November 10, 2023

Insider Threat Monitoring

Mike Lombardi, CISSP
Director, Mandiant

David Payne
Associate General Counsel, Coinbase

Khizar Sheikh
Vice President, American Express

Cody Wamsley, CISSP
Partner, Sterlington

Privacy+ Security Forum

Sterlington

Speakers

Mike Lombardi

Director
Mandiant

David Payne

Associate General Counsel
Coinbase

Khizar Sheikh

Vice President
American Express

Cody Wamsley

Partner
Sterlington

Insider Threats

sus

Insider Threat – Regulations

Privacy+ Security Forum

FFIEC

Management Booklet - Risk Measurement

"common types of risks that often have significant impact: …

- Insider events: Including *intentional or unintentional acts* by staff, such as carelessness, social engineering that results in **inappropriate access** or the installation of malware, and **improper changes** to transactions, systems, or databases."

SEC

Final Cybersecurity Rule for Public Issuers

"retaining 'unauthorized' in the incident definition as proposed. In general, we believe that an ***accidental* occurrence is an unauthorized occurrence**. Therefore, we note that an accidental occurrence may be a cybersecurity incident under our definition, even if there is ***no* confirmed malicious activity**. For example, if a company's *customer data are accidentally exposed*, allowing unauthorized access to such data, the data breach would constitute a 'cybersecurity incident' that would necessitate a materiality analysis to determine whether disclosure under Item 1.05 of Form 8-K is required."

NY DFS

Cybersecurity Regulation (Second Amendment)

"penetration testing of their information systems from both inside and outside the information systems' boundaries" [NY CRR 500.5(a)(1)]

"The comment that it may be unnecessary to test an application when the **network itself undergoes penetration testing** assumes that the only purpose of penetration testing is to test against remote attacks, likely from an external source, and **ignores insider threats** or users who have *fallen victim to social engineering* and allowed an attacker access to their systems, where once on their system, **boundary and network-layer defenses are meaningless**."

Insider Threat – Regulations cont.

Executive Order 13587

National Insider Threat Policy & Minimum Standards

U.S. Government executive branch departments and agencies are to establish, implement, monitor, and report on insider threat programs

26 minimum standards encompassing:

- Designation of Senior Official
- Insider Threat Personnel
- Access to Information
- Monitor User Activity on Networks
- Information Integration Analysis, and Response
- Employee Training and Awareness

HIPAA

PCI DSS

SOX

GLBA

Insider Threat – Privacy Issues

Privacy+ Security Forum

GDPR

CCPA, etc.

Works Council

Others?

Internal Control - History

Privacy+ Security Forum

1906 Meat Inspection Act

- *The Jungle* (Upton Sinclair) exposed unsanitary conditions in Chicago meat packing industry
- Required systems of inspections similar to Pure Food and Drug Act passed on same day

1992 Statement on Auditing Standards (SAS) 70

- used by accountants to determine effectiveness of companies internal financial controls
- became primary method to audit companies information security for financial systems

2002 Sarbanes-Oxley Act (SOX)

- Enron, WorldCom, and Tyco led to loss of hundreds of billions of dollars in market value
- root causes uncovered in management oversight, auditor independence, and corporate governance

2005 ISO 27001 - Information Security Management Systems

- emphasizes use of internal controls for managing information security risks
- structured framework for monitoring and improving (governing) internal controls

Insider Threat MERIT Models (US-CERT)

3 main types

Insider IT Sabotage

- Disgruntlement and unmet expectations
- Behavioral precursors
- Stressful events
- Technical precursors and access paths
- The Trust Trap

Insider Theft of IP

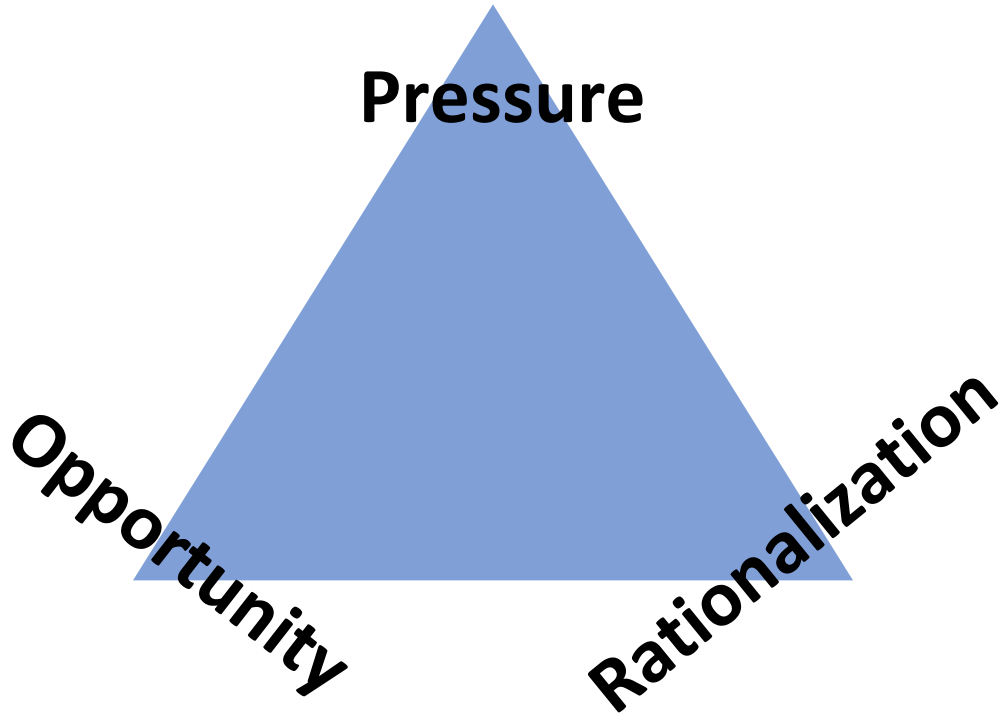
- The Entitled Independent
- The Ambitious Leader
- Influence of foreign governments or organizations

Insider Fraud

- The Fraud Triangle
- Continuing the fraud
- Outsider Facilitation
- Recruiting others
- Insider stressors
- Fraud involving Organized Crime

The Fraud Triangle

Donald Cressey's analysis of bank embezzlers



Research at Any Cost

Privacy+ Security Forum

Biopharma Company

- Initial Lead: Infosec team
- Time span of activity: 18 months
- Length of Investigation: 4 months
- Researcher found with proprietary research data on personal system
- Investigation identifies use of 3rd-party messaging and personal cloud storage
- Forensic investigation recovers chat snippets, inventory of historical files exchanged and some actual files
- Mandiant partner that specializes in HUMINT identifies multiple connections with nation state
- Takeaway: Restrict file sharing and communication methods to company accounts and platforms, enhance EDR

Watching the Watchers

Privacy+ Security Forum

Financial Services Company

- Initial Lead: Infosec Team
- Time span of activity: TBD
- Length of Investigation: Ongoing
- Information security head concerned w/abuse of administrator permissions
- HUGE SIEM data lake to support investigation of unjustified mailbox and file repository access of
- Takeaway: Prune administrator permissions, configure additional alerts, expand and audit just-in-time access

Creepy Co-worker

Privacy+ Security Forum

Services Company

- Initial Lead: Alert in company's EDR
- Time span of activity: at least 7 months
- Length of Investigation: 90 days
- Developer social engineered co-worker to provide work credentials
- Developer created SSH key to facilitate persistent remote access to co-worker company laptop
- Developer installed spyware, including camware and iPhone data, to ship data to cloud storage
- Takeaway: enhance EDR alerts, deploy just-in-time privileges

Disgruntled Departure

Privacy+ Security Forum

Manufacturing Company

- Initial Lead: Public article
- Time span of activity: TBD
- Length of Investigation: Ongoing
- Disgruntled employee finds and accesses confidential company information to share with journalist
- Company's logging captured employee activities
- Takeaway: Enhance detection and prevention methods via user analytics behavior alerts, enhance daily auditing of key repository access permissions for changes and/or stale permissions

No, Really, Please Leave

Privacy+ Security Forum

Insurance Company

- Initial Lead: EDR
- Time span of activity: 6 hours
- Length of Investigation: 30 days
- Recently let go employee remoted back into company system via private SSH key and remote access control list (ACL) on home network
- Takeaway: restrict SSH permissions, enhance EDR alerting and controls, enhance hardware decommission and return processes

Insider Threats

Practical Advice

- Know Thyself
  - Asset Inventory MUST be a core competency
  - Do you know where the Crown Jewels are stored? Can they be copied?
- It Didn’t Happen if it Didn’t Get Logged
  - Alerts are nice, but raw logs are better
  - See Know Thyself
- Most Incidents are NOT an Insider
  - But many customers gravitate to that explanation
- Just in Time Access
  - Least privilege
- Segregation of Duties and the Network
  - Limit the blast radius
- Required Role Rotations and Sharing
  - Enhance human visibility
  - Limit single points of failure
- Formalize and Audit Offboarding
  - Ensure processes account for accounts, hardware, activity and data audit analysis

Stages of Breach Denial

4 stages

Denial

- The TA claim is unwarranted
- Someone else got compromised

Insider

- It had to be an insider
- Only someone with insider knowledge could have moved so fully so quickly

Sophistication

- Our defenses are only penetrable against the most sophisticated nation states
- Only a 0-day that no one could have detected would have led to the breach

Anger

- Who did this to us and where do they live?

References

- National Insider Threat Task Force (NITTF)
  - https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-nittf
- Digital Asset Insider Trading
  - https://www.justice.gov/usao-sdny/pr/former-employee-nft-marketplace-charged-first-ever-
    asset-insider-trading-scheme
- Mandiant M-Trends 2020 Report – Threat From Within
  - http://www.mandiant.com/sites/default/files/2021-09/mtrends-2020.pdf
- Crown Jewels:
  - https://www.mandiant.com/resources/datasheets/consulting-services-crown-jewels-security-
    assessment-critical-information-asset-protection
- Insider Threat Program Development:
  - https://www.mandiant.com/services/insider-threat-assessment
- The CERT Guide to Insider Threats
  - https://www.amazon.com/CERT-Guide-Insider-Threats-Information/dp/0321812573
- National Insider Threat Policy
  - https://www.dni.gov/files/NCSC/documents/nittf/National_Insider_Threat_Policy.pdf

Speakers

Mike Lombardi

Director
Mandiant

David Payne

Associate General Counsel
Coinbase

Khizar Sheikh

Vice President
American Express

Cody Wamsley

Partner
Sterlington