Direct from an ASIS INTERNATIONAL COUNCIL

White Paper
ASIS Women In Security
Publications Committee

KEY CONSIDERATIONS WHEN BUILDING OUT YOUR INSIDER RISK PROGRAM

By: Suzanna Alsayed-Hills, MDEM, Silvia Fraser, CPP, Antoinette King, PSP, Sherri Ireland, CISSP, Lina Tsakiris, CPP

Introduction

Is Insider Risk something new, or something we need to look at in a new way? Traditionally we have put in place measures to protect the perimeter, to control access into our buildings or our systems. Why did we do this? We saw the biggest risks and threats coming from external sources. In a "less connected" world this made perfect sense. We housed our assets and managed accordingly. However, the world has changed. We are more inter-connected than ever, and in many ways, we've optimized against the external threats. We have become experts in "perimeter" protection. We cannot rest and let down on the perimeter, however, the perimeter being the primary focus has left us vulnerable in many ways. This paper discusses how we design our internal controls, both in physical and system realms, as we evolve our understanding on where risks really exist, and how we believe people might behave. Employees stealing physical or confidential information from their company and/or place of work is not new, however, the complexity of the environment that we protect is no longer simple, and the stakes are high. Our reputation, our credibility, and in some cases the financial viability of these organizations are at stake.

Does your organization understand how to measure insider risk; know where to start? The good news is that much of the existing security controls infrastructure and practices still apply. Insider risk can be integrated into current policies and practices. Creating an insider risk program will require organizations to examine the known risks in a new context of how they manage trust, control access, understand and evolve corporate culture, and ultimately prepare to manage and contain incidents when they happen. This paper will introduce the concept of Insider Risk across common domains of understanding "assets", the so-called Crown Jewels; discuss measures to supplement policy and programs for prevention, deterrence, detection mitigation and response. It will provide a framework for how to govern presently and for the future, with a business lens as the primary driver, and a starting point. Awareness and preparedness are the best defense against insider risk.

Essential One: Program Governance and Operations

At the base of an Insider Risk Program lies the internal risk coming from an employee, a contractor, a sub-contractor or a trusted third-party supplier and;

1. What they know: information, company trade secrets, processes;
2. What they have: access to information or physical assets; and
3. What they do: the very actions they take in the process of executing their functions.

Hence, the insider threat involves, by definition, all levels of the organization and a range of departments including Human Resources, Information Technology, Security, Records Management, Legal, Compliance, Strategy, Risk Management, Procurement, Communications, Finance and other relevant stakeholders.

The success of implementing an Insider Risk Program is dependent upon the collaboration between key stakeholders and their work in managing the insider risk from a variety of perspectives. Collaboration needs to be

created, nurtured, and fostered within the organizational culture. This can be done with an established governance model, specific to the Insider Risk Program.

Creating and Implementing a Governance Model for the Insider Risk Program

When developing an Insider Risk Program, organizations should start with a clearly defined governance model through which stakeholders collaborate to identify critical assets, risk indicators, relevant data sources, compliance requirements, cultural concerns, security and privacy implications. Consider these factors:

1. **Commitment / Why**: This is the very key of establishing a program. Commitment must be made at the highest levels within the organization and it needs to include adequate and robust resources.
2. **Accountabilities / Who:** Establish decision making roles & responsibilities.
3. **Stakeholder Participation & Support / How:** The success of an insider risk program depends on the support and participation of its stakeholders.

As an Insider Risk Program is realized through culture change, emphasis must be placed on the following factors:

Stakeholder Relationships: Stakeholders need to develop constructive working relationships to manage risk from within. These relationships need to be fostered and managed appropriately through transparency and building trust. This can be achieved through communication, storytelling and team building initiatives. Using approaches to understand common and unique risk postures and collective opportunities across stakeholders will assist.

Organization-wide, clearly defined and easy-to-follow policies and practices: There needs to be a reasonable balance between protection and access. We could look to manage risk by restricting access completely as a means of protection, however doing business would be challenged. Consider the following as a starting point: password policy, account policy, and information management and data policies and processes. Research shows that 95% of successful breaches result from simple opportunities. Lack of policies or poor policies and processes increase vulnerability. By implementing measures such as a strong password policy, effective account management policies and measures to control and manage access to data, many insider threats can be mitigated. Comprehensive policies regarding physical traffic flow within facilities, locations of data storage, and maintaining effective technology infrastructure (hardware, software, server, cloud, network, mobile and computer) asset and operational management practices including cyber-security best practices will create an additional layer of protection against insider threats.

Communication protocols: Clear communication protocols should be established if an employee recognizes unusual or unexpected activity that could trigger an elevated risk situation. It is imperative that an organization ensures that everyone has a clear understanding of who is responsible for receiving and taking action on reported issues, and what steps will be taken in order to address the various degrees of threats. As a best practice consider outlining different threat levels and how to properly escalate issues. These steps should be contained within a communication protocol for the Insider Risk Program; they should be precise and easy to follow. Additionally, as part of an awareness program, training on how to report an incident should be regularly provided through engagement across all levels within the organization with encouragement to ensure risks are reported. Consideration must also be given on how to report incidents anonymously.

Comprehensive training and awareness programs: A comprehensive security awareness program for all employees and trusted third-

party suppliers is important, however, continuous education and training are the lifeblood of the program, each of which will encourage and create a culture of security. All departments should have an 'education track' that is tailored to their role within the business, particularly addressing the unique challenges of that unit, and the general security concerns of the organization.

Essential Two: Protecting the Crown Jewels

An organization must protect their "Crown Jewels", their people, information, technology and facilities. As it concerns information the goal is CIA; Confidentiality (access to information on a need to know basis), Integrity (information has not been altered either maliciously or unintentionally) and Availability (data or resources are available when needed).
Insider threats take many forms, they can be an organization's employees, former employees, trusted third-party suppliers, contractors or subcontractors. They can be a malicious insider, someone with malicious intent, or an unintentional insider, someone, whom through their action or inaction, causes a threat to an organization's Crown Jewels.

Good hiring practices and screening of third-parties are essential; conduct reference checks, ask the question, "if given the opportunity would you hire them (or work with them) again?" Be diligent with criminal background checks of new employees. Have third-party contractors agree to annual criminal background checks of their own employees and have them supply results for employees working within your organization. Depending on the "crown jewels" this may necessitate a further step, including credit checks and even obtaining government clearances. Annual criminal background checks are a best practice.

Essential Three: Identifying Insiders, Prevention and Detection

Unintentional insider (someone through action or inaction causes a threat):
An insider can cause a threat to an organization in many ways. A senior executive posting on Facebook that they are on a business trip or vacation can make the organization vulnerable to a Social Engineering attack. Sometimes it's as simple as the improper disposal of files or records, a lost or stolen device such as a laptop, smart phone or USB. Company information downloaded onto personal devices, leaves the information more susceptible to unintentional disclosure.

Prevention Item #1. Provide security and cyber-awareness training for employees. Make them aware of social engineering techniques and encourage them to report anything that seems unusual to their manager or IT department.

Prevention Item #2. Consider best practice Cyber-Security practices such as those in the NIST Cyber-Security Framework that can be used to assess and improve capabilities to identify, protect, detect, respond and recover for cyber requirements. Simple measures such as limiting access to the USB ports on the company network can help prevents users from maliciously or unintentionally introducing viruses or malware to the network and potential data loss or breach for example. At a minimum, enforce encryption of USB devices.

Detection Item #1. Ensure IT infrastructure has current anti-virus and intrusion detection.

Detection Item #2. Ensure IT teams have management software in place to manage employee devices such as smartphones. This software enables good security practices, enforcing the use of passwords, use of strong passwords, automatically

locking the device if it is inactive, disabling and wiping the device remotely if it lost.

Detection Item #3. Actively monitor social media for mentions of your organization.

Employee has resigned:
Statistics show that within 30 days of giving their resignation, employees steal intellectual property or conduct some sort of IT sabotage or espionage.

An ex-employee may intentionally misuse credentials that were not removed from an access control system to gain unauthorized access to a facility. This is an example of an indirect intentional insider threat. [1]

Prevention Item #1. Communication is key, between HR, IT, Security and Managers. The team needs to communicate resignations. Especially if the employee has significant privileges (C-level executive, IT administrator privileges).

Prevention Item #2. Implement and audit the concept of least privilege. Access to physical spaces and to information should be setup on a need to know basis. Auditing is required, as over time, people gain extra privileges for specific assignments or assignments change and those permissions are seldom retracted once the assignment has concluded. Similarly, a person who has been demoted or reassigned without an update to IT or the security department, to change their access privileges, leaves an organization vulnerable.

Detection Item #1. IT infrastructure needs to monitor activity to identify anomalies – especially for employees that have resigned. Alerts should flag logging in after-hours, transferring large files, emailing large files, using a third-party file service such as Dropbox. These alerts need to be investigated in a timely fashion.

Trusted Employee:
Employee fraud typically occurs by employees with at least 5 years tenure. Their role would have access to customer or employee information and data and over time the employee has learned the security measures protecting this data. This type of fraud usually takes place over many years and is done during business hours. An example is the true story of 15-year employee in a cash counting position, who when randomly searched, was discovered with a $20.00 bill in their waistband. Was it $20.00 one time, or was it $20.00 every day for 15 years? Was it more than $20.00 each day over 15 years? Often the trusted employee is working in collusion with an outsider and their access privileges have accumulated over time.

Similarly, a current employee may improperly dispose of files or documents containing sensitive information whereby exposing the organization to unauthorized access to company data / assets. In this case, this is a direct unintentional insider threat (Behr, 2017)[2].

Prevention Item #1: Rotating roles promotes redundancy in an organization, improves employee morale by providing new challenges and learning and helps to deter employee fraud.

Prevention Item #2: Separation of duties is an internal business control that helps to prevent fraud and identify errors. This concept should be applied to all areas of the business that involve “crown jewels”. Separation of duties is separating the function of a role that typically could be completed by one person and assigning it to a second individual. This is understandably, more difficult to do in a small business. Businesses often have separation of duties in place when it comes to the financial aspect of the business, requiring two people to authorize cheques over a certain amount. Separating the person that

[1] https://insights.sei.cmu.edu/sei_blog/2014/09/designing-insider-threat-programs.html

[2] https://www.csoonline.com/article/2123120/separation-of-duties-and-it-security.html

receives the cheques from the one making deposits, and no one individual authorized to issue credits, they always need a second signature. This same methodology should be applied to organizational data. Look to segregate compliance from operations with controls and policies to apply.

Ask the following questions: Is there any one person within this organization who can alter or destroy data without being detected? Is there any individual that can steal or download sensitive information? Lastly, does any individual have ownership over the design, implementation and reporting of the effectiveness of the controls? The answer to all these questions should be "no." [3]

Prevention Item #3: If an employee is on short-term or long-term leave, ensure their access privileges are suspended.

Essential Four: Response

While we discussed detection and prevention tactics, a critical aspect of any program is response. With multiple stakeholders and a variety of policies in place, incident response for an insider risk is paramount. From how does an organization respond to the incident, to the communication and actions taken, all are vital to the success of the program.

Here are a few key aspects of the Response an organization must follow. Consistent to Emergency Management and Business Continuity best practices, insider risk is no different. You need to have a documented Incident Response Plan that is standardized, repeatable and consistent. It can be incorporated into your organization's general incident response plans or it can be a stand-alone document.

The plan needs to be authorized and supported by the senior leadership team and will outline plans for deterrence, training, detection, reporting, escalation, remediating and documenting an insider threat.

Responses will be different. The response to an unintentional insider may simply require notification and re-training of the individual. The response to a malicious insider could include escalation to law enforcement depending on the nature of the risk.

After every incident a review needs to be conducted. What worked well? What can be improved? Document lessons learned and ensure that the plan is updated accordingly.

Conduct an annual tabletop exercise, this will ensure that all stakeholders are aware of their responsibilities with respect to the insider risk plan.

Essential Five: The first 60 Days

It is crucial to understand that simply creating a thorough Insider Risk Program does not ensure its immediate success. [4]

Standing up a program within a short time frame can appear to be a daunting task, however, consider starting small and building from any related existing programs such as your Workplace Violence and or Cyber Security programs. Key considerations should be given to:

1. Determine what you have in place today and identify the greatest gaps.
2. Create an implementation roadmap to remediate the identified gaps.
3. Focus on building around your critical insider threats types (for your business). For example, if you are a high-tech business, you may want to start with IP Theft, IT Sabotage and Espionage.
4. Assemble a planning and implementation team to design your

[3] https://www.csoonline.com/article/2123120/separation-of-duties-and-it-security.html
https://www.computerworld.com/article/2532680/the-key-to-data-security--separation-of-duties.html

[4] http://www.sei.cmu.edu

framework and workflows. Improving existing procedures and workflows can provide quick wins.

5. Create a Concept of Operations and test it by creating a few use cases that are reflective of the threat types you have identified.

Overall, it is more essential to have a meaningful start and incremental build out of your program that can provide sustained value add, than trying to incorporate all program aspects from the onset. This will increase the likelihood of gaining top tier management support which may lead to additional funding, program growth and optimization opportunities.

Conclusion

All organizations need to have an Insider Risk Program. Promote awareness of the program to employees and managers and monitor for compliance. Ensuring open communications between management, security, HR and the IT teams serves to mitigate exposure to an insider risk. Ultimately, the process of building and Insider Risk Program is ongoing. Once a baseline has been established, periodic examination of policies and procedures ensures that the program will remain effective in the current environment, especially when threat landscapes are constantly changing. The final step in creating a successful Insider Risk Program is ensuring that there is a scheduled audit of the program that includes penetration testing and employee surveys to measure how the program is working.

Developing an Insider Risk program is an essential part of an organization's overall security ecosystem. Without it, an organization becomes more vulnerable to physical and/or cyber-security threats and attacks. In the early stages of creating a program, it is important to gain the endorsement of senior leadership and consider the organization's culture. Training and awareness will ensure that a well-designed program is executed and effective.

When an Insider Risk Program is created properly and collaboratively, it can easily be adapted to an organization's changing culture and security requirements.