NOT FOR PUBLIC DISSEMINATION – FOR USE BY INSIDER THREAT PEERS ONLY

Insider Threat Lessons Learned – Tim Kirkham 2019

The below is based upon my personal experience building Insider Threat Programs it does not represent policy or practice of my current or past employers:

- Effective Insider Risk monitoring, response and investigation is increasingly becoming a corporate expectation as opposed to a "special project" that must be sold to stakeholders
- There is no "one size fits all", this session is intended to help attendees benefit from lessons learned, consider and discuss options for your specific company, business or agency
- Building an **effective response process and investigations team is critical to successful mitigation** – DLP is not an Insider Threat Program
    - Response/Triage – My preference is cyber security owns the tools, conducts triage solely to eliminate false positives. ALL confirmed alerts are sent to Insider risk team for one of two types of review
        - Assessment - Limited scope to determine job scope, access, impact, motivation
        - Investigation – approved by working group based on predication
    - Number of investigators? Budget constraints. Fit the to assessment role (less skilled) or Investigation role (more skilled), ie. Investigator 1 and Investigator 2 system
    - Skill level? SOFT SKILLS ARE KEY for investigators
    - Prioritization – Risk Score? You need an effective way to prioritize cases. Think AIM
    - Workforce reductions- these will tax your systems
    - Offboarding – Secure offboarding programs Bring business value!
        - Consider the value of key verbiage in offboarding briefings especially on work force reductions:
            - Example: "We know that many employees store personal information on company issued systems. Our experience has shown offboarding employees often inadvertently mix sensitive company data in with personal data when downloading in preparation for departure. If you have downloaded any information from company systems, or sent via email or cloud storage, please allow us to examine that information to ensure no company owned data was inadvertently included. This will

avoid delays or complications in the offboarding process based upon our cyber security review"

- Often people will self-surrender storage devices based on this verbiage, it is most effective if it is read aloud to them.

- Working groups – Include all key stakeholders, meet on a regular basis
- Metrics – Loss Prevention vs. Recovery .. Why? I prefer term loss prevention, leverage business leaders to help provide values for data you keep in house
- **Technology**
  - Monitoring – do you really want to use this word?
  - DLP – Must have a good foundation for alerts
  - Data Inventory and Marking are critical to maximize tools
  - UBA
    - Data sources can be challenging to obtain
    - Data feeds need to be current

- **Employee Awareness**
  - Employee awareness is critical to your program's success
    - Gain buy in of stakeholders
    - Minimize unintentional insiders
    - Trade show USB's
    - Minimize exploitation potential
    - Talents programs – this can be sensitive but you must let your employees know they could be exploited by these programs
    - Elicitation – SOE's and others use elicitation to obtain information
    - Increased reporting of suspicious activity
  - Awareness IS prevention
- **Sustainability**
  - Policy and Standards
  - Corporate policy
  - Security policy

    - Standard
    - Charter
- **Insights**
    - Keeping your investigations team motivated can be a challenge
    - They will get 100 cases that result in nothing for every big win
    - Must constantly seek out that 1% that can truly damage the enterprise and then
    - BROADCAST THE WINS
    - Link your investigators up with forensics team
    - Investigators are better when they understand the forensics and logs
    - Work business unit contacts like sources
    - Your program will not succeed without BU buy in. When you find supporters find ways to stay in contact and provide service to them, it will pay off.
    - Collaborate closely with HR to gain traction in offboarding
    - Hire or develop investigators with good soft skills. If employees are surrendering removable media and thanking your team for keeping them out of trouble, you are winning
    - A prosecution is likely a loss for an Insider Threat program. Think Prevention
    - Root cause analysis is a great value add for the business
    - Secure offboarding saves $ and wins friends in the business

AIM = ACCESS, IMPACT, MOTIVATION – This is an example of my method to prioritize insider alerts which I refer to as AIM…..

AIM Score (Access, Impact, Motive)

Motive	Low	Medium	High
High	Medium	High-Medium	High
Medium	Low	Medium	High-Medium
Low	Low	Low	Medium

Access/Impact

Items to consider for Access/Impact:

Access to sensitive data? e.g.

- Financial data
- Mergers & Acquisitions (M&A)
- Customer lists or pricing
- Customer data
- Supplier data - pricing
- Business proposals
- NDA Product roadmaps
- Product vision/strategy
- Special projects
- Source code
- Proprietary Processes
- Design models / Prints / Drawings
- Manufacturing processes
- Executive communications
- Personal information
- Company credit card information

Elevated access? e.g.

- System administrator - 2 points
- Application administrator - 2 points
- Customer system access
- IT support / help desk
- Access to cloud-based systems
- Access to Financial systems, bank accounts

Items to consider for Motive (likelihood):

- Threaten or harass other employees
- Coworker conflicts, disagreements
- Cited for past security violations
- Foreign contacts or foreign travel
- Seeking employment with competitor
- Seeking employment with company on denied parties list
- Joined company less than 90 days ago
- Employee on WFR list
- Complaining about other employees or managers
- Unauthorized data transfers to USB, cloud, email
- Improper access and handling of confidential info
- Ethics issues
- Last / multiple performance ratings were low
- Performance Improvement Plan or anticipated PIP
- Passed over for promotion
- Perceived lack of recognition
- Demotion
- Inflated ego
- Financial debt or burden
- Noticeable change in behavior
- Working onsite late or weekends/odd hours for job role
- Unauthorized use of software

Scoring: Access / Impact

For each applicable item above, add 1 point unless otherwise noted.

Low	0-2
Medium	3-5
High	6+

Scoring: Motive

For each item noted above, add 1 point.

Low	0-1
Medium	2-4
High	5+