Building A Holistic and Risk Based Insider Threat Program

An Approach to Preventing, Detecting and Responding to Insider Threats

Michael G Gelles, Psy.D.
Deloitte Consulting LLP
October 2014
Insider Threat: A Baseline understanding

**Insider Threat Defined**: A person who has the potential to harm an organization for which they have inside knowledge or access.

Further….

- **Insider threat** exists within every organization where employees and contractors comprise the core of an organization’s operational plan and are key drivers of its mission execution.
- As a result (threat) of some perceived injustice, retaliation, sense of entitlement, or unwitting need for attention and/or validation, the employee or contractor takes action as part of a contrived solution that results in negative consequences. i.e., damage to information, brand, reputation, material, safety and security.
- **Insider actions** can be the result of malevolent intent, complacency or ignorance.
- **Perfect Storm** includes access, crisis and disposition.

**Underlying Themes – Context – What’s different? – New trends – Different consequences**
## Insider Threat Drivers

There are distinct and preventable drivers of insider threats which are influenced by an organization’s established policies, procedures, and values.

<table>
<thead>
<tr>
<th>Malice</th>
<th>Complacency</th>
<th>Ignorance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>An act that is malicious and intentional in nature to cause damage</strong></td>
<td><strong>Lax approach to policies, procedures, and potential security risks</strong></td>
<td><strong>Lack of awareness of policies and procedures creates security risk</strong></td>
</tr>
<tr>
<td>▪ Current or former employees that are triggered by a specific work-related or non-work-related incident such as a poor performance review and large amounts of debt</td>
<td>▪ Over time employees may become more lax about security policies</td>
<td>▪ Employee ignorance is a challenge to organizations attempting to manage and maintain a secure organization</td>
</tr>
<tr>
<td>▪ Insiders typically develop a plan in advance of the act that someone within the organization may detect</td>
<td>▪ Violators often assume that their specific behavior does not have a noticeable impact or that no one is monitoring their behavior</td>
<td>▪ Lack of understanding of security protocols, and the potential impact if not followed, further exacerbates the impact of unknowing exposure of critical information</td>
</tr>
<tr>
<td>▪ Examples: Information and asset exploitation such as espionage, fraud, corruption, and IT system exploitation</td>
<td>▪ Examples: Removal of proprietary or classified information or material from secure areas; forwarding information to home email addresses to work on a task after hours; inappropriately placing information in an open and unsecure area</td>
<td>▪ Examples: Disclosure or dissemination of information determined to be proprietary or classified to persons without clearance or purpose to have the information; irresponsible handling of classified or proprietary information; irresponsible use of information systems</td>
</tr>
</tbody>
</table>

Instances of ignorance and complacency are prime for exploitation by employees with harmful intent.
An Increased Potential For Insider Threat

### Characteristics of the new workforce demographic
- As the Boomer generation retires, 75 million Generation Y will replace them, inevitably changing the workplace to reflect their ideas and values.
- The new generation is defined by the Internet and electronic social networks and public forums such as Facebook and Twitter.
- To share information and be comfortable with ever-advancing technology in part defines their identity.
- Generation Y are “tech-savvy,” expect access to information and want it with speed and accuracy.
- The new candidate is oriented towards a culture where information is readily available and accessible, and shared across a larger community.
- Not satisfied with the “passive” attributes of information sharing, waiting for a data owner to grant access and then make it available.

### Characteristics of the new workplace
- The average supervisor will have five to seven years of experience as a result of the shifting demographic.
- The new candidate is oriented towards a culture where information is readily available and accessible, and shared across a larger community.
- Proactively obtain information based on their emergent knowledge and solution requirements.
- Workplaces are expanding social network tools such as gov loop and internal Facebook models.
- Social networking broadens exposure and vulnerability to being identified, assessed etc.

---

Potential new type of risk in a secure work environment based on copycat malicious acts (i.e., Snowden is admired by some and celebrated as a patriot), the need for rapid fire communication, constant connectivity and a natural propensity to share information.
A Layered Approach to Mitigating Risk

- **Mitigation Approach**:
  - **Training By Role**: Develop curriculums based on role within the organization and include targeted behavior and observation skills, and provide training to enhance employee vigilance and reporting of suspicious behavior.

- **Mitigation Approach**:
  - **Employee Lifecycle**: Beginning with the hiring process through termination, monitor and respond to suspicious or disruptive behavior.

- **Mitigation Approach**:
  - **Layered Security**: Use available internal and external data or potential risk indicators to better understand and more accurately analyze events involving insider risk.

- **Mitigation Approach**:
  - **Access Controls**: Analyze and document access controls and analyze how systems are accessed and segmented.
  - **Policies and Procedures**: Review the organization’s hiring, recruitment, resignation, transfer, and retirement processes for vulnerabilities.

**Increasing Complexity and Difficulty to Detect**

- **Ignorance**
- **Complacency**
- **Malice**

Note that mitigation approaches are additive and form a layered approach to reducing the risk.
1. Define Your Insider Threats – Don’t be surprised if your organization hasn’t defined what an insider threat is. The reality is few organizations have a specific internal working definition as security and IT budgets have historically prioritized external threats.

2. Define Your Risk Appetite? – Define the critical assets (e.g., facilities, source code, IP and R&D, customer information) that must be protected and the organization’s tolerance for loss or damage in those areas.

3. Optimize A Broad Set Of Stakeholders – The program should have one owner but a broad set of invested stakeholders. Establish a cross-disciplinary insider threat working group that can serve as change agents and ensure the proper level of buy-in across departments and stakeholder (e.g., legal, physical security, policy, IT security, human resources, ethics, etc.).

4. Don’t Forget the Fundamentals – The insider threat challenge is not a purely technical one, but rather a people-centric problem that requires a holistic and people-centric solution. Organizations should avoid the common pitfall of focusing on a technical solution as the silver bullet.

5. Trust But Verify – Establish routine and random auditing of privileged functions, which is commonly used to identify insider threats across a broad spectrum of threats in a variety of industries.
6. **Look For Precursors** – Case studies have shown that insider threats are seldom impulsive acts. Rather, insiders move on a continuum of the idea of committing an insider act to the actual act itself (e.g., Fraud, Espionage, Workplace Violence, IT sabotage, and IP&RD theft.

7. **Connect The Dots** – By correlating precursors or potential risk indicators captured in virtual and non-virtual arenas, your organization will gain insights into micro and macro trends regarding the high risk behaviors exhibited across the organization.

8. **Stay A Step Ahead** – Insiders’ methods, tactics and attempts to cover their tracks will constantly evolve, which means that the insider threat program and the precursors that it analyzes should continuously evolve as well.

9. **Set Behavioral Expectations** – Define the behavioral expectations of your workforce through clear and consistently enforced policies (e.g., social media, removable media, reporting incidents, BYOD, etc.) that define acceptable behavior and communicate consequences for violating policies.

10. **One Size Does Not Fit All** – Customize training based on the physical and network access levels, privilege rights and job responsibilities.)
What good looks like…Insider Threat – Program Structure

The insider threat program structure includes the routine engagement of stakeholders that sit on an insider threat working group, foundational building blocks that are likely in place within the organization and the use of an advanced analytics solution.

**Insider Threat Program Components**

- Pre-employment Investigations & Procedures
- Security Education and Awareness
- Personnel Management
- Security Capabilities
- Termination Procedures
- Physical Security Access
- IT Security Access and Technical Controls
- Off-The-Network Indicators (Complaints, Investigations, Foreign Travel, etc.)
- Virtual Indicators

**Insider Threat Program Stakeholders**

- Multidisciplinary groups will coordinate and provide input and meet on a reoccurring basis

**Program Foundation**

- Security policies, procedures and technology provide the foundation for mitigating insider threat
- Vetting, managing, and releasing personnel properly and safeguarding data and information in systems

**Access and Technical Controls**

- Serve as barriers to entry for personnel and require continued re-evaluation of necessary access
- In the event of an incident, resilience (e.g., system and data back-up and recovery procedures) is critical

**Individual Monitoring**

- Aggregating data from disparate but related data sources provides improved insight into the risk profiles of individual employees
- Types of data collected will include PII and must be safeguarded to the fullest extent; access to this security information will be limited

**Data Analysis & Reporting**

- Data from disparate sources is combined to identify individual employees at-risk
- Advanced analytics tool provides automated analysis and reporting based on a risk algorithm that aligns with the organization’s risk tolerance

**Employee Risk Continuum**

- Based on factors such as virtual and off-the-network actions coupled with contextual descriptors risk mitigation efforts will focus on individuals perceived to be at an elevated risk

**Active Monitoring**

- Creates proactive awareness and potential for cross-disciplinary coordination, intervention, and resolution.