Managing insider threat through the lens of a seasoned investigator

19 January 2017
Today’s speakers

Moderator:
► Kevin Jacobsen, Executive Director, Ernst & Young LLP, US

Speakers:
► Lou Bladel, Executive Director, Ernst & Young LLP, US
► Luke Dembosky, Partner, Debevoise & Plimpton LLP
► Douglas Thomas, Director, Counterintelligence Operations & Corporate Investigations, Lockheed Martin
Agenda

► Summary from last insider threat webcast
► Case studies from public and private sectors
► Lessons learned from Lockheed Martin
► Legal considerations in developing insider threat programs
Attendee polling question #1

What does your company see as the biggest impediment to implementing an insider threat program?

1. Lack of C-suite support
2. Lack of understanding of this threat
3. No dedicated insider threat analysts/investigators
4. Lack of clear policies that define data protection
5. Lack of funding and resources
6. Cultural barriers to implementation
7. Others
Case studies from public and private sectors
Kun Shan “Joey” Chun
Chronological events

- Born in Guandong, China, in 1969; naturalized American citizen in 1985
- 1997: Hired as an FBI electronics technician
- 1998: Granted a top secret clearance with access to classified information of FBI and other government agencies
- 2006: Recruited by the Chinese Ministry of State Security (MSS) and became a consultant to a Chinese Company in exchange for financial benefits
- 2014: FBI became aware of Kun Shan Chun’s activities. Chun attempted to recruit a FBI undercover employee (UCE) on behalf of the Chinese MSS and expressed to UCE desire to pass USG information to the Chinese Government. The FBI used Foreign Intelligence Surveillance Act coverage of over 40 facilities.
- March 2016: Arrested and charged in SDNY with violation of Title 18 USC:
  - § Sec. 1001(a)(1)(2)(3) — Making materially false, fictitious, or fraudulent statements
  - § Sec. 951(a) — Acting as an agent of a foreign power
- August 2016: Pleaded guilty to § Sec. 951(a)
Kun Shan “Joey” Chun
Key takeaways

- FBI didn’t have formalized training of insider threat protocols pushed out to the operational divisions (FBI instituted new insider threat protocols in Spring 2014).
- Chun’s immediate supervisors failed to recognize unusual travel patterns and irregularities in spending patterns.
Edward Snowden
Chronological events

- Born in 1983; high school dropout
- 2004: Enlisted in US Army Reserve as special forces recruit in May; discharged without completing training by September
- 2005: Hired by NSA as a security guard
- 2006: Hired by CIA as an IT system administrator
- 2009: Hired by Dell as an NSA subcontractor
- April 2013: Hired by BAH as a senior consultant and became a system administrator at an NSA facility in Hawaii
- Jan – May 2013: Initiated a number of contacts with the media using alias “Verax” and encrypted communications (e.g., filmmaker, Laura Poitras, Glenn Greenwald @the Guardian, Barton Gellman @the Washington Post). Arrived in Hawaii in May.
- June 1, 2013: Greenwald and Poitras interviewed Snowdon in Hong Kong
- June 5 - 9, 2013: First story published UK Guardian; Snowden voluntarily revealed his identity in UK Guardian
- June 14, 2013: Charged in EDVA with violation of Title 18 USC:
  - § 793(d) — Unauthorized disclosure of national security information
  - § 798(a)(3) — Unauthorized disclosure of classified communication intelligence
  - Sect. 641 — Theft of government property
- June 15 - 23, 2013: Provisional arrest request made to HKSAR authorities; Snowden’s US passport revoked; Snowden departed Hong Kong for Moscow
- August 1, 2013: Snowden granted political asylum in Russia for one year.
- January, 2014: Russia announced that Snowden can stay in country “indefinitely”
Edward Snowden
Key takeaways

- Considered in 2013 to be the “security gold standard” failed
- Perfect storm of arrogance, lack of understanding of vulnerabilities, unwillingness to question inappropriate activities
- Leadership did not take insider threat seriously
- Focused on perimeter security, failed to embrace repeatable, holistic program
Attendee polling question #2

How confident does your company feel relative to protecting your most sensitive business information, critical infrastructure, trade secrets or intellectual property?

A. Very confident
B. Somewhat confident
C. Not confident
D. Don’t know
DuPont investigation

Walter Liew
Naturalized US citizen
Owner and executive of USA Performance Tech Inc. (USAPTI)
Sentence: 15 years plus US$27m fine

Christina Liew
Naturalized US citizen
Owner/executive of USAPTI; wife of Walter Liew
Sentence: three years of probation plus US$6m fine

Robert Maegerle
US citizen
DuPont engineer (1956–991)
Sentence: 30 months plus US$375k fine

Tze Chao
Naturalized US citizen
Former DuPont scientist (1966–2002)
Sentence: 15 years
DuPont investigation key takeaways

- Inadequate understanding of the threat to its intellectual property
- Insufficient measures to secure trade secrets
- Limited pre-, post-employment checks, security protocols
- Failed to detect the breach in time
Attendee polling question #3

Which of the following describe the state of your organization’s insider threat incident response planning? (check all that apply)

A. We have a pre-established and well-tested plan.
B. We have a plan but hardly tested.
C. We have formed a core team that can be mobilized quickly.
D. We form a team when an investigation is needed.
E. We conduct tabletop exercises regularly with all stakeholders.
F. We conduct tabletop exercises randomly and with a focus group only.
G. None of the above.
Lessons learned from Lockheed Martin
Perspective change

- **Government**
  - Private industry, law firms, financial institutions, universities

- **Classified information**
  - Corporate proprietary information, intellectual property, pre-classified research

- **National security**
  - US technological edge, financial prosperity, brand preservation

- **Foreign nations**
  - Industry competition, self-interest
Increase in insider threat

- Employee financial hardships during economic downturns
- Employer affordability initiatives
  - Reduction of benefits and pension plans, lay-offs, etc.
- The global economic crisis
  - Foreign nations more eager to acquire new technologies and R&D results
  - Mergers, acquisitions, divestitures, joint ventures
- Ease of stealing anything stored electronically
- Increasing exposure to foreign intelligence entities (FIE) presented by the reality of global business, joint ventures, and the growing international footprint of American firms
- Office of Personnel Management (OPM) breach
# Insider threat detection program

## Planning
- Selling leadership
  - Shifting landscape
  - Trends
  - Cost considerations
  - Peer benchmarking

- Peer benchmarking
  - Challenges/successes
  - Population size
  - Privacy considerations
  - Program governance
  - Budget
  - Live analyst support

- Identify stakeholders
  - Legal, privacy, HR, communications, ethics, information security
  - CONOPs
  - Codification of policy
  - Communications plan

## Development
- Tool procurement/development
- Establish potential risk indicators
  - Determine appropriate weights and aging
- Identification of required data sets
  - Agreements with data owners

## Implementation
- Data ingestion and tool calibration
- Roll-out message to employees
  - Transparency in objective
  - Reinforcement of leadership support
  - Proper vehicles for voicing concerns
- Incident management
  - Conducting inquiries
  - Opening investigations
  - Coordination with law enforcement agencies

## Governance
- Steering committee
  - Security, legal, HR, ethics, information security
  - Receive quarterly briefings on results
  - Manage policy updates
- Corporate oversight
  - Internal audit
  - Risk and compliance committee
  - Board of directors
  - Government oversight
  - NISPOM
- Metrics
  - Tool analysis
  - Employee surveys
  - Red team

---

Managing insider threat through the lens of a seasoned investigator
Privacy and communications

- Properly introduce to employees — IMPERATIVE!
- Absolute transparency in purpose and objective
- Communication of adherence to corporate value structure
- Joint strategy development (HR, communications, PR)
- Proper adoption of local restrictions applicable to foreign and expatriated employees
- Access to automated tool heavily restricted
- “Red team” ensures the highest level of system defenses
- Continual coordination with the Privacy General Counsel
- No profiling
Insider threat program metrics

- Employee classified information (CI) training and awareness
- Receipt of threat information/implementation of mitigation
- Suspicious contact reports (SCR) generating government referrals or intelligence information reports (IIR)
- Name checks
- CI leads from insider threat tool
- CI cases/inquiries opened
- Cases referred to federal law enforcement
- Files recovered
- Case disposition
Lessons learned

- Organizational leadership buy-in NOT “won and done”!
- Long process; funding can be incremental
- Functional area partnerships key to program success
- Counterintelligence response team, security, HR, ethics, legal, communications
- Continual coordination with General Counsel
- Internal audit engagement
- Communications plan
- Suicide and workplace violence prevention
- Break down “business as usual” mindset
Primary takeaways

- Corporate proprietary information and intellectual property - hot targets!
- Reporting indicates steady upward trend in targeting
- Threat is real, formidable and aggressive
- Current business environment exposes us to more vulnerabilities
- Strong partnerships are key (internal and external)
- Automated analysis capability is essential for any large organization
- Data loss prevention tool ≠ insider threat detection capability
- Program transparency—mitigate concern, promote deterrence, garner program support
Legal considerations in developing insider threat programs
Some practical legal considerations

- Law enforcement requests to allow the conduct to continue (weighing liability and reputational concerns)
- System monitoring considerations
- Addressing the employee’s own devices
- Issues related to remote access
- Disclosure considerations where data is lost
- Legal challenges involving an employee who exceeds authorized system access
Key steps for building an insider threat program

- Gain senior leadership endorsement, develop policies that have buy-in from key stakeholders and take into account organizational culture
- Develop repeatable processes to achieve consistency in how insider threats are monitored and mitigated
- Use analytics to strengthen the program backbone, but remember implementing an analytical platform does not create an insider threat detection program in and of itself
- Coordinate with legal counsel early and often to address privacy, data, protection and cross-border data transfer concerns
- Screen employees and vendors regularly, especially personnel who hold high-risk positions or have access to critical assets
- Implement clearly defined consequence management processes so that all incidents are handled following consistent standards, involving the right stakeholders
- Create training curriculum to generate awareness about insider threats and their related risks
- Leverage information security and corporate security programs, coupled with information governance, to identify and understand critical assets
Attendee polling question #4

What functions are involved in addressing insider threats in your organization? (check all that apply)

A. IT
B. Information security
C. Legal counsel
D. Investigations
E. Human resources
F. Business unit leaders
G. All of the above
H. Other functions not listed above
A brief introduction to managing insider threat

https://www.youtube.com/watch?v=OTix30TvjU&feature=youtu.be
Questions and answers

Join us in upcoming webcasts:

- **Are regulators and litigants better at analytics than you?**
  Thursday, 16 February 2017 | 12:00 p.m.–1:00 p.m. Eastern Time

- **Effective document review: real-world success stories**
  Friday, 17 March 2017 | 12:00 p.m.–1:00 p.m. Eastern Time

- **Cybersecurity in eDiscovery**
  Tuesday, 25 April 2017 | 12:00 p.m.–1:00 p.m. Eastern Time
About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

About EY’s Fraud Investigation & Dispute Services
Dealing with complex issues of fraud, regulatory compliance and business disputes can detract from efforts to succeed. Better management of fraud risk and compliance exposure is a critical business priority — no matter the size or industry sector. With over 4,500 fraud investigation and dispute professionals around the world, we will assemble the right multidisciplinary and culturally aligned team to work with you and your legal advisors. We work to give you the benefit of our broad sector experience, our deep subject-matter knowledge and the latest insights from our work worldwide.

© 2017 EYGM Limited.
All Rights Reserved.

1701-2161236
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com