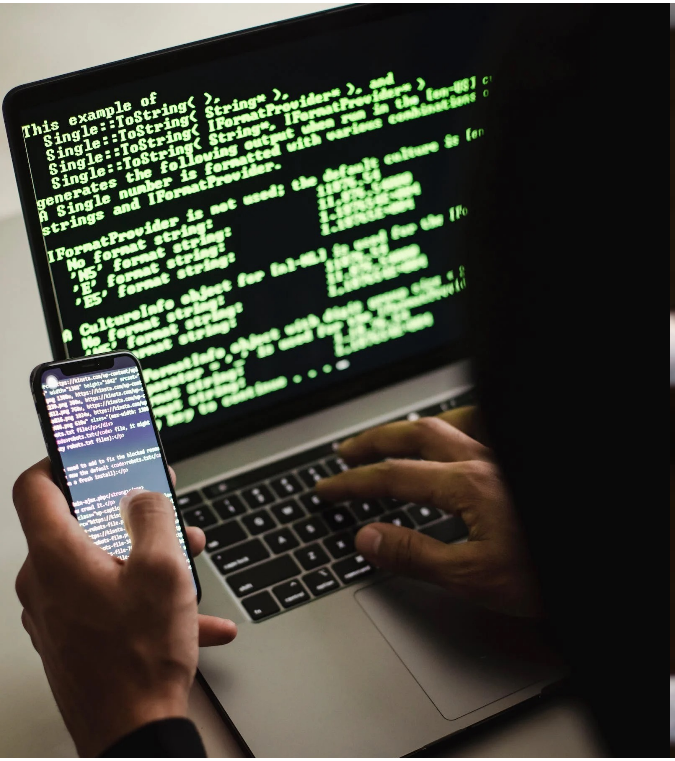


# Healthcare Insider Threat Training

## By: John Petrozzelli
## Director, MassCyberCenter

December 14, 2023

# Overview

1

Part I. Initiation - Why do I need an Insider Threat Program

2

Part II. Planning – How do we build it

3

Part III. Day-to-Day Operations

4

Part IV. Feedback/Interview
s

# Defining an Insider Threat

An insider is any person who has or had authorized **access to or knowledge of** an organization’s resources, including personnel, facilities, information, equipment, networks, and systems.

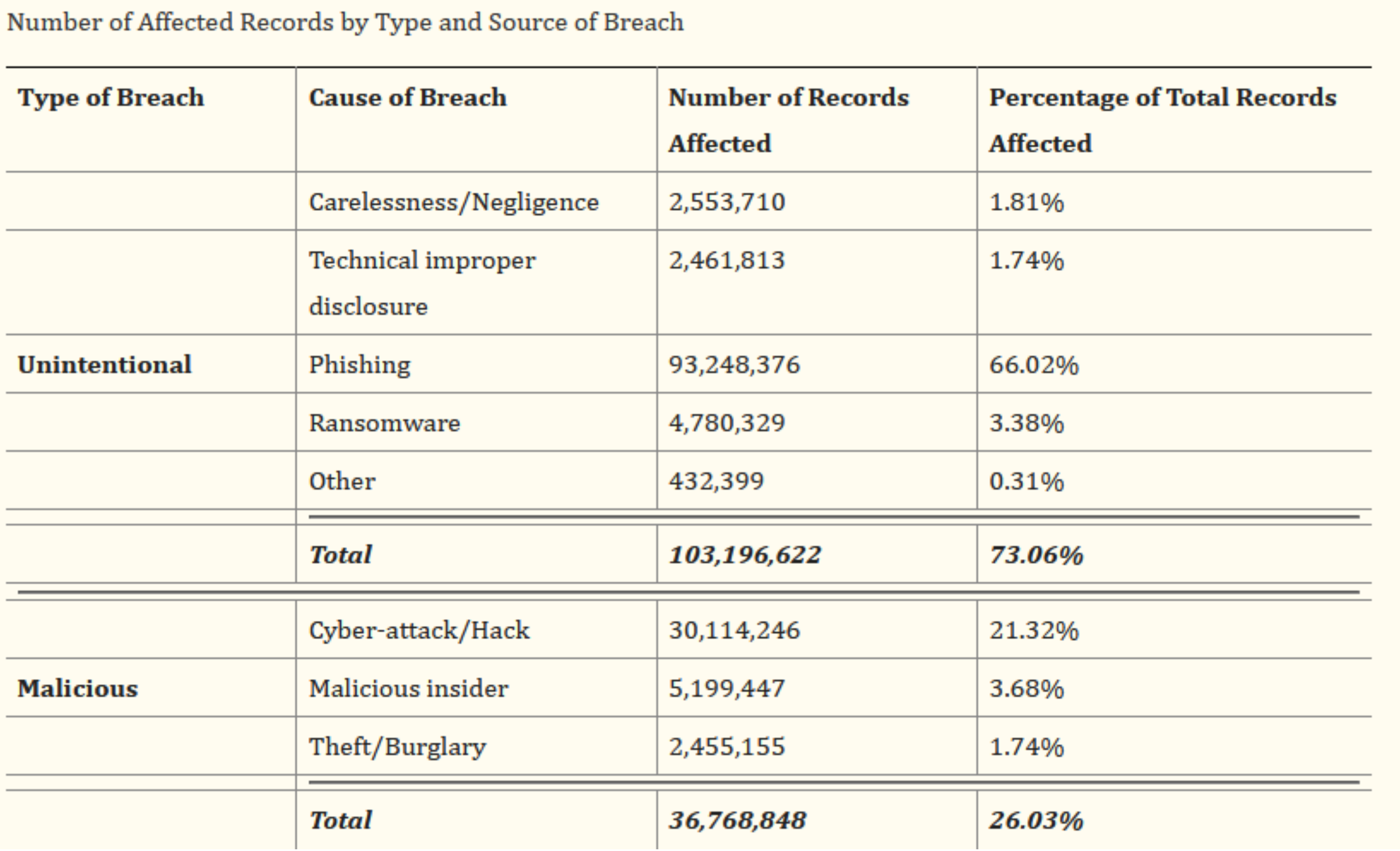
Source: CISA

USD 4.90M

Although relatively rare at 6% of occurrences, attacks initiated by malicious insiders were the costliest, at an average of USD 4.90 million, which is 9.6% higher than the global average cost of USD 4.45 million per data breach

Source: IBM 2023 Cost of a data breach, https://www.ibm.com/reports/data-breach

# Insider Threat Types



Number of Affected Records by Type and Source of Breach

| Type of Breach | Cause of Breach | Number of Records Affected | Percentage of Total Records Affected |
|---|---|---|---|
| Unintentional | Carelessness/Negligence | 2,553,710 | 1.81% |
| | Technical improper disclosure | 2,461,813 | 1.74% |
| | Phishing | 93,248,376 | 66.02% |
| | Ransomware | 4,780,329 | 3.38% |
| | Other | 432,399 | 0.31% |
| | ***Total*** | ***103,196,622*** | ***73.06%*** |
| Malicious | Cyber-attack/Hack | 30,114,246 | 21.32% |
| | Malicious insider | 5,199,447 | 3.68% |
| | Theft/Burglary | 2,455,155 | 1.74% |
| | ***Total*** | ***36,768,848*** | ***26.03%*** |

NIH Study: 1,485 breach events January 2015 and December 2020

Source: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9123525/

Yeo LH, Banfield J. Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis. Perspect Health Inf Manag. 2022 Mar 15;19(Spring):1i. PMID: 35692854; PMCID: PMC9123525.

- **Malicious**
  - Maximus Employee (2022)
    - Breach on last day
    - Sent records to private email account
- **Negligent**
  - Unauthorized access or disclosure
- **Collusive**
  - Lockbit Bounty (2021)
- **Third Party**
  - MOVEit (2023)

# Compliance

- Sarbanes-Oxley Act
- National Industrial Security Program Operating Manual or NISPOM
- Payment Card Industry Data Security Standard
- Health Insurance Portability and Accountability Act
- Gramm-Leach-Bliley Act/FTC Safeguards Rule
- Bank Secrecy Act
- General Data Protection Regulation (EU) 2016/679 (GDPR)
- NIST 800-53 Rev. 5 and E.O 13587

# Health Insurance Portability and Accountability Act

5 HIPAA Requirements Insider Threat Monitoring Tools Can Help Address

- **308 – Compliance Reviews**
    - Easily access comprehensive user activity audits and reports on-demand, and (optionally) automatically distribute reports to the right people.
- **306 – Security Standards**
    - Coach user behavior in the event that they are about to breach policy or HIPAA compliance standards, update them on policy changes, or ensure understanding of policy with in-the-moment messaging.
- **308 – Administrative Safeguards**
    - Understand how your users are accessing systems and data with full metadata capture (both text-based and video), tracking access to files, folders, and policy breaching keyword triggers and alerts.
- **132 – Technical Safeguards**
    - Obtain visibility into every user action (with the ability to anonymize key identifying information), including applications without internal logs, so you can understand exactly what a user did. In addition, it is possible to provide manual and automatic log off to any system.
- **414 – Administrative Requirements & Burden of Proof**
    - Tie all visual and textual metadata logs to individual users, thanks to a requirement for individual credentials to access systems, servers, and networks, ensuring that all data is captured in the event that proof of policy or compliance breach is needed.

https://www.proofpoint.com/us/blog/insider-threat-management/how-meet-hipaa-compliance-requirements-insider-threat-monitoring

# Risk Assessment

Cybersecurity Insurance

Third Party Vendor Questionaires

Risk Management Programs

# Overview

1

Part I. Initiation - Why do I need an Insider Threat Program

2

Part II. Planning – How do we build it

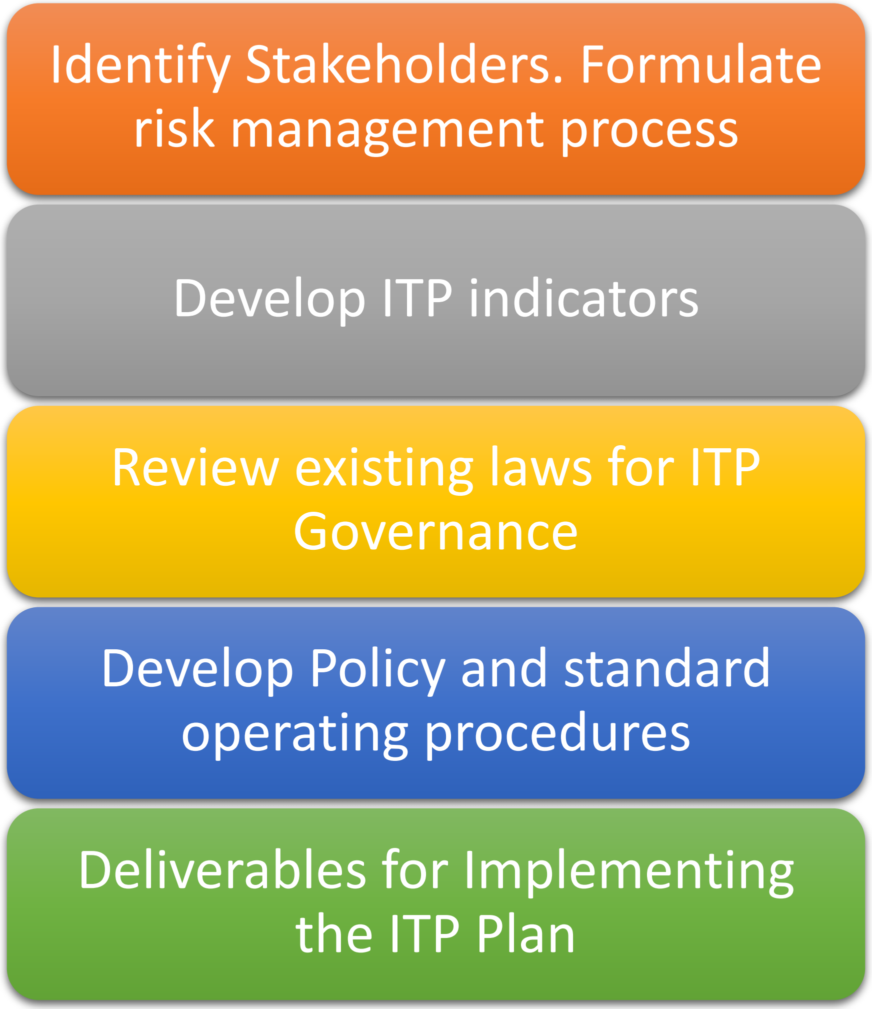
3

Part III. Day-to-Day Operations

4

Part IV. Feedback/Interview s

# Risk Assessment: How do we build it?



Identify Stakeholders. Formulate risk management process

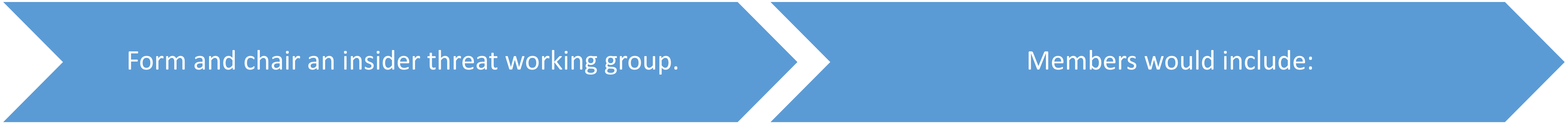
Develop ITP indicators

Review existing laws for ITP Governance

Develop Policy and standard operating procedures

Deliverables for Implementing the ITP Plan

# Identify Stakeholders



Form and chair an insider threat working group.

Members would include:

- Legal
- Compliance
- Security
- Human Resources
- C-Suite representatives to include representative of the Chief Trust Officer or Chief Information Security Officer
- IT Operations
- Security Engineering
- Finance
- Product Management
- Science and Technology
- Business Operations
- Media

# Formulate Risk Management Process

a. Identify key assets (evaluate assets based upon criticality, reputation, financial damage, loss of trust, etc).

b. Identify insider and outsider threats.

c. Vulnerability assessment (based upon exposure and access).

  i. Likelihood

  ii. Consequences

  iii. Criticality

  iv. Vulnerability

  v. Threat actor intent

  vi. Threat actor capability

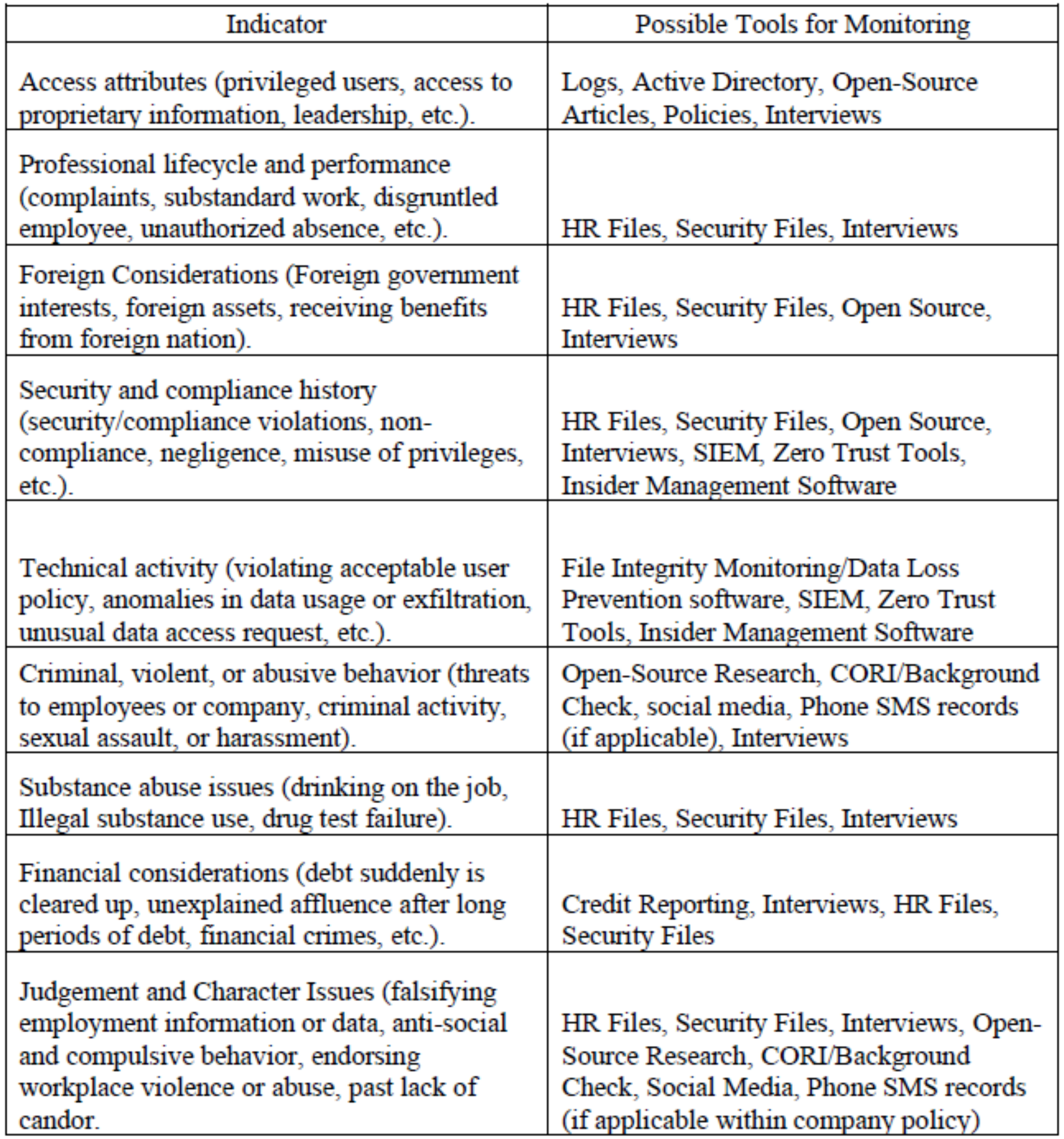
https://www.dhs.gov/sites/default/files/publications/rma-risk-management-fundamentals.pdf

# Develop ITP Indicators

a. Access attributes (privileged users, access to proprietary information, leadership, etc.).
b. Professional lifecycle and performance (complaints, substandard work, disgruntled employee, unauthorized absence, etc.).
c. Foreign Considerations (Foreign government interests, foreign assets, receiving benefits from foreign nation).
d. Security and compliance history (security/compliance violations, non-compliance, negligence, misuse of privileges, etc.).
e. Technical activity (violating acceptable user policy, anomalies in data usage or exfiltration, unusual data access request, etc.).
f. Criminal, violent, or abusive behavior (threats to employees or company, criminal activity, sexual assault or harassment).
g. Substance abuse issues (drinking on the job, Illegal substance use, drug test failure).
h. Financial considerations (debt suddenly is cleared up, unexplained affluence after long periods of debt, financial crimes, etc).
i. Judgement and Character Issues (falsifying employment information or data, anti-social and compulsive behavior, endorsing workplace violence or abuse, past lack of candor.

https://www.cdse.edu/documents/toolkits-insider/INTJ0181-insider-threat-indicators-job-aid.pdf

# Develop ITP Indicators (Cont.)



| Indicator | Possible Tools for Monitoring |
|---|---|
| Access attributes (privileged users, access to proprietary information, leadership, etc.). | Logs, Active Directory, Open-Source Articles, Policies, Interviews |
| Professional lifecycle and performance (complaints, substandard work, disgruntled employee, unauthorized absence, etc.). | HR Files, Security Files, Interviews |
| Foreign Considerations (Foreign government interests, foreign assets, receiving benefits from foreign nation). | HR Files, Security Files, Open Source, Interviews |
| Security and compliance history (security/compliance violations, non-compliance, negligence, misuse of privileges, etc.). | HR Files, Security Files, Open Source, Interviews, SIEM, Zero Trust Tools, Insider Management Software |
| Technical activity (violating acceptable user policy, anomalies in data usage or exfiltration, unusual data access request, etc.). | File Integrity Monitoring/Data Loss Prevention software, SIEM, Zero Trust Tools, Insider Management Software |
| Criminal, violent, or abusive behavior (threats to employees or company, criminal activity, sexual assault, or harassment). | Open-Source Research, CORI/Background Check, social media, Phone SMS records (if applicable), Interviews |
| Substance abuse issues (drinking on the job, Illegal substance use, drug test failure). | HR Files, Security Files, Interviews |
| Financial considerations (debt suddenly is cleared up, unexplained affluence after long periods of debt, financial crimes, etc.). | Credit Reporting, Interviews, HR Files, Security Files |
| Judgement and Character Issues (falsifying employment information or data, anti-social and compulsive behavior, endorsing workplace violence or abuse, past lack of candor. | HR Files, Security Files, Interviews, Open-Source Research, CORI/Background Check, Social Media, Phone SMS records (if applicable within company policy) |

MassCyberCenter
at the MassTech Collaborative

# Review Existing Laws for ITP Governance

Sarbanes-Oxley Act

National Industrial Security Program Operating Manual or NISPOM

Payment Card Industry Data Security Standard

Health Insurance Portability and Accountability Act

Gramm-Leach-Bliley Act

Bank Secrecy Act

General Data Protection Regulation (EU) 2016/679 (GDPR)

NIST 800-53 Rev. 5 and E.O 13587

# Develop Policy & Standard Operating Procedures

a. Review existing policy to determine current processes. Identify existing authorities, policies, procedures, incident response plans, and tools/collected data sources.

b. Consider existing data retention requirements for possible modification. The ITP requirements may need longer data retention.

c. Hold one-on-one or one-on-many introductory stakeholder meetings to explain ITPM's background and goals: solicit feedback on program.

d. Review existing technical collection platforms available in the Security infrastructure. Review current publicly available data collection techniques utilized by Security to detect insider/outside threats.

e. Coordinate policy drafts with Legal, Compliance, Security, HR, C-Suite representatives to include CISO, CTO,  CIO or IT Operations, Security Engineering, Finance, Product Management.

1) Incorporate as much existing policy, human capitol, and technology already sharing roles compatible with the insider threat mission.

2) Modify existing policies and procedures to include insider threat mitigation.

**Onboarding and offboarding procedures are key to make sure employees have role-based access only when necessary**

# Acceptable Use Policy

- Consent to monitoring
- Use of social media
- Examples of acceptable behavior
- Examples of unacceptable behavior
- Guidance on reporting insider threats
- Guidance on mobile device usage or refer to BYOD policy
- Guidance on work related travel

# Deliverables for Implementing the ITP Plan

Insider Threat working group charter (Authored by ITPM and ITP Working Group)

ITP Standard Operating Procedures (Authored by ITPM and ITP Working Group)

Incident response plan (ITPM is lead author: co-authored/reviewed by ITP Working Group)

Indicators and corresponding investigative actions (Authored by ITPM: reviewed by ITP Working Group)

Insider Threat training module

# Overview

1

Part I. Initiation - Why do I need an Insider Threat Program

2

Part II. Planning – How do we build it

3

Part III. Day-to-Day Operations

4

Part IV. Feedback/Interview s

# Part III: Day to Day Operations

### Establish Trust

1 Say hi when you don't need something

2 Deliver on any commitments

### Review available data

1 Audit Data

2 Personnel files

3 Sign-ins

### Stay current on insider threat activity worldwide

1 Technology available to thieves

2 Trends (insider ransomware)

# Overview

1

Part I. Initiation - Why do I need an Insider Threat Program

2

Part II. Planning – How do we build it

3

Part III. Day-to-Day Operations

4

Part IV. Feedback/Interview s

# Part IV: Interviews

Clarifying – Initial fact gathering

Informational – cordial fact gathering

Soft – Present some findings and ask for responses – not challenging

Hard – Present findings, challenge responses, provide warnings, provide possible outcomes of non-compliance

# Questions?