Managing the risk of insider threats and cyber attacks

April 28, 2017
Agenda

► Insider threat: definition and risk impact
► Key considerations of an insider threat program
► Prepare and protect with information governance
► What is a critical digital asset?
► Seven key steps for building an insider threat program
► Questions
What is insider threat?

A malicious insider is a current or former employee, contractor or business partner who:

- Has or had authorized access to an organization’s 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 fraud, intellectual property (IP) theft, unauthorized trading, espionage or information technology sabotage
The impact of insider threat

56% say that employees are most likely sources of an attack

Source: 2015 EY Global Information Security Survey

The most expensive type of attack comes from malicious insiders with the highest average annualized cost of $144,542, weighted by attack frequency.

It takes the most amount of time, on average, to resolve attacks from malicious insiders – 54.4 days.

Source: Ponemon Institute 2015 Cost of Cyber Crime Study

32% believe the level of cyber breach and insider threat risk has significantly increased

60% rate cyber breach and insider threat as the key drivers in Forensic Data Analytics (FDA) investment

Source: 2016 EY Global Forensic Data Analytics Survey
Types of insider

Negligent:
These employees may accidentally delete or modify critical information or unwittingly share sensitive information. Negligent behaviour can come in the form of sending confidential data to the wrong party or posting proprietary information on social media sites.

Malicious:
These insiders deliberately cause harm by stealing critical firm data for profit, personal benefit or revenge. They cause harm through sabotage, espionage, subversion or terrorism.

Compromised Actors:
Insiders who have legitimate access to systems, networks, and data but who are acting in accordance with, or under the influence of, an external threat actor. This can include hostile states, organisations, criminals or corporate entities.
## Insider threat indicators and actions

### Motivations
- Termination
- Passed over for promotion
- Financial issues
- Legal issues
- Psychological issues

### Activities
- Economic espionage
  - Contact with state-sponsored actor
- Industrial espionage
  - Contact with competitor
- IT sabotage

### Targets
- Removable storage
- Cloud storage
- Working odd hours/removing data
- Email to external agent or personal email account
Insider threat industry examples

► An engineer was charged with stealing trade secrets belonging to two former employers, both of which develop and manufacture medical devices used to treat cardiac and vascular ailments.

► Scientists working at a US research facility engaged in a scheme to steal trade secrets related to research data, procedures, and manufacturing processes for biopharmaceutical products.
So, there’s a problem…

What’s the solution?
Start an insider threat management program! For example...

<table>
<thead>
<tr>
<th>Key activities</th>
<th>Plan and collect</th>
<th>Review and analyze</th>
<th>Develop strategic framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>► Identify program owner and key stakeholders</td>
<td>► Evaluate the effectiveness of existing relevant policies and processes</td>
<td>► Formalize program objectives and obtain buy-in by key stakeholders</td>
<td></td>
</tr>
<tr>
<td>► Gather current security related policies and procedures</td>
<td>► Examine corporate hiring and screening procedures</td>
<td>► Create insider threat detection framework and high-level process flows</td>
<td></td>
</tr>
<tr>
<td>► Catalogue past incidents within the organization to drive use case development</td>
<td>► Determine the foundational requirements scope for each component of the program (e.g., internal communication, training, employee and vendor screening, consequence management)</td>
<td>► Formulate program implementation roadmap</td>
<td></td>
</tr>
<tr>
<td>► Identify relevant legal and regulatory issues</td>
<td>► Identify and understand “crown jewels” and their related risks</td>
<td>► Define program resource requirements (e.g., roles, skill sets)</td>
<td></td>
</tr>
<tr>
<td>► Obtain consequence protocols and procedures</td>
<td>► Understand the privacy and cultural considerations that may impact the adoption of insider threat program</td>
<td>► Design an enterprise communication and training plan that include all affected employees and third parties</td>
<td></td>
</tr>
<tr>
<td>► Inventory existing monitoring tools and processes, including analytics technologies and models</td>
<td>► Evaluate the existing monitoring capability including user behavior analytics models</td>
<td>► Understand the inner relationships between all relevant policies and processes and develop integration plans</td>
<td></td>
</tr>
<tr>
<td>► Evaluate the effectiveness of existing relevant policies and processes</td>
<td>► Develop or refine behavior analytics models based on defined insider threat detection strategy</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
EY’s insider threat program framework

- Assess business continuity and resiliency
- Evaluate and incorporate lessons learned
- Review KPI 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 (IP)
- Review historical-use cases
- Highlight privacy/legal concerns

- Set policies and procedures
- Establish awareness and training
- Evaluate access controls
- Enhance employee screening
- Formulate key measures (KPI)

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

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

- Full spectrum approach
- Continuous evaluation
- Recover
- Prepare
- Protect
- Respond
- Detect
Information governance is critical to manage and protect Critical Digital Assets (CDA)

EY’s information governance principles

1. Adopt a risk-based approach
2. Identify physical locations of your CDA
3. Advocate user access management hygiene
4. Establish business rules of CDA management
What are critical digital assets (CDAs)?

Digital assets = data (in files) + context (in the form of metadata)


- CDAs are:
  - Essential and priority files that represent high value to the business in terms of business operations or regulations
  - Typically segmented as corporate confidential or regulated data sets
    - Corporate confidential: IP, business strategies, legal, contracts, etc.
    - Regulated: credit card information (CCI), personal health information (PHI), personally identifiable information (PII), 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

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

Source: 2015 EY Global Information Security Survey
Behavioral access outlier analysis can proactively detect insider threats
### Data sources and risk indicators

<table>
<thead>
<tr>
<th>Priority</th>
<th>Data source</th>
<th>Indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HR (HRMS/SaaS)</strong></td>
<td>Terminations, layoffs, performance issues</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Criminal records (employee screening)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Financial issues (credit check)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Legal issues (employee screening)</td>
<td></td>
</tr>
<tr>
<td><strong>Email (Exchange logs, email headers, content)</strong></td>
<td>Contact with state-sponsored actors, competitors, attachments sent to personal accounts</td>
<td></td>
</tr>
<tr>
<td><strong>Data Loss Prevention logs</strong></td>
<td>Alerts for movement of data containing proprietary markings, sensitive materials, PII</td>
<td></td>
</tr>
<tr>
<td><strong>Travel data (vendor)</strong></td>
<td>Travel to countries known for IP theft, or hosting competitors</td>
<td></td>
</tr>
<tr>
<td><strong>Corporate credit card (vendor)</strong></td>
<td>Credit card activity</td>
<td></td>
</tr>
<tr>
<td><strong>Network logs (proxy, internal servers, SharePoint, etc.)</strong></td>
<td>Suspicious activity</td>
<td></td>
</tr>
<tr>
<td><strong>Security data (endpoint monitoring, anti-virus, SIEM alerts, etc.)</strong></td>
<td>Data hoarding, copying from internal sites/repositories, removable device usage</td>
<td></td>
</tr>
<tr>
<td><strong>Phone logs (VoIP, vendor)</strong></td>
<td>Calls to/from countries known for IP theft or hosting competitor</td>
<td></td>
</tr>
<tr>
<td><strong>Open source data (LinkedIn, Twitter, Facebook, etc.)</strong></td>
<td>Leaks via social networking, indications of employee leaving to competitor</td>
<td></td>
</tr>
<tr>
<td><strong>Employee HR/ethics hotline</strong></td>
<td>Complaints of hostile, abnormal or illegal behavior, living beyond means</td>
<td></td>
</tr>
<tr>
<td><strong>Full packet captures</strong></td>
<td>Suspicious activity</td>
<td></td>
</tr>
<tr>
<td><strong>Badge access logs</strong></td>
<td>Accessing areas at odd hours, accessing restricted areas</td>
<td></td>
</tr>
</tbody>
</table>
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
- Lateral movement and recon

**Discover and identify malicious behavior**
Insider threat program industry perspectives: Summary trends

- EY surveyed 10 Fortune 500 companies from the following sectors:
  - Finance
  - Manufacturing
  - Media and Entertainment
  - Technology
  - Defense

- 9 of 10 of survey participants have a formal Insider Threat Program
- 8 of the Insider Threat Programs have a core team model
  - Core team: A defined team focused on implementing and maintaining the organization’s Insider Threat Program.
- 5 of the 10 Insider Threat Programs report to the Chief Information Security Officer (CISO)

- Insider Threat Program objectives focus on: threats posed by rogue IT employees, departing employees, theft of intellectual property, and theft of PII.

- A majority of organizations have Data Protection Programs with supporting Data Loss Prevention (DLP), User Behavior Analytics (UBA), and other enterprise security technologies.
Seven key steps for building an insider threat program

1. Gain senior leadership support and participation.
2. Develop policies that integrate key stakeholders and provide repeatable processes.
3. Adopt a phased approach for data access/ingestion.
4. Use analytics as its backbone. Implementing an analytical platform that does not create an insider threat detection program in and of itself.
5. Coordinate with Legal to address privacy and cross-border concerns.
6. Evaluate employee and vendor screening and consequence management processes.
7. Create training programs that develop awareness.
Questions?
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.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

© 2017 Ernst & Young LLP.
All Rights Reserved.

1606-1957692
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