Building Incident Response Scenarios for Insider Threats

Brian Reed
@breed0
We Are Told the Insider Threat Looks Like This ...
In reality It’s the Good Natured yet Error Prone...
... And for Nine Companies It’s a $100M+ Loss ...

- U.S. Securities and Exchange Commission
  - Securities Exchange Act of 1934
  - Release No. 84429/October 16, 2018
- Nine companies combined for $100M loss
  - All companies lost > $1M
  - Two of nine lost > $30M
... Because of Insider Threats and Impersonators

Fake Executives

Fake Vendors
Key Issues

1. How do we define an insider threat?
2. How do we start to build incident response scenarios for insider threats?
3. What are recognized practices for incident scenario development?
Key Issues

1. How do we define an insider threat?

2. How do we start to build incident response scenarios for insider threats?

3. What are recognized practices for incident scenario development?
Many Types of Insider Threats

Disgruntled Employee

Determined Saboteur

Good-Natured Bozo
Insider Threats Are a Part of Working Life

• There is always the trade-off with collaboration and information sharing that some will misuse their privileges.

• Often many organizations do not account for temporary or role-based privilege escalation, and do not follow well-defined plans to reduce or remove access.

• This can help foster an environment where the barrier of success for a motivated insider is low.
The Cost of Insider Threats

ObserveIT 2018 Cost of Insider Threats:

• 159 Global Organizations surveyed
• Insider Threats caused by:
  • Negligence (64%); $3.81M USD
  • Criminal insider (23%); $2.99M USD
  • Credential Theft (13%): $1.96M USD
• Average of 73 days to contain an incident
  • 16% contained in < 30 days
Insider Incidents Are Based Upon Abuse of Role

- Payroll fraud by HR admin.
- Expenses fraud — collusion by employee and supervisor
- Supplier-invoice fraud
- IP exfiltration
- Customer-targeted fraud

... Not Always Hacking!
We Depend Upon Event Detection Capabilities

- Network and OS anomalies
- ERP application misuse
- Messaging subsystem injections
- Abnormal access requests
- Abnormal data consumption
- Abnormal data movement
There Are a Variety of Insider Threat Personas
Employees Jumping Ship
Looking for or Just Accepted a New Job

Warning Signs:
Frequent absences, unexplained disappearances or unexpected medical appointments.
Workers who accept a new job are the most likely to give data to a competitor, especially in positions such as sales, product development and business intelligence.

Behavioral Clues:
Dissatisfaction with current position
Negative attitude
Trash talking about company goings-on
The Unhappy Camper
Poor Performance Review, Passed Over for Promotion or Placed on Performance Improvement

Warning Signs:
Employee may be consistently out sick the day after receiving news of poor performance or reprimand. Employee keeps score and shows a propensity toward revenge or vindictive behavior.

Behavioral Clues:
Negative affect
“Out-to-get-me” attitude
Quick to point the finger and shift blame
Poisons the well
The Spendthrift
Experiences Acute or Chronic Financial Problems

Warning Signs:
Employee talks excessively about money and how much everything costs. Always seems to be in a financial jam, may get calls from collection agencies at work or talk about taking a second job or freelancing.

Behavioral Clues:
Admission of financial problems
Talking about new sources of income
Lifestyle does not match income level
Borrowing money from coworkers
The Charmer
Poor Performance Review, Passed Over for Promotion or Placed on Performance Improvement

Warning Signs:
Often a fast talker who brags about gaming the system at work and in personal life. No qualms about breaking the rules or cutting corners to get ahead.

Behavioral Clues:
Inappropriately charming, fast talker
Tendency to take things just too far
Willing to break the rules to get ahead
Always on the lookout for a new angle
The Uploader
Saves All Work to a Personal Cloud Account, Regardless of Company Policy

Warning Signs:
Whether deliberate or unintentional, the uploader saves everything to a personal cloud account
He or she refuses to use company sanctioned network drives or cloud stores

Behavioral Clues:
Lacks trust in corporate systems and software
Virtually no files saved to computer or personal network storage
Hesitant to share work
**The Ex**

Romantically Involved With a Co-Worker and Has Experienced Difficulties (or the End)

**Warning Signs:**
Constantly obsesses about a co-worker in a former relationship. May attempt to access business accounts or personal files of the former paramour, often triggering multiple failed password attempts.

**Behavioral Clues:**
Stalker-like behavior
Propensity toward revenge or vindictive behavior
Rage-filled commentary e.g., “they’ll be sorry”
The Lone Worker
Role Requires Working Solo Often in a Remote Location

Warning Signs:
Failure to check in to home base.
Inaccessible via normal contact methods (email, mobile phone)
Failure to make scheduled appointments

Behavioral Clues:
None. Because the role requires lone working, we need to take proactive steps rather than waiting for a crisis situation
Key Issues

1. How do we define an insider threat?

2. How do we start to build incident response scenarios for insider threats?

3. What are recognized practices for incident scenario development?
Look at Your Own Past Incidents

• Can you relate to any of these personas?
• Have you had personas like these (or others) be the cause of security incidents (or a full blown crisis)?
• Are you taking lessons learned from the past, making them candidate improvements for your future IR preparations?
• Have you ever run a table-top exercise to simulate an insider threat (data exfiltration, whistleblower, IP theft, extortion/blackmail)?
Where to Start?

- Governance and Strategy
- Investigation and Mitigation
- Background Investigation
- Awareness and Training
- Asset Management
- User Activity Monitoring

Insider Threat Management Ecosystem
A Harmonized View of Incident Handling

Incident Handling

Legend:
- Similar Tasks and Practices
- Divergent Tasks and Practices

Preparation
- Priorities
- Team

Detection and Analysis
- Collection
- Normalize and Filter

Containment, Eradication and Recovery
- Triage
- Assign

Postincident Activity
- Review
- Report

Candidate Improvements
- Postincident Activity

Recover
- Respond

Candidate Improvements
- Preparing

Respond
Mitigating Insider Threats

- Mitigate Risky Behavior
- Educate and Warn
- Take Action

- Know Your People
- Background Checks
- Continuously Evaluate
- Educate Employees and Vendors

- Monitor Behavior
- Detect People Violating Policy
- Detect Data or Service Misuse
- Investigate Risky Behavior

- Know Your Assets
- Identity Critical Data and Services
- Assess Impact

Mitigate

People

Behavior

Assets
Scenario 1: Compromised Credentials
Scenario 1: Compromised Credentials

Questions to Ask:

• How are you monitoring privileged access?
• What thresholds raise awareness to a potential incident?
• How are you monitoring failed login attempts?
• Do you adjust failed login thresholds differently based on higher-risk systems or users?
Scenario 1: Compromised Credentials

Additional Questions to Ask:

• Do you look at where users have logged in from geographically?

• Are you monitoring (or do you allow) users who share credentials?

• Do you track failed login attempts of disabled, non-existent and removed accounts?

• What is your access lockout policy?
Scenario 2: The Insider Threat
Scenario 2: The Insider Threat

Insider Threat is multi-faceted:

• Abuse of access or privileged that were never revoked
• Also results from over-privileged users with unchecked data access
• The truly malicious insider threat is a minority case but does happen
Scenario 3: Ransomware

All your important files are encrypted!

#What happened?
All your important files (database, documents, images, videos, music, etc.) have been encrypted! And only we can decrypt!
To decrypt your files, you need to buy the decryption key from us. We are the only one who can decrypt the file for you.

#Attention
Trying to reinstall the system and decrypting the file with a third-party tool will result in file corruption, which means no one can decrypt your file (including us), if you still try to decrypt the file yourself, you do so at your own risk!

#Test decryption
As a proof, you can email us 3 files to decrypt, and we will send you the recovered files to prove that we can decrypt your files.

#How to decrypt
1. Buy 0.18 Bitcoin
2. Send 0.18 Bitcoin to the payment address
3. Email your ID to us, after verification, we will create a decryption tool for you.

Remember, bad things have happened, now look at your determination and action!

Your ID
Email: bakhkfiles@protonmail.com
Payment: 3EZGSBP439PbBenWjsGYjSSaAHn9CnKDRQ
Scenario 3: Ransomware

Is your Ransomware response different than your malware response?

• Are their scenarios where you might ever pay a ransom?

• If so, keep in mind your likelihood of being added to a "list" and hit again are much higher.

• If you have cyberinsurance, do not count on response assistance, and do not assume cost recovery on a claim
Key Issues

1. How do we define an insider threat?
2. How do we start to build incident response scenarios for insider threats?
3. What are recognized practices for incident scenario development?
Consult With Others to Profile Realistic Personas

- Finance
- Human Resources
- Legal
- Audit and Compliance
- Remote Business Units
- Other Geographies
Learning From Past Incidents

• Ask yourself — can you turn a past incident into a scenario or tabletop exercise?
• Make this a checkbox on your post-incident report:
  • Candidate for scenario planning development (Y/N)?
  • What missing defenses could have mitigated this incident?
  • How could we decrease our time to respond, contain and remediate?
Equip Your IR Teams Based on Experience

• If your IR team is unfamiliar or new to insider threats, use this as a secondary part of the main exercise (such as data exfiltration)

• If your team is relatively experienced with insider threats, use a complex example (such as employee under duress from extortion, blackmailed employee, corporate espionage, etc.)
Data-centric Tools Can Provide Visibility

CASB – monitor cloud data activity

DCAP – monitoring data across multiple data types (DB, Files) and as data changes

DLP – Can be useful for data visibility and monitoring

UEBA – can correlate user account activity with data events
Compromise Assessments

Proactive assessments of specific systems or networks

You might be able to use proactive hours as part of your IR retainer

Many cyberinsurance carriers also offer limited assessments included with your premiums
Red Team – Blue Team Exercises

No, this is NOT a political debate.

Comes from military origins, one team attacks (**Red**) and one team defends (**Blue**)

Helps to eliminate psychological barriers such as group think, recency effect and confirmation bias

Run internally or bring in a third-party to help coordinate
Tabletop Exercises and Scenario Planning

Some Ideas for Tabletop Exercises:
Use an outside party to facilitate:
• IR Retainer, services provider
• Non-IT/non-InfoSec group/person
Use real-world examples:
• Executive credentials stolen and misused
• Disgruntled employee/contractor/third-party
• Negligence and Theft scenarios – will invoke BCMP and other recovery functions
Recommendations

☑ If you do not have an incident response plan, put one in place.
☑ Add organization-specific scenarios to your incident response plan.
☑ Monitor your risky or high-value employees (not just executives).
☑ Communicate within your organization to understand what insider threat personas potentially carry the highest amount of risk.
☑ Document and test your incident response procedures related to insider threats.
Recommended Gartner Research

- Building Incident Response Scenarios for Insider Threats
  Brian Reed, Jonathan Care (G00380185)

- Market Guide for Employee Monitoring Products and Services
  Jonathan Care (G00353551)

- Market Guide for Digital Forensics and Incident Response Services
  Brian Reed, Toby Bussa (G00349347)

- Toolkit: Security Incident Response Scenario for Phishing Attacks
  Brian Reed, Neil Wynne (G00380176)

- Ignition Guide to Building an Insider Threat Management Program
  CEB Research (G00363867)