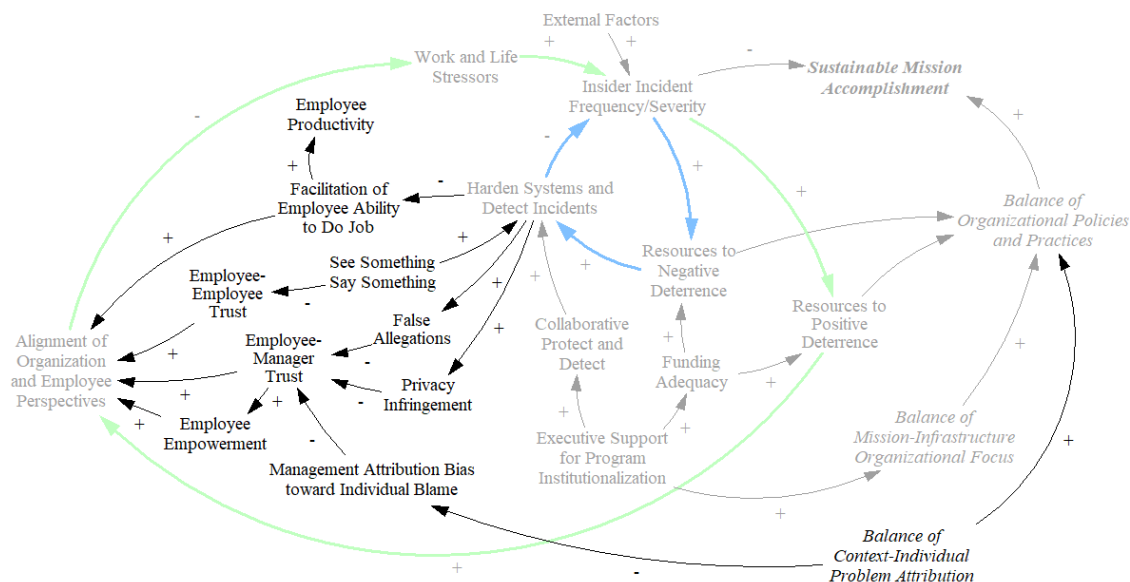


Figure 14: Challenge of Balancing Positive and Negative Deterrence

Balancing the context-individual problem attribution can be a means to both improve the trust relations within the workplace and improve the alignment between the employee and the organization, thus reducing work and life stressors. This is where POS can pay big dividends; employers who express

²⁰ Attribution bias is a well-known cognitive bias in the cognitive psychology literature.

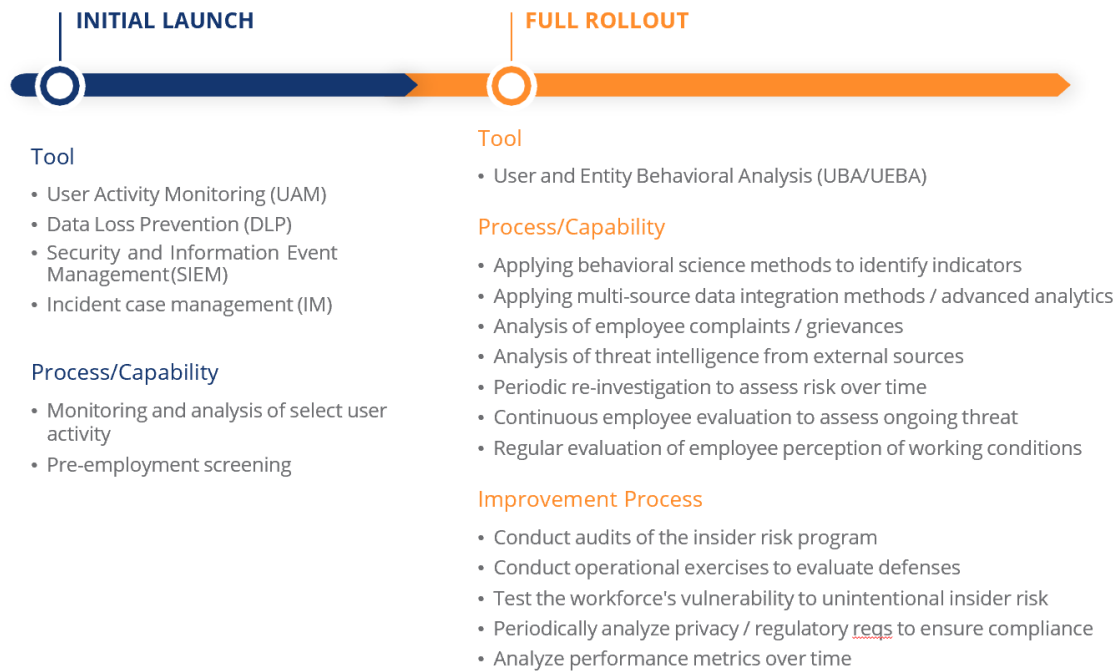
positive value for their employees' contributions, demonstrate care for their well-being, and treat them fairly will help employees manage their work and life stress. Empathic managers that support employees through difficult times, both personally and professionally, can help. Within the insider risk program, investigators that look for both confirming and disconfirming evidence of wrongdoing can reduce the negative impacts of false positives identified using available technology. Attribution bias can be difficult to overcome, but organizational training and supportive policies and practices can help to achieve a good balance and sustain the mission in the long term.

A well-balanced set of organizational policies and practices can avoid negative unintended consequences of an insider risk program, creating a net positive for both the employee and the organization. In effect, a balanced program can cause employees to view traditional insider risk controls as a more appropriate function of the enhanced relationship between the organization and its employees.

Incremental Program Building: Analytical Tools, Processes, and Capabilities

The survey includes three questions on tools, processes, and capabilities (questions 21 to 23). These questions were structured to determine when in what insider risk program implementation phase each item would best be implemented. The phase options are *initial launch* - the first year of the program - and *full rollout* - about two to three years after program launch. We also had an option for *enhanced rollout* involving five or more years after program launch, but this was not a most common response for any item. Table 6 provides an overview of the recommendations with the detail provided in subsequent sections.

Table 6: Overview of Most Commonly Recommended Deployment or Implementation



Tools

Table 7 shows that of the five tools covered by the question, only one had more than 50% of respondents recommend waiting until full capability to implement: user and entity behavioral analysis. Although we cannot know the exact reason for this, presumably respondents consider the tools recommended for initial launch to be essential to program development and think that beginning to gain experience with them from the start is important. Available tools are usually built by different vendors and their integration can be quite challenging. It makes sense to start the journey of integration of tools with business processes and other technology early during initial launch when simpler insider risk management processes and data sources are the focus.

It is noteworthy that the values between UAM and UBA/UEBA for initial launch and full capability are reversed. However, it is not the case that respondents simply answered initial for one and full for the other—the reversed values are the result of changes in responses across all three implementation phases.

One respondent included “Other” as a response and pointed out that during initial launch, the insider risk program should use other tools that the organization already has in place.

When analyzing the data by sector, there are no major differences in the responses. When looking at responses based on respondent experience level, the notable differences are for data loss prevention and security and information event management. For both of these tool types, respondents with extensive experience are twice as likely than the other levels to choose a non-initial launch response.

Table 7: Recommended Deployment of Tools

When would you recommend the deployment of the following tools in the development of an insider risk program?				
Tool	Respondent Count	Initial Launch	Full Capability	Enhanced Capability
User Activity Monitoring (UAM)	48	✓	*	
User and Entity Behavioral Analysis (UBA/UEBA)	50	*	✓	
Data Loss Prevention (DLP)	51	✓		
Security and Information Event Management (SIEM)	49	✓		
Incident Case Management (IM)	47	✓		

Legend
 ✓ Most common rating
 At least 50% respondents
 At least 75% respondents
 * At least one-third (33.3%) respondents

Tools for Initial Launch

As shown in Figure 15, the user activity monitoring, data loss prevention, security and information event management, and incident management tool answer were all heavily in favor of implementation at initial launch. With the exception of UAM, each tool had around 70% to 75% of respondents answer initial launch.

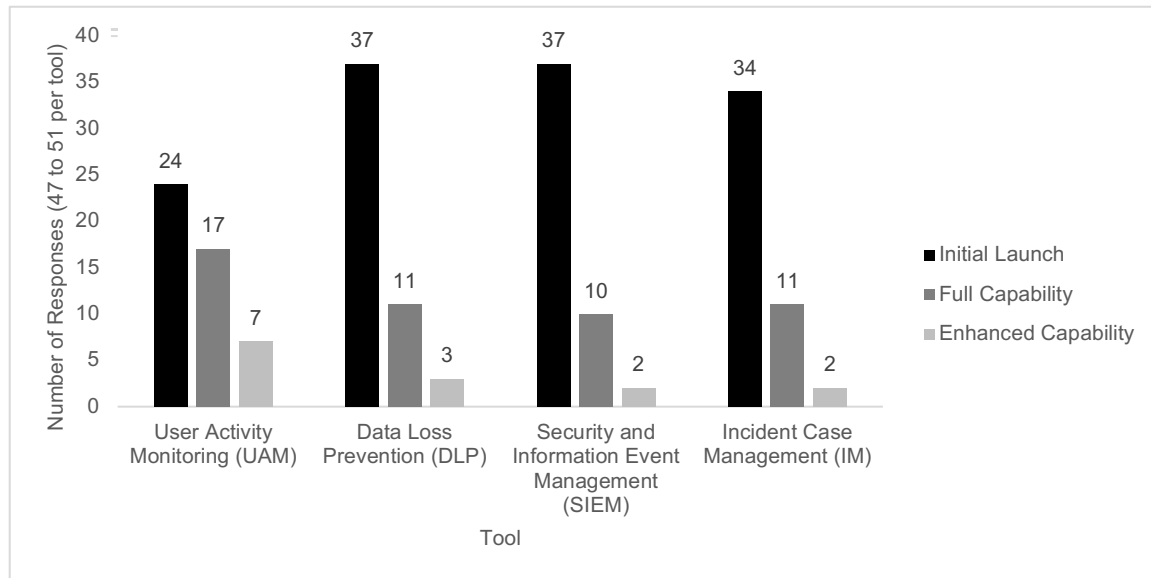


Figure 15: Tools for Initial Launch

Tools for Full Capability

User and entity behavior analysis tools were the only tool type that the majority of respondents indicated as being most appropriate for implementation once at full capability, as illustrated in Figure 16. Even so, a full third of respondents felt these tools were appropriate for initial program launch.

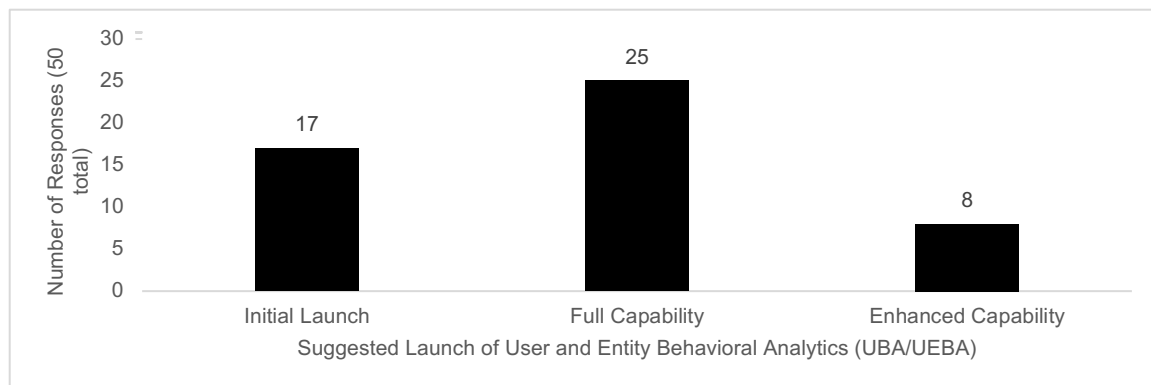


Figure 16: UEBA Suggested for Full Capability

Processes and Capabilities

For implementation of processes and capabilities, the most common response for each all had at least 45% of respondents selecting the response, as outlined in Table 8. This question had the most respondent select enhanced capability for options, with five of the nine having at least 20% of responses be enhanced capability. These are:

- Applying behavioral science methods to identify indicators
- Applying multi-source data integration methods and advanced analytics
- Periodic re-investigation to assess risk over time
- Continuous employee evaluation to assess ongoing threat
- Regular evaluation of employee perception of working conditions

As for the tools question, there are no major sector differences in responses. Looking at the differences between respondent experience level, there are notable differences for four items:

- For “applying multi-source data integration methods and advanced analytics”, knowledgeable and experienced respondents are more than twice as likely to choose enhanced capability than those with extensive experience.
- For “analysis of threat intelligence from external sources”, knowledgeable respondents are about twice as likely as those with more experience to choose initial launch.
- For “periodic re-investigation to assess risk over time”, knowledgeable respondents choose enhanced capability about twice as often as the other levels. Experienced respondents have a fairly even distribution of responses. Those with extensive experience however, choose full capability about 80% of the time.
- For “regular evaluation of employee perception of working conditions”, only a small number of respondents with extensive experience placed the process as for initial launch. The other experience levels both had a more even distribution of answers.

Table 8: Recommended Deployment of Processes

When would you recommend the implementation of the following processes and capabilities in the development of an insider risk program?				
Process / Capability	Respondent Count	Initial Launch	Full Capability	Enhanced Capability
Monitoring and analysis of select user activity	48	✓		
Applying behavioral science methods to identify indicators	47		✓	
Applying multi-source data integration methods and advanced analytics	49		✓	
Analysis of employee complaints / grievances	47	*	✓	
Analysis of threat intelligence from external sources	49		✓	
Pre-employment screening (e.g., background checks, credit checks, or interviews)	49	✓		
Periodic re-investigation to assess risk over time	42		✓	
Continuous employee evaluation to assess ongoing threat	47		✓	
Regular evaluation of employee perception of working conditions	46		✓	

Legend

- ✓ Most common rating
- At least 50% respondents
- At least 75% respondents
- * At least one-third (33.3%) respondents

Processes for Initial Launch

Overall, the processes are more likely to be selected for implementation during full capability. Only monitoring and analysis of select user activity and pre-employment screening were indicated by the majority of respondents as most appropriate during initial implementation as shown in Figure 17.

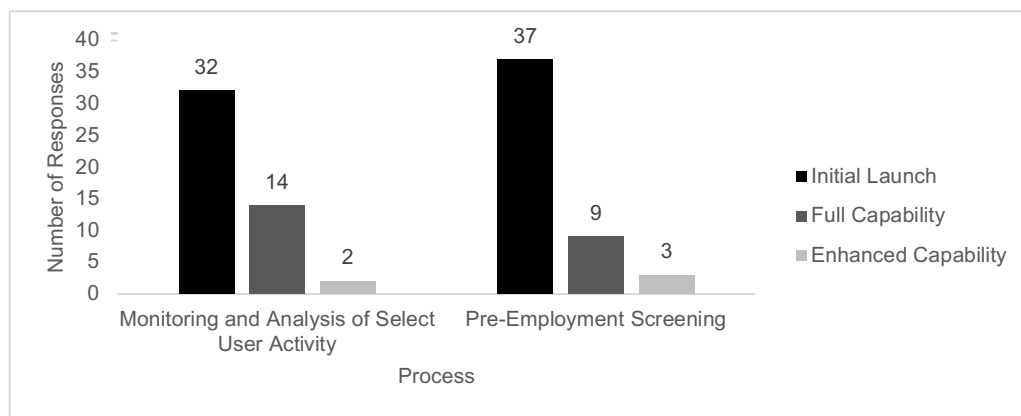


Figure 17: Processes for Initial Launch

Processes for Full Capability

While each of the seven other processes all favored implementation during full capability as shown in Figure 18, the distribution of answers between initial launch and enhanced capability is much closer than for other questions. Though the tendency is slightly towards initial launch, it is only slight. Overall for these questions, 52% of the non-majority answers are initial launch and 47% are enhanced capability.



Figure 18: Processes for Full Capability

Improvement Processes

Overall, Table 9 shows that improvement processes were recommended to coincide with full capability of insider risk programs. There were no major sector differences, but there are some slight experience level differences.

Table 9: Recommended Deployment of Improvement Processes

When would you recommend the implementation of the following improvement processes in the development of an insider risk program?				
Improvement Process	Respondent Count	Initial Launch	Full Capability	Enhanced Capability
Conduct audits of the insider risk program	51		✓	
Conduct operational exercises to evaluate defenses	50		✓	
Test the workforce's vulnerability to unintentional insider risk (e.g., social engineering)	50	*	✓	
Periodically analyze privacy and regulatory requirements to ensure organizational compliance	51	*	✓	
Analyze performance metrics over time	49		✓	

Legend

- ✓ Most common rating
- At least 50% respondents
- * At least one-third (33.3%) respondents

The details of the response are shown in Figure 19, with a few observations apparent:

- For “conduct operational exercises to evaluate defenses”, only a few experienced respondents selected initial launch and they chose enhanced capability about twice as often. The other two experience levels had answers that were more evenly distributed.
- For “test the workforce’s vulnerability to unintentional insider risk”, those respondents with extensive experience chose enhanced capability about twice as often and initial launch at about half the rate of the other two experience levels. Respondents at the knowledgeable and experienced levels answered initial launch and full capability at about the same rates.
- For “analyze performance metrics over time”, no respondent with extensive experience chose enhanced capabilities. For these respondents the answers were closely split, with a slight preference for full capability.

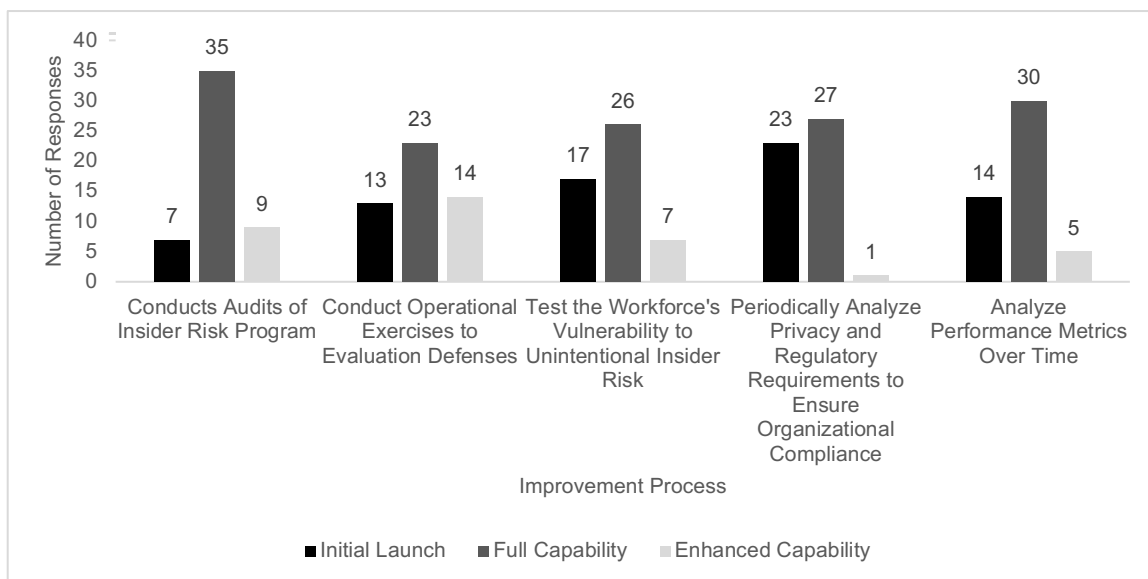


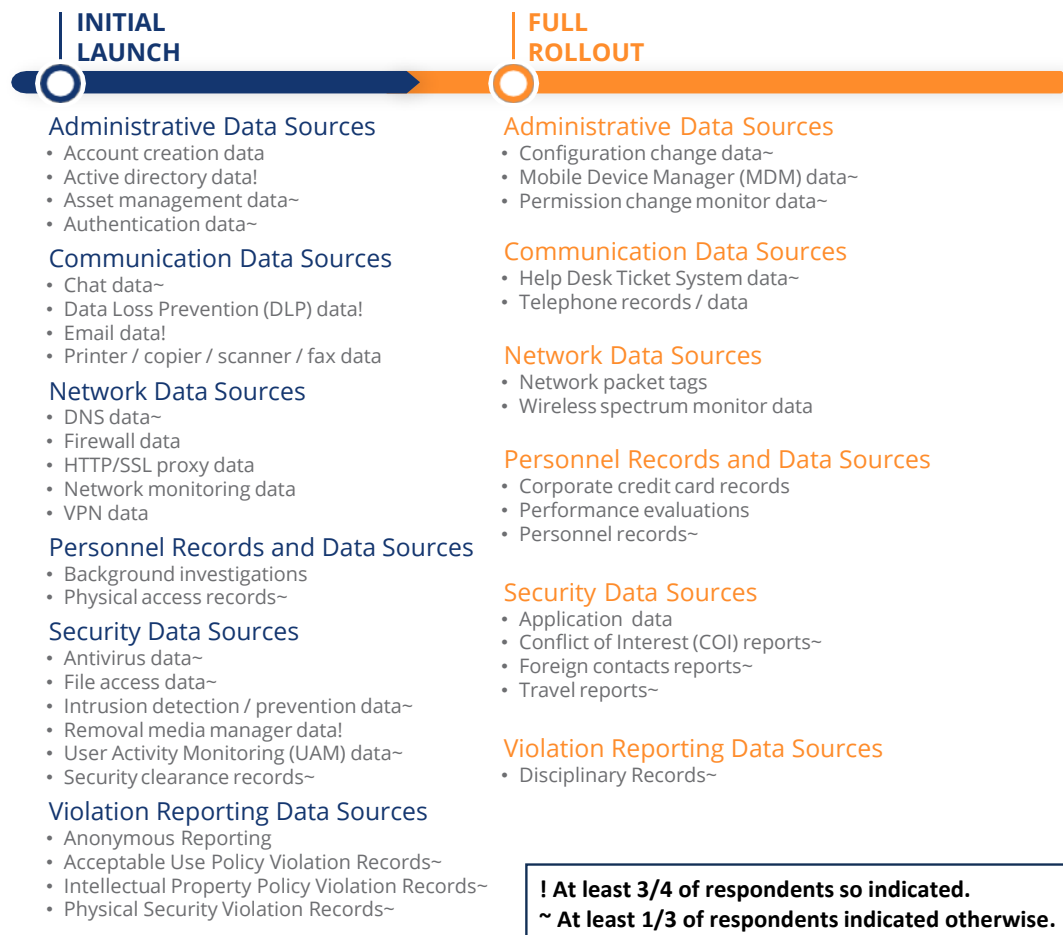
Figure 19: Improvement Processes for Full Capability

Incremental Program Building: Data Sources

Of course, monitoring insider behaviors is an essential aspect of any insider risk program. Organizational data sources provide insight into insider behaviors but their integration into insider threat analytics can be complex. The variety of available data sources adds to this complexity. Table 10 provides an

overview of the most commonly recommended phase for usage of data in the insider risk program. There was no most common recommendation for usage in the Enhanced Rollout phase.

Table 10: Overview of Most Commonly Recommended Phase for Data Usage



The following data source categories were considered in this survey:

- **Administrative:** Administrative data sources have to do with system privilege, account, asset, permission, and configuration data, which can give insight into abuses of insider access that may take place.
- **Communication:** Communication data sources involve insiders' communication with other individuals, printing/copying information, or other transfer of information between domains that may be unauthorized and/or part of insider compromise.
- **Network:** Network data sources involve the insider's use of computer system networks to access data, including data outside the organizational domain.
- **Personnel:** Personnel data sources include human resources records including background investigations, performance evaluations, and physical access.

- **Security:** Security data sources involve data related to system security or other organizational security issues such as conflict of interest or clearance investigation.
- **Violation Reporting:** Violation reporting data sources involve records associated with organizational violations or disciplinary actions, including anonymous reporting of such violations.

The majority of the data sources that were recommended for full rollout are those that would have a greater complexity of implementation than those identified for initial launch. The administrative data sources identified are those that are potentially more verbose in their output, or that might have a greater degree of latency. With the exception of the administrative data chosen for full rollout, the data sources identified are those that do not necessarily generate standardized logs or events for input to a tool; a greater degree of human interaction and manipulation is required to make the resulting data more suited to aggregation and correlation at scale. Taken together with behavioral science methods/tools being recommended for full rollout, it would seem that complexity of implementation is a deciding factor for respondent's recommendation to delay.

Subsequent sections describe these results in more detail and with greater nuance.

Administrative Data Sources

Table 11 shows that for administrative data sources, the majority response was chosen by over 50% of respondents, except in the case of “mobile device manager data”. “active directory data” at over 80% and “account creation data” at two-thirds of respondents were heavily favored for being implemented during initial launch. “mobile device manager data” had over 20% of respondents select enhanced capability. “asset management data” and “configuration change data” were about 7% for enhanced capability and the rest were all less than 5%.

Table 11: Recommended Deployment of Administrative Data Sources

When would you recommend the use of the following administrative data sources in the development of an insider risk program to support insider risk management?				
Administrative Data Source	Respondent Count	Initial Launch	Full Capability	Enhanced Capability
Account creation data	43	✓		
Active directory data	46	✓		
Asset management data	46	✓	*	
Authentication data	46	✓	*	
Configuration change data	44	*	✓	
Mobile Device Manager (MDM) data	46	*	✓	
Permission change monitor data	44	*	✓	

Legend

- ✓ Most common rating
- At least 50% respondents
- At least 75% respondents
- * At least one-third (33.3%) respondents

Looking at responses by experience level, there are a few notable differences:

- For “active directory data”, those with extensive experience more often selected full or enhanced capability. No-one at the lower experience levels chose enhanced capability for that option.
- For “asset management data”, the rates for selecting initial launch were consistent, but almost 20% of respondents at the knowledgeable experience level selected enhanced capability. No-one at the other experience levels selected the option.
- For “authentication data”, knowledgeable respondents were more often to select initial launch (about 70% of the time, versus about 50% for the other levels).

Communication Data Sources

For communication data sources, “data loss prevention data” and “email data” were heavily favored for initial launch as shown in Table 12, with over 80% and 90% respectively of respondents selecting that option. No respondents selected waiting until enhanced capability for either of these. Of all the data sources, only “telephone records / data” (about 15%) had more than 10% of respondents choose enhanced capability.

Looking at the answers by respondent experience level, a few observations stand out.

- For “help desk ticket system data”, those with extensive experience chose initial launch half as often as the other two experience levels. Though overall the preference was slightly in favor of full capability, initial launch was the slight favorite for knowledgeable and experienced respondents.
- For “printer / copier / scanner / fax data”, experienced respondents chose full capability more than twice as often as those at the knowledgeable or extensive experience levels and was the majority response for that group.
- For “telephone records / data”, there are interesting differences between each group. Knowledgeable respondents heavily favored full capability at over 70% of respondents.

Experienced respondents had a more even mix of responses, with 41%, 35%, and 24% for initial launch, full capability, and enhanced capability respectively. Respondents with extensive experience favored full capability, but not as heavily as knowledgeable respondents. The break down for this group was 54%, 31%, and 15% for full capability, initial launch, and enhanced capability respectively.

Table 12: Recommended Deployment of Communication Data Sources

When would you recommend the use of the following communication data sources in the development of an insider risk program to support insider risk management?				
Administrative Data Source	Respondent Count	Initial Launch	Full Capability	Enhanced Capability
Chat data	47	✓	*	
Data Loss Prevention (DLP) data	51	✓		
Email data	50	✓		
Help Desk Ticket System data	49	*	✓	
Printer / copier / scanner / fax data	49	✓		
Telephone records / data	48		✓	

Legend

- ✓ Most common rating
- At least 50% respondents
- At least 75% respondents
- * At least one-third (33.3%) respondents

Network Data Sources

Table 13 shows that for network data sources, only “network packet tags” and “wireless spectrum monitor data” had responses that favor waiting for full capability. For both of these, a fair number of respondents select enhanced capability: 20% and 26% respectively. No source had a majority response with at least 75% respondents. “Network monitoring data” had the highest rate for the majority answer at 71% for initial launch.

Looking at the data by experience level, two items are notable. First, for “DNS data”, though the overall response rate favors initial launch, respondents with extensive experience favored full capability. None of them chose enhanced capability as the response for this data source. Second, for “wireless spectrum monitor data”, respondents at the experienced level favored enhanced capability, choosing that response 40% of the time. Those knowledgeable and at the extensive experience levels chose enhanced capability only 18% of the time.

Table 13: Recommended Deployment of Network Data Sources

When would you recommend the use of the following network data sources in the development of an insider risk program to support insider risk management?				
Network Data Source	Respondent Count	Initial Launch	Full Capability	Enhanced Capability
DNS data	46	✓	*	
Firewall data	46	✓		
HTTP/SSL proxy data	49	✓		
Network monitoring data	48	✓		
Network packet tags	44	*	✓	
VPN data	47	✓		
Wireless spectrum monitor data	43		✓	

Legend
 ✓ Most common rating
 At least 50% respondents
 * At least one-third (33.3%) respondents

Personnel Records and Data Sources

For personnel records, Table 14 shows that two of the five items are favored for initial launch, with the other three for full capability. Four of the five items have at least 50% of respondents selecting the majority answer. Four of the five also have at least 10% of respondents selecting enhanced capability (“physical access records” are the exception).

Table 14: Recommended Deployment of Personnel Records and Data Sources

When would you recommend the use of the following personnel records and data sources in the development of an insider risk program to support insider risk management?				
Personnel Record or Data Source	Respondent Count	Initial Launch	Full Capability	Enhanced Capability
Background investigations	51	✓		
Corporate credit card records	49		✓	
Performance evaluations	49		✓	
Personnel records	49	*	✓	
Physical access records	50	✓	*	

Legend
 ✓ Most common rating
 At least 50% respondents
 * At least one-third (33.3%) respondents

Looking at the data by experience level, there are two things to note. First, for all question, respondents with extensive experience choose enhanced capability more often. This is especially notable for “background investigation” and “corporate credit card records” where 23% and 33% respectively of respondents with extensive experience select enhanced capability, which is about twice as often as the other levels. Second, for “personnel records”, respondents favor initial launch as the answer, while the others favor full capability.

Security Data Sources

Table 15 shows that of the ten security data sources, six were favored for initial response, three were favored for full capability, and one tied of initial launch and full capability. The majority response for all but “application data” and “conflict of interest reports” had at least 50% of the total responses. “Removal media manager data” had the highest consensus at 79% of respondents choosing initial launch.

Table 15: Recommended Deployment of Security Data Sources

When would you recommend the use of the following security data sources in the development of an insider risk program to support insider risk management?				
Security Data Source	Respondent Count	Initial Launch	Full Capability	Enhanced Capability
Antivirus data	46	✓	*	
Application data	45	✓		
File access data	48	✓	*	
Intrusion detection / prevention data	46	✓	*	
Removal media manager data	48	✓		
User Activity Monitoring (UAM) data	46	✓	*	
Security clearance records	42	✓	*	
Conflict of Interest (COI) reports	47	*	✓	
Foreign contacts reports	46	*	✓	
Travel reports	48	*	✓	

Legend

- ✓ Most common rating
- At least 50% respondents
- At least 75% respondents
- * At least one-third (33.3%) respondents

When looking at the data by experience level in Figure 20, three items are notable. For “antivirus data”, both knowledgeable respondents and those with extensive experience chose initial launch most often, but those with extensive experience less often. They chose enhanced capability most often at 17% of responses. Experienced respondents favored full capability with their responses, choosing that answer 56% of the time.

Looking at the tied item, “application data”, responses for knowledgeable and experienced respondents were very close, favoring full capability. However, those with extensive experience chose initial launch twice as often. The rates of choosing enhanced capability were similar for all three.

“User activity monitoring data” is interesting in that each progressive experience level chose initial launch more often than the previous. It went from 44% for knowledgeable respondents, 59% for experiences, and 77% for respondents with extensive experience.

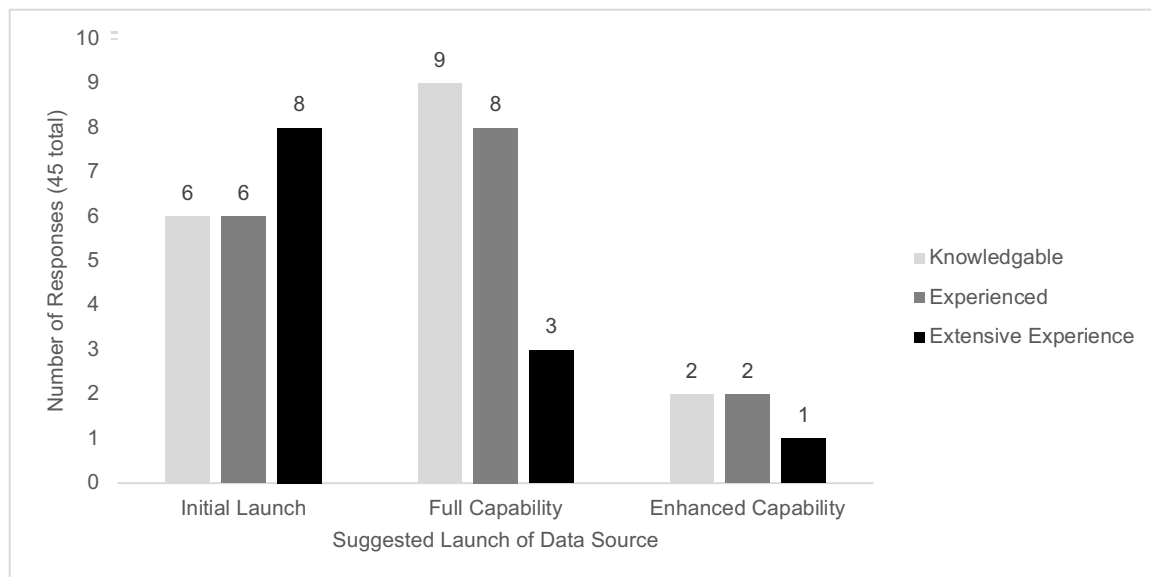


Figure 20: Suggested Launch of Application Data by Experience of Respondent

Violation Reporting

For all violation data reporting sources illustrated in Table 16, over 90% of respondents would implement either during initial launch or full capability. There was no notable sector differences, but there were for “disciplinary records” and “intellectual property policy violation records” by experience level. For both of those, respondents with extensive experience were most likely to select initial launch, which they did about twice as often as the other experience levels. Both experience levels chose initial launch only about a third of the time for “disciplinary records”. The split for “intellectual property policy violation records” was fairly close—about 52% versus 47% in favor of full capability.

Table 16: Recommended Deployment of Violation Reporting Data Sources

When would you recommend the use of the following violation reporting sources in the development of an insider risk program to support insider risk management?				
Violation Reporting Data Source	Respondent Count	Initial Launch	Full Capability	Enhanced Capability
Anonymous Reporting	50	✓		
Acceptable Use Policy Violation Records	50	✓	*	
Disciplinary Records	49	*	✓	
Intellectual Property Policy Violation Records	51	✓	*	
Physical Security Violation Reports	49	✓	*	

Legend

- ✓ Most common rating
- At least 50% respondents
- * At least one-third (33.3%) respondents

Conclusion

Public and private organizations building insider risk programs face a daunting array of people, organizational, and technological challenges that need to be met in order to position the organization to satisfy its mission sustainably, with acceptable risk. The results from the survey described in this report illustrates the broad range of realized insider threats that organizations face. Core challenges that an organization must overcome have primarily to do with institutionalization of the program – gaining executive support, sufficient funding, and collaboration across the organization for key insider threat detection and risk mitigation activities, especially cross-departmental data sharing. Management needs to find the right balance of holding people accountable for their actions while recognizing when the workplace context (including culture, policies, and practices) have the potential to exacerbate the threat. The survey results identified negative unintended consequences of high concern to program managers and ways of mitigating those consequences operationally.

The survey results should help organizations understand and overcome challenges associated with building insider risk programs in part through incremental rollout of the program. Survey respondents emphasized initial focus on 1) pre-employment screening to ensure congruence of individual and organizational expectations and values and 2) monitoring and analysis of select user activity. They recommended waiting until two to three years after launch to consider more advanced behavioral science and analytics, as well as process improvement activities overall. Recommendations on the inclusion of data sources in program rollout reflects this incremental approach leaving those data sources that have greater implementation complexity for after program launch. A gradual rollout of insider risk management policies, practices, and technologies helps to give time for the organization to gain the experience necessary to fine-tune its approach going forward. With a balance of positive and negative deterrence that is right for the organization, the insider risk program can become known as an advocate of employee well-being and a means for improving employee productivity, engagement, connection, and commitment for the benefit of both the employee and the organization overall.

Appendix Survey Questions

Question		Response Options
Q1	Have you ever been involved with creating an <u>insider risk program</u> for an organization that did not have one?	Yes/No
Q2	Do you currently hold or have you previously held a position within an organization's <u>insider risk program</u> ?	Yes, currently and previously; Yes, currently but not previously; Yes, previously; No
Q3	What current positions do you hold within your organization's risk management activity? Indicate the number of years in each current position you hold.	Designated senior official, Program manager, Senior risk analyst, Risk analyst, Behavioral scientist or psychologist, Human resources or behavioral specialist, System / software security subject matter expert, Data scientist / analyst, Incident investigator, Incident responder

Question	Response Options
Q4 What previous positions have you held within an organization's risk management activity? Indicate the number of years in each previous position you have held. .	Designated senior official, Program manager, Senior risk analyst, Risk analyst, Behavioral scientist or psychologist, Human resources or behavioral specialist, System / software security subject matter expert, Data scientist / analyst, Incident investigator, Incident responder
Q5 What level of knowledge and experience do you have in developing <u>insider risk programs</u> ?	Cursory knowledge and experience, at most; A fair amount of knowledge but not much experience; A fair amount of knowledge and experience; Extensive knowledge and experience
Q6 What sector or business classification is your organization most closely aligned with?	Natural resources and mining (agriculture, mining, quarrying, and gas extraction); Construction; Manufacturing (food, beverage, textiles, apparel, chemical / pharmaceutical, etc.); Wholesale trade; Retail trade; Transportation and warehousing (air, rail, truck, and couriers); Utilities; Information technology and telecommunications (data processing and hosting, publishing, broadcasting, etc.); Financial services (finance, insurance, funds, trusts, and real estate); Professional and business services
Q7 How many employees are currently in your organization?	Less than 100; 100 to 500; 501 to 1,000; 1,001 to 10,000; 10,001 to 100,000; More than 100,000
Q8 Does your organization have an <u>insider risk program</u> ?	Yes/No
Q9 How many years has your organization had <u>insider risk program</u> ?	0 to 2; 3 to 5; 6 to 10; 11 to 20; More than 20
Q10 What percentage of employees in your organization are covered by the insider monitoring practices associated with your organization's <u>insider risk program</u> ?	Less than 10%; 10% to 24%; 25% to 49%; 50% to 74%; 75% to 89%; 90% to 100%
Q11 How many staff <u>full time equivalents</u> (FTEs) are allocated to the <u>insider risk program</u> ?	0 to 2; 3 to 5, 6 to 10, 11 to 30, More than 30
Q12 Indicate the current priority level for each of the following insider threats to your organization.	5-point scale from High to Low rating: Irrational Individual, Thief, Disgruntled Insider, Activist, Terrorist, Organized Crime Member, Competitor, Nation-State
Q13 Indicate the current priority level for each of the following insider threats to your organization.	5-point scale from High to Low rating: Reckless Insider, Untrained / Distracted Insider, Sympathizer to External Influences
Q14 Indicate the current priority level for each of the following insider event types for your organization.	5-point scale from High to Low rating: Insider financial fraud, Insider sabotage of operational capability, Insider theft of information / data, Insider physical theft, Insider workplace violence, Insider misuse of organizational resources, Insider harassment in the workplace, Insiders tricked by outsiders, Other accidental leaks of information / data by an insider
Q15 a In the last year, roughly how many malicious insider events have happened at your organization? Indicate which insider events are included in your estimate first.	Insider financial fraud, Insider sabotage of operational capability, insider theft of information / data, Insider physical theft, Insider workplace violence
Q15 b Estimate of the total number of the above insider events combined in the last year.	Open-ended
Q16 a In the last year, roughly how many other harmful insider events have happened at your organization? Indicate which insider events are included in your estimate first.	Insider misuse of organizational resources, Harassment in the workplace by insiders, Insiders tricked by outsiders in compromise, Other accidental leaks of information / data by insider

Question	Response Options
Q16 Estimate of the total number of the above insider events combined in the last year.	Open-ended
Q17 To what extent are you concerned about each of the following potential negative unintended consequences for <u>insider risk programs</u> ?	5-point scale from High to Low rating: Insider risk controls inhibiting productivity, Undermining trust between management and other employees, Undermining trust among all employees, Reducing retention of good employees, Undermining goodwill of good employees, Investigations unfairly affecting employee careers, Workplace becoming more confrontational, Infringing on employee privacy rights and civil liberties
Q18 What policies, practices, or mitigations would you recommend to ensure that <u>insider risk program</u> activities are not significantly affected by the above negative consequences, e.g., do not conflict with employees' expectations of privacy?	Open-ended
Q19 How extensive is the challenge of achieving each of the following for <u>insider risk programs</u> ?	5-point scale from High to Low rating: Coordinating and communicating across business / operational units, Establishing the insider risk program scope and organizational structure, Ensuring compliance with all applicable legal requirements, Developing policy and formalizing the program, Incorporating insider risk controls for trusted business partners, Obtaining adequate funding for program operation, Developing and administering insider threat awareness training, Hiring and retaining qualified insider risk program personnel, Sharing information across the organization's departments / units, including Human Resources (HR)
Q20 How important are of each of the following operational measures in insider risk decision making for senior leadership?	5-point scale from High to Low rating): Number of cases, Number of monitored employees, Number of cases escalated for review, Number of findings per year, Number of incidents avoided due to technical controls)
Q21 When would you recommend the deployment of the following tools in the development of an <u>insider risk program</u> ?	3-point scale from Initial launch (first year), Full Rollout (2 to 3 years after launch), Enhanced Rollout (5 to 10 years after launch) rating: User Activity Monitoring (UAM) tool, User and Entity Behavioral Analysis (UBA/UEBA) tool, Data Loss Prevention (DLP) tool, Security and Information Event Management (SIEM) management tool, Incident case management (IM) tool
Q22 When would you recommend the implementation of the following processes and capabilities in the development of an <u>insider risk program</u> ?	3-point scale from Initial launch (first year), Full Rollout (2 to 3 years after launch), Enhanced Rollout (5 to 10 years after launch) rating: Monitoring and analysis of select user activity, Applying behavioral science methods to identify indicators, Applying multi-source data integration methods and advanced analytics, Analysis of employee complaints / grievances, Analysis of threat intelligence from external sources, Pre-employment screening (e.g., background checks, credit checks, or interviews), Periodic re-investigation to assess risk over time, Continuous employee evaluation to assess ongoing threat, Regular evaluation of employee perception of working conditions
Q23 When would you recommend the implementation of the following improvement processes in the development of an <u>insider risk program</u> ?	3-point scale from Initial launch (first year), Full Rollout (2 to 3 years after launch), Enhanced Rollout (5 to 10 years after launch) rating): Conduct audits of the insider risk program, Conduct operational exercises to evaluate defenses, Test the workforce's vulnerability to unintentional insider risk (e.g., social engineering), Periodically analyze privacy and regulatory requirements to ensure organizational compliance, Analyze performance metrics over time
Q24 When would you recommend the use of the following violation reporting	3-point scale from Initial launch (first year), Full Rollout (2 to 3 years after launch), Enhanced Rollout (5 to 10 years after launch) rating:

Question	Response Options
sources in the development of an insider risk program to support insider risk management?	Anonymous Reporting, Acceptable Use Policy Violation Records, Disciplinary Records, Intellectual Property Policy Violation Records, Physical Security Violation Reports
Q25 When would you recommend the use of the following administrative data sources in the development of an insider risk program to support insider risk management?	3-point scale from Initial launch (first year), Full Rollout (2 to 3 years after launch), Enhanced Rollout (5 to 10 years after launch) rating: Account creation data, Active directory data, Asset management data, Authentication data, Configuration change data, Mobile Device Manager (MDM) data, Permission change monitor data
Q26 When would you recommend the use of the following communication data sources in the development of an insider risk program to support insider risk management?	3-point scale from Initial launch (first year), Full Rollout (2 to 3 years after launch), Enhanced Rollout (5 to 10 years after launch) rating: Chat data, Data Loss Prevention (DLP) data, Email data, Help Desk Ticket System data, Printer / copier / scanner / fax data, Telephone records / data
Q27 When would you recommend the use of the following security data sources in the development of an insider risk program to support insider risk management?	3-point scale from Initial launch (first year), Full Rollout (2 to 3 years after launch), Enhanced Rollout (5 to 10 years after launch) rating: Antivirus data, Application data, File access data, Intrusion detection / prevention data, Removal media manager data, User Activity Monitoring (UAM) data, Security clearance records, Conflict of Interest (COI) reports, Foreign contacts reports, Travel reports
Q28 When would you recommend the use of the following network data sources in the development of an insider risk program to support insider risk management?	3-point scale from Initial launch (first year), Full Rollout (2 to 3 years after launch), Enhanced Rollout (5 to 10 years after launch) rating: DNS data, Firewall data, HTTP/SSL proxy data, Network monitoring data, Network packet tags, VPN data, Wireless spectrum monitor data
Q29 When would you recommend the use of the following personnel records and data sources in the development of an insider risk program to support insider risk management?	3-point scale from Initial launch (first year), Full Rollout (2 to 3 years after launch), Enhanced Rollout (5 to 10 years after launch) rating: Background investigations, Corporate credit card records, Performance evaluations, Personnel records, Physical access records
Q30 When would you recommend the inclusion of the following stakeholders into insider risk decision making activities in the development of an insider risk program ?	3-point scale from Initial launch (first year), Full Rollout (2 to 3 years after launch), Enhanced Rollout (5 to 10 years after launch) rating: Human Resources, Information Technology, Physical Security, Executive Leadership, Enterprise Risk, Legal, Privacy
Q31 What advice would you give to an organization that is establishing an insider risk program for the first time?	Open ended
Q32 What one factor or practice is the most important for an organization to get right to mature its insider risk program ?	Open ended
Q33 What is the biggest barrier to effective insider risk mitigation today?	Open ended