Spotlight on Insider Fraud in the Financial Services Industry

Sarah Miller, CISSP, CIPT, CIPP/US
National Insider Threat Center
CERT® Division
Presenter Biography

Sarah Miller (CISSP, CIPT, CIPP/US) is an Insider Threat Researcher supporting the CERT® Division’s National Insider Threat Center (NITC) at Carnegie Mellon University’s Software Engineering Institute.

- Serves as the Chair of the Open Source Insider Threat (OSIT) information sharing group for industry insider threat practitioners.
- Develops detection and mitigation strategies for insider threat programs.
- Collaborate on insider threat program building for customers.
- Teaches public and custom insider threat courses.
- Conducts sector-specific, supply chain, cybersecurity best practices, collusion, kinetic threats, privacy, and other insider threat research.

Education
- MS in Information Security Policy and Management, Heinz College, Carnegie Mellon University
- MA in Rhetoric, Carnegie Mellon University
- BA in English and Psychology, McDaniel College
The CERT Division’s National Insider Threat Center (NITC)

- **Focus:** Providing insider threat expertise across sectors
- **History:** Launched work in 2001 with the U.S. Secret Service and formalized as NITC in 2017
- **Mission:** Enable effective insider threat mitigation, incident management practices, and develop capabilities for deterring, detecting, and responding to evolving cyber and physical threats
- **Action and Value:** Conduct research, modeling, analysis, and outreach to develop and transition socio-technical solutions to combat insider threats
The NITC Definition of Insider Threat

The potential for an individual who has or had authorized access to an organization’s assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization.
## What / Who Is an Insider Threat?

<table>
<thead>
<tr>
<th>Individuals</th>
<th>Organization’s Assets</th>
<th>Intentionally or Unintentionally</th>
<th>Negatively Affect the Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current or Former</td>
<td>People</td>
<td>Fraud</td>
<td>Harm to Organization’s Employees</td>
</tr>
<tr>
<td>Full-Time Employees</td>
<td>Information</td>
<td>Theft of Intellectual Property</td>
<td>Degradation to CIA of Information or Information Systems</td>
</tr>
<tr>
<td>Part-Time Employees</td>
<td>Technology</td>
<td>Cyber Sabotage</td>
<td>Disruption of Organization’s Ability to Meet its Mission</td>
</tr>
<tr>
<td>Temporary Employees</td>
<td>Facilities</td>
<td>Espionage</td>
<td>Damage to Organization’s Reputation</td>
</tr>
<tr>
<td>Contractors</td>
<td></td>
<td>Workplace Violence</td>
<td>Harm to Organization’s Customers</td>
</tr>
<tr>
<td>Trusted Business Partners</td>
<td></td>
<td>Social Engineering</td>
<td></td>
</tr>
</tbody>
</table>

- **Use that access**: who have or had authorized access to.
- **Intentionally or Unintentionally**: use that access to act in a way that could.
- **Negatively Affect the Organization**: harm to organization’s employees, degradation to CIA of information or information systems, disruption of organization’s ability to meet its mission, damage to organization’s reputation, harm to organization’s customers.
Collaborations (Past, Current, Future)

<table>
<thead>
<tr>
<th>Organizations</th>
<th>Focus Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain experts</td>
<td>• Psychology (Secret Service, FBI, DoD, NITC Visiting Scientists)</td>
</tr>
<tr>
<td></td>
<td>• Espionage (DoD)</td>
</tr>
<tr>
<td>Interagency working group</td>
<td>• Espionage case collection and analysis</td>
</tr>
<tr>
<td></td>
<td>• Identification of patterns of espionage indicators</td>
</tr>
<tr>
<td></td>
<td>• Counterintelligence</td>
</tr>
<tr>
<td>Federal law enforcement</td>
<td>• Case analysis and information from victim organizations and perpetrators</td>
</tr>
<tr>
<td></td>
<td>• Organizational vulnerabilities</td>
</tr>
<tr>
<td></td>
<td>• Effective countermeasures</td>
</tr>
<tr>
<td>National labs, FFRDCs, critical infrastructure providers</td>
<td>• Automated detection enhancements</td>
</tr>
<tr>
<td></td>
<td>• Sector-specific assessments</td>
</tr>
<tr>
<td>Tool vendors, infrastructure providers</td>
<td>• Automated detection enhancements</td>
</tr>
<tr>
<td></td>
<td>• Emerging technologies (e.g., cloud computing)</td>
</tr>
<tr>
<td>Large auditing/consulting firms</td>
<td>• Assessments/follow-on guidance</td>
</tr>
</tbody>
</table>
The CERT National Insider Threat Center Approach to the Problem
NITC Incident Corpus

Collection of over 1600 analyzed insider threat incidents, with hundreds more identified

Standardized incident coding methodology allows analysis of technical actions and observable behaviors

Body of empirical data provides a basis for threat models, technical and administrative control development, and risk quantification

'host=HECTOR [search host="zeus.corp.merit.lab" Message="A user account was disabled. *" | eval Account_Name=mvindex(Account_Name, -1) | fields Account_Name | strcat Account_Name "@corp.merit.lab" sender_address | fields - Account_Name] total_bytes > 50000 AND recipient_address!="*" corp.merit.lab" startdaysago=30 | fields client_ip, sender_address, recipient_address, message_subject, total_bytes'
Representation of Financial Services in Incident Corpus

Over 1 in 4 victim organization records in the CERT Insider Threat Incident Corpus involves Fraud in the Financial Services sector.
Adapting the CERT National Insider Threat Center Approach to Insider Threat Program Operations
NITC’s Critical Path to Insider Risk

Insider Threats Impacting Banks and Credit Unions

Case Examples
A foreign currency trader took advantage of both administrative and technical vulnerabilities in order to conceal their declining work performance. The insider was ordered to pay $700 million in restitution and sentenced to 7.5 years in prison. The insider was required to pay the victim organization $1,000 a month during 5 years of probation.
A manager and at least 9 unwitting accomplices enable the theft of almost $50 million over almost 20 years from the employer.

**Background**
- Drug and alcohol abuse
- Substantial gambling habit

**Insider social engineered management**
- New computer system with improved controls
- Convinced management they should keep using old computer system

**Issued fraudulent refunds to fake companies**
- Almost 20 years
- Nearly 250 fraudulent checks
- Totaled nearly $50 million

**Liked helping people**
- Gave coworkers money for tuition, funerals, clothing, etc.
- Told coworkers they had received inheritance
- Owned multiple homes valued at several million dollars
- Owned luxury cars, expensive jewelry, …
A manager at a small, local bank engaged in a lapping scheme over the course of five years. The damages caused by the insider were estimated to be as high as $1 Million. The insider was sentenced to 30 months in prison and restitution.

The insider took efforts to conceal their theft:
- Stealing money from one account to pay back the other (i.e., lapping)
- Created and directly sent false bank statements of victim’s accounts
- Modified victim accounts to have legitimate bank statements sent elsewhere

The insider’s coworkers noticed security violations by the insider, but did not report them:
- Using coworkers’ computers
- Teller drawers out of balance

The insider experienced personal issues:
- Grief related to death of a relative
- Other relatives began observing a “spending problem” in the insider after this loss

The insider was discovered through an audit:
- The insider fell ill and had to be hospitalized, making them unable to keep up with their concealment.
- A customer that had a compromised account lodged a concern.
- In response, the bank conducted an audit and discovered the insider’s activity.
Sabotage and Fraud

A systems administrator at a financial services firm distributed a logic bomb on their employer’s systems. The victim organization never fully recovered from the insider’s actions. The insider was sentenced to more than 90 months imprisonment.

The organization announced to employees that bonuses would be half of what they normally were.

• The insider had complained about the lower bonus to their supervisor.

The insider built and distributed a logic bomb on one of the organization’s networks.

• 2,000 servers at HQ impacted
• 370 servers at branch offices impacted
• Used VPN from home

Before the logic bomb’s planned detonation, the insider purchased put options (an option to sell assets at an agreed price on or before a particular date) on the company.

• The insider expected the subsequent detonation of the logic bomb would drive stock prices down.

Although stock prices did not drop, the victim organization lost over $3 million in reports and loss of operations.

• The victim organization began to suspect the insider.
• The insider then resigned.
• A forensic investigation revealed the insider’s involvement.
Insider Fraud Study and Updated Statistics
Insider Fraud Study


• Conducted by the NITC in collaboration with the U.S. Secret Service (USSS)

Low and Slow

Criminals who executed a “low and slow” approach accomplished more damage and escaped detection for longer.

There are, on average, approximately 5 years between a subject’s hiring and the start of the fraud. There are 42 months between the beginning of the fraud and its detection.
Average Financial Impact by Position Type in Finance and Insurance

Executive: $2,385,335
Management: $2,241,495
Non-management: $5,308,614

Financial Impact (in USD)

- Average Impact (Low Estimate)
- Average Impact (High Estimate)
General Fraud Trends from NITC Corpus
Non-Technical Positions

Over three-quarters of fraudsters occupied non-technical positions, such as

- Bank teller
- Bookkeeper
- Cashier
- Clerk
- Receptionist
- Secretary

Positions Held by Insiders

- Non-Technical: 77%
- Technical: 10%
- Unknown: 13%
Fraud by Non-Managers vs. Managers

Financial Impact of Fraud by Employee Type

- **Managers**
  - Average: $2,728,503
  - Median: $500,000

- **Non-Managers**
  - Average: $2,767,776
  - Median: $172,003
Fraud and PII

Personally identifiable information (PII) is a prominent target of those committing fraud.

Non-PII targets primarily involved money, accounting records, and payment systems.
Most fraud cases do not involve collusion. However, it is important to note that

- Approximately 31% of fraudsters do collude.
- Fraud involves collusion more often than other cases.
External collusion is most common in fraud cases, i.e., a bank insider colluding with an external party to facilitate the crime.
Audits, Complaints, and Suspicions

Most incidents were detected through an audit, customer complaints, or co-worker suspicions.

- The most common way attacks were detected was through routine or impromptu audits.
- Over half of the insiders were detected by other victim organization employees, though none of the employees were members of the IT staff.
- As expected, most initial responders to the incidents were managers or internal investigators (75 percent).
### Who were the Fraudsters?

<table>
<thead>
<tr>
<th><strong>Insider Demographics</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Position</strong></td>
<td>Current employees in nontechnical positions</td>
</tr>
<tr>
<td><strong>Tenure</strong></td>
<td>Typically 5 years or more</td>
</tr>
<tr>
<td><strong>Age Range</strong></td>
<td>Two-thirds are between the ages of 31 and 40</td>
</tr>
<tr>
<td><strong>Gender</strong></td>
<td>Fairly even split between male and female</td>
</tr>
<tr>
<td><strong>Marital Status</strong></td>
<td>Fairly even split between single and married</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Attack Metrics</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Target(s)</strong></td>
<td>Personally Identifiable Information (PII), Customer Information (CI), Accounting and Payment Systems</td>
</tr>
<tr>
<td><strong>Method(s)</strong></td>
<td>Authorized access</td>
</tr>
<tr>
<td><strong>Location</strong></td>
<td>On-site</td>
</tr>
<tr>
<td><strong>Time</strong></td>
<td>During normal working hours</td>
</tr>
<tr>
<td><strong>Average Length</strong></td>
<td>38.1 months</td>
</tr>
<tr>
<td><strong>Impact</strong></td>
<td>Average between $2 Million and $2.8 Million</td>
</tr>
</tbody>
</table>
Countermeasures for Fraud

- Clearly document and consistently enforce policies and controls.
- Institute periodic security awareness training for all employees.
- Include unexplained financial gain in any periodic reinvestigation of employees.
- Log, monitor, and audit employee online actions.
- Pay special attention to accountants and managers.
- Restrict access to personally identifiable information.
- Develop an insider incident response plan.
- Provide an Employee Assistance Program or other recourse for employees experiencing personal or financial problems.
Final Thoughts and Additional Case Examples
Theft of IP

The insider had violated policies regarding data exfiltration, encryption, and password settings at a financial firm. The victim organization had over $1 million in damages, but was only awarded $750,000 in restitution.
The insider was motivated by revenge against the victim organization and made no attempt to conceal their activity. Nearly all of the victim organization’s domestic networks had a loss of availability as the result of the insider’s actions. The insider was sentenced to 21 months in prison and ordered to pay nearly $80,000 in restitution.

The same evening that they were warned of their pending termination, the insider committed sabotage.

- Used on-site access outside of work hours
- Transmitted malicious code to 10 routers, erasing configuration files in nine
- Estimated to have taken less than 2 minutes

Ten months after their promotion, the insider had a discussion with their supervisor discussing the insider’s work performance.

- The discussion took place shortly before a major holiday.
- The supervisor indicated to the insider that their termination was probable.

The insider was a contract employee before being promoted to full-time.

- The insider’s requests were rebuffed by the victim organization’s management.

Spotlight on Insider Fraud in the Financial Services Industry
© 2021 Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.
Programs Typically Focus on Insider Incident Management
Programs Need To Develop Insider Risk Management Capabilities
## Recommended Best Practices for Insider Threat Mitigation

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong></td>
<td>Know and protect your critical assets.</td>
</tr>
<tr>
<td><strong>2</strong></td>
<td>Develop a formalized insider threat program.</td>
</tr>
<tr>
<td><strong>3</strong></td>
<td>Clearly document and consistently enforce policies and controls.</td>
</tr>
<tr>
<td><strong>4</strong></td>
<td>Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.</td>
</tr>
<tr>
<td><strong>5</strong></td>
<td>Anticipate and manage negative issues in the work environment.</td>
</tr>
<tr>
<td><strong>6</strong></td>
<td>Consider threats from insiders and business partners in enterprise-wide risk assessments.</td>
</tr>
<tr>
<td><strong>7</strong></td>
<td>Be especially vigilant regarding social media.</td>
</tr>
<tr>
<td><strong>8</strong></td>
<td>Structure management and tasks to minimize unintentional insider stress and mistakes.</td>
</tr>
<tr>
<td><strong>9</strong></td>
<td>Incorporate malicious and unintentional insider threat awareness into periodic security training for all employees.</td>
</tr>
<tr>
<td><strong>10</strong></td>
<td>Implement strict password and account management policies and practices.</td>
</tr>
<tr>
<td><strong>11</strong></td>
<td>Institute stringent access controls and monitoring policies on privileged users.</td>
</tr>
<tr>
<td><strong>12</strong></td>
<td>Deploy solutions for monitoring employee actions and correlating information from multiple data sources.</td>
</tr>
<tr>
<td><strong>13</strong></td>
<td>Monitor and control remote access from all endpoints, including mobile devices.</td>
</tr>
<tr>
<td><strong>14</strong></td>
<td>Establish a baseline of normal behavior for both networks and employees.</td>
</tr>
<tr>
<td><strong>15</strong></td>
<td>Enforce separation of duties and least privilege.</td>
</tr>
<tr>
<td><strong>16</strong></td>
<td>Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.</td>
</tr>
<tr>
<td><strong>17</strong></td>
<td>Institutionalize system change controls.</td>
</tr>
<tr>
<td><strong>18</strong></td>
<td>Implement secure backup and recovery processes.</td>
</tr>
<tr>
<td><strong>19</strong></td>
<td>Close the doors to unauthorized data exfiltration.</td>
</tr>
<tr>
<td><strong>20</strong></td>
<td>Develop a comprehensive employee termination procedure.</td>
</tr>
<tr>
<td><strong>21</strong></td>
<td>Adopt positive incentives to align the workforce with the organization.</td>
</tr>
<tr>
<td><strong>Upcoming:</strong></td>
<td>22 – Learn from insider threat incidents.</td>
</tr>
</tbody>
</table>
Acceptable Levels?

Risks can be expressed as a function of **impact** and **likelihood**

Deploying controls doesn’t necessarily reduce the likelihood of a threat occurring, especially for insider threats.

How much insider risk is our organization willing or able to withstand while still carrying out its mission?

• To begin to answer this question, we need quantifiable and actionable **risk appetite statements**
  - To do this, we need reliable, sound methods for measuring the likelihood and impact of insider threats
Contributing Factors in Risk Perception

- **Human / Cognitive Factors**
  - Fatigue or tiredness
  - Subjective mental workload
  - Situational awareness
  - Mind wandering
  - Framing
  - Other cognitive biases

- **Psychological and Sociocultural Factors**
  - Personality predispositions
  - Culture and subculture
  - Gender
  - Mood

- **Physiological Factors**
  - Age effects and variations over time
  - Influence of drugs and / or hormones

- **General Organization Factors**
  - Business process requirements (BPRs)
Past, Present, and Future Research

What do insider incidents look like?
- Insider Threat Incident Corpus
- Threat Models
  - Fraud
  - Theft of IP
  - IT Sabotage
  - Espionage
  - Unintentional Insider Threats
  - Workplace Violence
- Critical Path to Insider Risk
- Insider Threat Vulnerability Assessment

What motivates and enables insider to carry out their attacks?
- Insider Threat Incident Corpus
- Threat Models
  - Fraud
  - Theft of IP
  - IT Sabotage
  - Espionage
  - Unintentional Insider Threats
  - Workplace Violence
- Critical Path to Insider Risk
- Insider Threat Vulnerability Assessment
- Common Sense Guide
- CERT Guide to Insider Threats
- Standards (National Insider Threat Policy and Minimum Standards, NIST 800-53 Rev. 4 Insider Threat Controls)

What should organizations do to prevent, detect, and respond to insider incidents?
- What should organizations do to manage insider risk, and what resources are required?
- How can we prove that recommended controls are working, or will work?
- When do autonomous systems need to be considered insiders?
- How can organizations positively deter insider threats?
- What is the security equivalent to the Turing test?
- Can we trust autonomous systems to watch the watchers?
- Developing and validating analytics that align to the concepts of engagement, connectedness, and organizational supportiveness

- Big data and text analytics for insider risk management
- Potential Risk Indicator Development and Validation Processes
- Insider Threat Program Evaluation
- Insider Threat Training Courses
- Lab Development
- Tool Testing
- Test Data Synthesis
- Modeling and Simulation
- What is the security equivalent to the Turing test?
NITC Publications and References


Open Source Insider Threat (OSIT) Information Sharing Group

- Community of Interest for insider threat program practitioners across industry organizations
- Over 550 members from over 220 organizations
- Supports volunteer-run special interest groups
  - Data Analytics (DA SIG)
  - Financial Services (FinSer SIG)
- Launched a “partner” community of interest, the Privacy Special Interest Group (PSIG)
Questions?