Overview of Insider Threat Best Practices Guide

- The Core components of an insider threat mitigation program mirror those denoted in the NIST Cybersecurity framework: Identify, Protect, Detect, Respond and Recover
  - The components leverage a risk based approach to threat assessment and resource allocation
  - The Framework’s flexibility allows firms to scale their implementation based on business model and available resources

- Unlike a typical cybersecurity program, each component of an insider threat mitigation program has a distinctly human element
  - Best practices encourage leveraging
    - Technical tools, such as network monitoring software
    - Knowledge of human behaviors that foreshadow attacker’s intent
    - Counterintelligence skills to detect and investigate suspicious insider behaviors
  - Investigative challenges are inherent to the human element of insider threats

- Legal Risks
  - Although privacy and employment laws in the United States are generally permissible of employers’ efforts to protect their assets, electronic communication privacy laws and background check restrictions at the state and federal level impose some procedural hurdles
  - Laws abroad – particularly in the European Union – are more restrictive and in some cases may prohibit employers from taking certain insider threat precautions.

- Firms should use Best Practices and the structure of the Cybersecurity Framework as a starting point – local counsel should be consulted throughout the development and implementation of an insider threat mitigation program.
Financial Institutions have long been especially lucrative targets for insider attacks, but, with computerization of firm systems and assets, attacks can now be launched on a larger scale than ever before.

| What is an Insider Threat? | • Insider threats involve authorized individuals who misuse their access to systems, networks or information in a manner that negatively impact the confidentiality, integrity, or accessibility of legitimate business processes  
| | • Frequently, insider threats involve the intentional theft, loss, alteration or destruction of an organization’s data, resources or intellectual property. |
| Who are Insiders and What are Their Motives? | • In the financial services space, insider security incidents emanate from all types of roles and responsibilities with enhanced capabilities when combined with external actors such as organized crime, former employees, competitors and acquaintances.  
| | • The majority of insider events are financially motivated, but other motives may be drivers as well. Another specific concern is the increasing rate of business related espionage, especially where employees take data to competing organizations |
| Insider Threat Mitigation Program | • Cybersecurity defenses alone cannot adequately protect against insider threats. Rather, successful programs take an “interdisciplinary” approach involving a combination of technology, legal, policy, physical security, awareness and training, and counterintelligence resources.  
| | • An insider threat mitigation team is essential to coordinate firm wide prevention efforts and alert relevant personnel to suspected or detected threats.  
| | • The insider threat mitigation team can be a part of the HR or IT organization within a firm and should be responsible for conducting insider threat investigations and routine monitoring  
| | • Senior representatives from other functions (e.g., legal) can serve as members of an insider threat “working group” that would be consulted when developing new insider threat policies or responding to detected threat risks  
| | • The NIST Cybersecurity Framework’s “core” components – Identify, Protect, Detect, Respond, Recover – can be used as a useful framework to implement an insider threat mitigation program |
| Risk Management | • A successful insider threat program is embedded within and based on a sound risk management program to help inform where resources, effort and focus should be spent. |
Risk Management – The Foundation of an Effective Program

RISK MODEL

1. Critical assets (information, systems, programs, people, equipment or facilities) for which there is no known vulnerability and no known threat exposure.

2. Vulnerabilities in systems, programs, people, equipment or facilities that are not associated with critical assets and for which there is no known threat exposure.

3. Threat environment for which there is no known threat to critical assets or access to vulnerabilities (or vulnerability information).

4. Critical assets for which there are known vulnerabilities, but no known threat exposure.

5. Critical assets for which there are known vulnerabilities and threat exposure.

6. Threat has acquired specific knowledge and/or capability to exploit a vulnerability although not a critical asset vulnerability.

7. Critical asset for which there are no known vulnerabilities, but there is exposure to a specific threat.

Figure 1 – Department of Defense Risk Model.
## Overview of Core Components: Adopting the NIST Framework to Insider Threat Mitigation Best Practices

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Identify</td>
<td><strong>Asset Management</strong>: Ensure that the data, personnel, devices, systems and facilities at risk are identified and prioritized. <strong>Governance</strong>: Structure an insider threat team and develop policies and procedures for monitoring and management. <strong>Risk Assessment</strong>: Understand the risk that insiders pose to organizational operations and a firm’s assets. <strong>Risk Management Strategy</strong>: Establish policies and procedures to identify the kinds of behaviours that indicate malicious insider activity.</td>
</tr>
<tr>
<td>2. Protect</td>
<td><strong>Access Control</strong>: Implement appropriate technical and administrative safeguards to ensure access is limited to authorized users with a business need. <strong>Awareness &amp; Training</strong>: Implement programs to alert personnel to insider threat risks, consequences and behaviours. <strong>Information Protection Processes</strong>: Maintain policies, processes and procedures to protect systems and assets. <strong>Protective Technology</strong>: Use technical security solutions to safeguard data and systems that could potentially be exploited.</td>
</tr>
<tr>
<td>3. Detect</td>
<td><strong>Anomalies &amp; Events</strong>: Implement network and application monitoring tools, allocating the most resources to systems identified as &quot;critical&quot; in the risk assessment. <strong>Security Continuous Monitoring</strong>: Designate appropriate personnel for insider threat mitigation team and implement continuous intelligence monitoring. <strong>Detection Processes</strong>: Implement means for reporting and discovering suspicious insider behaviour.</td>
</tr>
<tr>
<td>4. Respond</td>
<td><strong>Communications</strong>: Establish, memorialize and standardize the investigation and response procedures to include interaction with law enforcement. <strong>Analysis</strong>: Classify incidents to determine appropriate investigative procedures and escalation. <strong>Mitigation</strong>: Prevent expansion of event by addressing its cause.</td>
</tr>
<tr>
<td>5. Recover</td>
<td><strong>Recovery Planning</strong>: Execute processes and procedures to control the scope of the incident and restore affected data. <strong>Improvements</strong>: Evaluate incident and incorporate lessons into future activities and processes. <strong>Communications</strong>: Communicate with internal and external parties to ensure coordinated response to incident.</td>
</tr>
</tbody>
</table>
Network Monitoring

- Utilize network monitoring software
- Establish a network activity baseline to determine suspicious activity
- Monitor the network for security violations: (e.g., failed log-in attempts, downloading large amounts of data, altering coding on sensitive files) and investigate suspicious activity

Insider Threat Mitigation Policy

- Monitor for personnel issues: (disputes with co-workers or superiors, threats, chronic absenteeism).
- Implement reporting mechanisms for employees and supervisors to report suspicious activity

Training and Prioritization

- Train all personnel how to identify indicators of insider threat risks, include new hires and refresher
- Stress the importance of reporting suspicious behavior, policy violations, personnel conflicts or any other signal for insider risk.
- Provide confidential/anonymous means to report suspicious activity; e.g., Whistleblower Hotlines

Example of structuring a predictive model that combines psychosocial and cyber data into red flag identification

The Human Element & Investigative Challenges of Insider Threats

- Insider threats commonly exhibit human behaviors that foreshadow the attacker’s intent
- Human intelligence, monitoring and good management oversight are necessary to identify the potential warning signs of insider activity and the appropriate method to intervene before an attack occurs and mitigate the effects if an attack does take place
Structuring an Insider Threat Mitigation Program

- While it may be virtually impossible to completely eliminate insider attacks, an insider threat mitigation program can greatly reduce their prevalence and impact.
- Successful programs take a holistic approach involving a combination of technology, legal, policy, physical security, awareness and training and counterintelligence resources.

Establish a Working Group

- Provides governance, oversight and direction
- Dependant upon sufficient personnel, technology and financial resources
- Must be supported by top-level management
- Includes senior representatives from technology, legal, policy, physical security, awareness and training and counterintelligence resources.
- This group should be consulted when developing new insider threats policies or responding to detected threats.

Establish and Insider Threat Team

- Maintains a separate identity to the rest of the firm- separation enables an insider threat team to conduct independent, unbiased investigations.
- Facilitates communication across different functions of the firm- keeping the information flow between abuses reported to HR, IT and security open.
- Establish internal controls to maintain integrity of the program- personnel assigned to insider threat mitigation are not immune to posing an insider threat risk themselves.
  - Involve senior personnel in regularly scheduled compliance reviews
  - Avoid unwarranted invasions of privacy
  - Develop special access procedures for extremely sensitive information
## Implementing an Insider Threat Mitigation Program

### 7 Core Steps

<table>
<thead>
<tr>
<th>Step 1</th>
<th><strong>Prioritize and Scope.</strong> The organization identifies its business/mission objectives for its insider threat program, high-level organizational priorities and associated risk tolerances</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td><strong>Orient.</strong> Once the scope of the program has been determined for the business, the organization identifies related systems and assets, regulatory requirements, legal constraints and overall risk approach. The organization then identifies threats to, and vulnerabilities of, those systems and assets</td>
</tr>
<tr>
<td>Step 3</td>
<td><strong>Assess Current State.</strong> The organization develops a current state for their insider threat program</td>
</tr>
<tr>
<td>Step 4</td>
<td><strong>Conduct a Risk Assessment.</strong> The organization analyzes the operational environment in order to discern the likelihood of an insider driven event and the impact that the event could have on the organization</td>
</tr>
<tr>
<td>Step 5</td>
<td><strong>Create a Target State.</strong> The organization develops a future state for their insider threat program</td>
</tr>
<tr>
<td>Step 6</td>
<td><strong>Determine, Analyze, and Prioritize Gaps.</strong> The organization compares the current state to the future state to determine gaps. Next it creates a prioritized action plan to address those gaps that draws upon mission drivers, a cost/benefit analysis, and understanding of risk to achieve the outcomes in the target state</td>
</tr>
<tr>
<td>Step 7</td>
<td><strong>Implement Action Plan.</strong> The organization determines which actions to take in regards to the gaps identified in the previous step. It then monitors its current practices against the target state</td>
</tr>
</tbody>
</table>
Privacy & Employment Laws and Legal Risk

Although insider threat mitigation programs can protect firms from potentially crippling theft and system damage, they may also expose firms to some legal risk.

The best practices framework articulates guidelines around some of the most common legal risks inherent to an insider threat mitigation program for consideration and encourages the use of legal counsel throughout implementation.

<table>
<thead>
<tr>
<th>1. Electronic communications monitoring</th>
<th>2. Background checks and screening</th>
<th>3. Foreign Privacy and Employment Law Constraints</th>
<th>4. Dismissal</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Federal Laws generally permits employers that provide employees with internet and email service to monitor those services to the extent that they are used in the ordinary course of the employers’ business. Employers that provide internet or email service through a third party, or those that wish to monitor internet use that falls outside of the ordinary course of business, may wish to rely instead on the “consent exception”</td>
<td>• The Fair Credit Reporting Act (FCRA)- Employers will minimize their risk exposure by complying with FCRA standards for all types of financial background investigations and screening</td>
<td>• Foreign countries’ privacy and employment regulations and protections often differ significantly from those of the United States. While firms should always consult local counsel in foreign jurisdictions where they intend to implement an insider threat mitigation program, the best practices guide provides a general overview of some of the principal laws that may impact such programs in Germany, the United Kingdom (UK), India, and Hong Kong.</td>
<td>• Dismissal based on Valid Reason must be proven in one of these categories: capability or qualifications, conduct, redundancy, breach of a statutory duty or restriction and “some other substantial reason”</td>
</tr>
<tr>
<td>• Only a few states have enacted statutes that specifically address electronic monitoring in the workplace</td>
<td>• EEOC Guidance on the consideration of Criminal History suggest that use of such criminal history in making employment decisions may violate Title VII of the Civil Rights Act of 1964, because national data suggests that criminal history exclusions have a disparate impact on certain racial and ethnic minorities</td>
<td>• Social Media: While examining publicly-available social media profiles can be an informative part of applicant screening, firms should be mindful that nineteen states have enacted laws prohibiting employers from forcing applicants or employees to reveal their personal, private profiles</td>
<td>• Fair Procedure should be followed investigating all outstanding issues, informing employee of the issues in writing, right of accompaniment, disciplinary hearings, employee opportunity to appeal written decisions</td>
</tr>
<tr>
<td>• Providing employees notice of monitoring is always a best practice especially careful to fully disclose their monitoring policies</td>
<td></td>
<td>• Penalties offer a less severe disciplinary measure if appropriate</td>
<td>• Notice: Consider terms in employment contract as measured against jurisdiction</td>
</tr>
</tbody>
</table>