EY Fraud Investigation & Dispute Services
Legal, Compliance and Technology Webcast Series

Managing insider threat: a holistic approach to managing risk from within

13 June 2016
Today’s speakers

Moderator:
Mike Janosov, Senior Manager, Ernst & Young LLP, US

Speakers:
Rowena Fell, Director, Ernst & Young LLP, UK
Paul Alvarez, Senior Manager, Ernst & Young LLP, US
56%

Of respondents say that employees are the most likely sources of an attack

– 2015 EY Global Information Security Survey
Overview

The Centre for the Protection of National Infrastructure, the UK Government security authority for infrastructure protection, has identified the following five main types of insider activity:

► Unauthorized disclosure of sensitive information
► Process corruption
► Facilitation of third-party access to an organization’s assets
► Physical sabotage
► Electronic or IT sabotage

The most frequent types of insider activity identified were unauthorized disclosure of sensitive information (47%) and process corruption (42%).
Overview

Available demographic information findings include:

- Significantly more males engage in insider activity (82%) than females (18%)
- 49% of insider cases occur within the 31–45 years age category
- The majority of insider acts are carried out by permanent staff (88%)
- The duration of the insider activity ranges from less than six months (41%) to more than five years (11%)
- The majority of insider cases are self-initiated (76%)
- It is common for insiders to have more than one motivation. Financial gain is the most common primary motivation (47%), followed by ideology (20%) and a desire for recognition (14%)
Overview

There is a clear link between an insider act taking place and exploitable weaknesses in an employer’s protective security and management processes:

► Inadequate management practices and inadequate corporate governance
► Insufficient use of auditing functions
► Lack of protective security controls and a poor security culture
► Poor pre-employment screening
► Poor communication between business areas
► Lack of awareness of people risk at a senior level
Insider threat

- An insider is a current or former employee, contractor or business partner who:
  - Has or had authorized access to an organization’s buildings, network system or data
  - Has intentionally used that access to compromise the confidentiality, integrity or availability of the organization’s data or information systems
- Insider threat is defined to include activities that result in fraud, trade secret compromise, intellectual property (IP) theft, unauthorized trading, espionage or information technology sabotage.
“89% of respondents say that they feel at least somewhat vulnerable to insider attacks. 34% felt extremely vulnerable.”

– 2015 Vormetric Insider Threat Report
Attendee polling question

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

A. Lack of C-suite support
B. Lack of understanding of this threat
C. No dedicated insider threat analysts/investigators
D. Lack of funding and resources
E. Cultural barriers to implementation
F. Other
EY’s insider threat program framework

- Assess business continuity and resiliency
- Evaluate and incorporate lessons learned
- Review KPIs and assess effectiveness
- Assist with remediation and law enforcement notification/actions

- Identify stakeholders and create governance
- Assess and scope program
- Inventory and map high-value assets
- Review historical-use cases
- Highlight privacy/legal concerns

- Set policies and procedures
- Establish awareness and training
- Evaluate access controls
- Enhance employee screening
- Formulate key performance indicators (KPIs)

- Establish playbook/response plans
- Proactively monitor using behavioral analytics
- Leverage technical and non-technical data
- Review employee reporting of insider activity

Recover Prepare Respond Protect Detect

Continuous evaluation

Full spectrum approach

- Execute response playbook
- Ensure notification and escalation protocols
- Collect evidence for prosecution
- Mitigate damage and contain the threat
EY insider threat maturity model

Initial
► Processes or functions are ad hoc and siloed
► Lacking defined roles and responsibilities
► Activities are largely reactive in nature with minimal to no formal prevention strategy

Repeatable
► Leveraging existing security processes or functions to prevent insider threat, no formal insider threat program
► No formalized training for employees or vendors
► Procedure communication strategies underdeveloped

Defined
► Formal insider threat program exists with dedicated policies and processes that align with and leverage existing information security and corporate security programs
► Defined insider threat detection strategy
► Incident response plans incorporate insider threat event handling
► Formal consequence management procedures are in place
► Defined program governance with buy-in by key stakeholders
► Dedicated insider threat resources
► Developed training curriculum for employees and vendors
► Lack of full understanding of the organization’s critical assets

Managed
► Key performance indicators are in place to perform routine assessment of program effectiveness
► An interactive approach that provides continuous improvement
► Strong information governance disciplines underpinning the insider threat program
► Some risk indicators are developed to monitor the critical assets
► Leveraging data analytics technologies such as behavior analytics to identify hidden relationships and motives

Optimizing
► Insider threat program is fully integrated into the enterprise risk management strategy
► Increased focus on proactively defending and responding to insider threat
► Big data infrastructure that provides access to and integration of all required data sources across the organization
► Expanded suite of risk indicators leveraging the big data platform, advanced data analytics technologies and organizational context (non-technical)
### Sample activities to start an insider threat program

#### Plan and collect
- Identify program owner and key stakeholders
- Gather current security-related policies and procedures
- Catalog past incidents within the organization to drive use case development
- Identify relevant legal and regulatory issues
- Obtain consequence protocols and procedures
- Inventory existing monitoring tools and processes, including analytics technologies and models

#### Review and analyze
- Evaluate the effectiveness of existing relevant policies and processes
- Examine corporate hiring and screening procedures
- Determine the foundational requirements and scope for each component of the program (e.g., internal communication, training, employee and vendor screening, consequence management)
- Identify and understand “crown jewels” and their related risks
- Understand the privacy and cultural considerations that may impact the adoption of an insider threat program
- Evaluate the existing monitoring capability, including user behavior analytics models

#### Develop strategic framework
- Formalize program objectives and obtain buy-in by key stakeholders
- Create insider threat detection framework and high-level process flows
- Formulate program implementation road map
- Define program resource requirements (e.g., roles, skill sets)
- Design an enterprise communication and training plan that includes all affected employees and third parties
- Understand the inner relationships between all relevant policies and processes and develop integration plans
- Develop or refine behavior analytics models based on defined insider threat detection strategy
Attendee polling question

What maturity level do you think your insider threat program is at today?
A. Initial
B. Repeatable
C. Defined
D. Managed
E. Optimizing
F. Don’t know
What are critical digital assets?

Digital assets = Data (in files) + Context (in the form of metadata)


- Critical digital assets (CDAs) are:
  - Essential and priority files that represent high value to the business in terms of revenue generation, business operations or regulations
  - Typically segmented as corporate confidential or regulated data sets
    - Corporate confidential: IP, trade secrets, business strategies, legal, contracts, etc.
    - Regulated: credit card information, personal health information, personally identifiable information, etc.
  - “Massive incident of data fraud/theft” is viewed as one of the top four technological risks according to the World Economic Forum’s *The Global Risks Report 2016.*
  - CDAs vary by industry and by organization.

Source: 2015 EY Global Information Security Survey

- 56% of respondents viewed data leakage/data loss prevention as a high priority for their organization over the next 12 month.
- 42% of respondents say that knowing all their assets is a key information security challenge.
Identifying, inventorying and valuing CDAs

► What is valuable?
  ► Information security
    ► Classification
    ► Access
      ► Screening/vetting
  ► Inventoried
    ► Key terms (data loss prevention)
  ► Risk if lost, compromised
    ► Reputational risk
    ► Financial risk
Locating your CDA

► Where does this data reside?
  ► Within your organization’s firewall?
  ► Third parties?
  ► Cloud?
  ► External devices?
  ► Staff personal computers?
Protecting your CDAs

► What data needs protection?
► What tools exist within your organization?
► Does it fit into your future state strategy and is it compatible with other tools?
► How can analytics be applied to provide you with ongoing information about your crown jewels?
Attendee polling question

How confident does your company feel relative to knowing where your “crown jewels” are within the company?

A. Very confident
B. Somewhat confident
C. Not confident
D. Don’t know
The amount of time, on average, to resolve attacks from malicious insiders – 54.4 days

– Ponemon Institute 2015 Cost of Cyber Crime Study
Insider threat indicators and actions

Motivations

► Termination
► Passed over for promotion
► Financial issues
► Legal issues
► Psychological issues
► New job
► Beliefs

Activities

► Economic espionage (e.g., contact with state-sponsored actor)
► Industrial espionage (e.g., contact with competitor)
► IT sabotage
► Data theft

Indicators

► Removable storage use
► Cloud storage uploads
► Working odd hours/ removing data
► Email to external agent or personal email account
► Excessive printing
► Requesting access to previously denied areas/systems
Prioritizing behavior by analyzing raw data

Raw data

- Terabytes of event data collected daily
- At a rate of thousands events per second
- Across thousands of assets and users

Consolidate

- File transfers
- Website usage
- Cloud usage
- Network share accesses
- Software installations
- Usage patterns

Prioritize

- Remote account takeover
- Destructive activity
- Malicious communications
- Data theft
- Backdoor deployment

Discover and identify malicious behavior
Creating a risk-ranking score system

01 Anomaly detection through machine learning

02 Linguistic analysis

03 Assessment of non-technical indicators

04 Risk ranking
Attendee polling question

How confident does your company feel relative to proactively detecting insider threats?

A. Very confident
B. Somewhat confident
C. Not confident
D. Don’t know
Seven key steps for building an insider threat program

1. Gain senior leadership endorsement; develop policies that have buy-in from key stakeholders and take into account organizational culture

2. Develop repeatable processes to achieve consistency in how insider threat is monitored and mitigated

3. Leverage information security and corporate security programs, coupled with information governance, to identify and understand critical assets

4. 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

5. Coordinate with legal counsel early and often to address privacy, data protection and cross-border data transfer concerns

6. Conduct employee and vendor screening on a recurring basis, especially for personnel who hold high-risk positions or have access to critical assets

7. Implement clearly defined consequence management processes so that all incidents are handled following uniform standards, involving the right stakeholders

8. Create training curriculum to generate awareness about insider threat and its related risks
Attendee polling question

What do you think is the most likely step your company will take with respect to insider threats within the next 6–12 months?

A. Solidify senior leadership support
B. Create or finalize program governance
C. Implement behavioral analytics or other detection systems
D. Enhance training/awareness programs
E. Develop robust consequence management
F. Implement robust employee risk screening efforts
G. Don’t know
Questions and answers
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 industry sector. With our more than 4,200 fraud investigation and dispute professionals around the world, we 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.

© 2016 EYGM Limited
All Rights Reserved.

1605-1955470
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