Managing insider threat

A holistic approach to dealing with risk from within

EY
Building a better working world

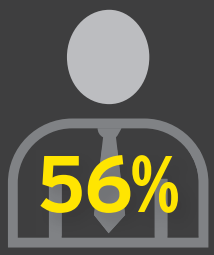
How safe are your critical assets?

An organization's critical digital and physical assets are becoming more and more exposed through increased connectivity, differing global regulatory requirements, joint ventures and business alliances, and potential security weaknesses within complex multinational supply chains.

What is insider threat?

An insider threat is when a current or former employee, contractor or business partner, who has or had authorized access to an organization's network systems, data or premises, uses that access to compromise the confidentiality, integrity or availability of the organization's network systems, data or premises, whether or not out of malicious intent. Insider threats can include fraud, theft of intellectual property (IP) or trade secrets, unauthorized trading, espionage and IT infrastructure sabotage.

56% of respondents view data leakage/data loss prevention as a high priority for their organizations over the next 12 months.



56% of respondents view employees as the second most likely source of an attack, closely following criminal syndicates (59%).

42% of respondents say that knowing all their assets is a key information security challenge.

Source: EY's Global Information Security Survey 2015

The financial, reputational and regulatory impact of having an organization's critical assets stolen or damaged can be catastrophic. Anyone with trusted access can exploit the vulnerabilities that protect critical assets, causing millions of dollars of damage. In order to mitigate this risk, organizations should establish a program to protect their critical assets from insider threats. Depending on the organizational culture, this program could be defined as the "insider threat program" or, instead, be aligned with data – for example, the "intellectual property and trade secrets protection program." For ease of discussion, we will be using "insider threat program" for the rest of the document.

Insider threats can originate from lack of awareness. For example, employees creating workarounds to technology challenges or using their own personal devices (i.e., bring your own device – BYOD) to access work emails can create new vulnerabilities within an organization's physical security processes and IT systems. This document considers insider threats stemming from intentional fraudulent or criminal activities. To combat this insidious type of threat, organizations need a holistic response.

Although technology can play an important role in identifying potential insider threats, it is not just an IT issue. It takes an enterprise-wide approach – including many human elements – to plan for, prevent, detect, respond to and recover from insider threats. Managing insider threat risk should be part of a holistic corporate security program, from both information security and physical security perspectives. However, there are unique information security challenges that must be addressed. These challenges lie in the fact that the threats created by insiders are hidden in plain sight and are therefore difficult to detect. For example, they:

- Do not need to "break in" because they already have access and knowledge pertaining to the location of critical assets
- Are within an organization's confines, so their illicit activities are harder to detect via traditional signature-based detection than an external attacker

Identify the indicators that reveal insiders at work

Insider attacks may demonstrate characteristics of an external attack; they also may leave unique digital footprints that are identifiable risk indicators.

An insider threat may be present or developing over a period of time with indications that can be categorized as "direct" or "indirect," each requiring different types of tracking mechanisms. "Direct" risk indicators are usually abnormal activities that deviate from day-to-day work activities. Examples include downloading large volumes of data to external drives, accessing sensitive information that bears no direct relevance to normal job duties or emailing confidential data to a personal account. "Indirect" risk indicators are usually patterns of human behavior that require analysis to reveal suspicious motives. Examples include sudden overuse of negative emotive words in electronic communications, expressing desire to resign over social media, and demonstrating ties to high-risk personnel or outside parties.

Other common insider threat indicators include:

- Attempts to bypass security controls
- Requests for clearance or higher-level access without need
- Frequent access of workspace outside of normal working hours
- Irresponsible social media habits
- Behaviors that demonstrate sudden affluence without obvious cause, such as large pay raise, inheritance, etc.
- Maintaining access to sensitive data after termination notice
- Use of unauthorized external storage devices
- Visible disgruntlement toward employer or coworkers
- Chronic violation of organization policies
- Decline in work performance

These red flags alone should not be viewed as demonstrations of harm; instead, they should invoke a process of review and clarification. The review process needs to amalgamate the risk indicators and analyze them collectively in order to uncover hidden relationships, which usually reveal more detail than when they are examined individually. To assess these risk indicators, organizations need to access both structured and unstructured data sources. Examples of data and risk pairs include:

Structured information:

- Travel and entertainment data: violation of corporate policies
- Network access data: web browsing history, network crawling, data hoarding, copying from internal repositories
- Physical facility access logs: anomalies in employee work hours, attempts to access restricted areas
- Travel records: countries known for IP theft or hosting competitors
- Phone logs: calls with known high-risk personnel or external parties

Unstructured information:

- Social media postings (public view only): indications of living beyond means, discussions of resigning or new business venture
- Emails/instant messages: malicious intent
- HR records: terminations, layoffs and performance issues
- Employee hotline logs: complaints of hostile, abnormal, unethical or illegal behaviors

Insider threat program maturity model

The starting point for an insider threat program is to determine the organization's ability to detect and mitigate insider threats and to develop a strategy that will both evolve with shifting risk priorities and grow to the level of desired maturity.

Software development has long used maturity models as a tool to objectively assess the degree of repeatability, consistency and effectiveness of certain activities or processes. Insider threat is not a new risk, but it is a relatively new practice for companies to implement a risk management program that specifically targets insider threats. To help companies develop an insider threat strategy that aligns with their risk profiles and growth priorities, EY developed an insider threat maturity model based on our experience in helping companies detect and mitigate insider threats.

Our maturity model consists of a set of characteristics that classify an organization's capabilities to detect insider threats and represent a progression in managing insider threat risk. The model reflects leading practices gleaned from both private and public sectors and incorporates relevant industry standards, such as the Cybersecurity Framework from National Institute of Standards and Technology. It provides a benchmark against which an organization can evaluate the capability of its insider threat program and set goals and priorities for improvement.

EY Insider Threat Maturity Model

Initial

Characteristics:

- Ad hoc or siloed processes or functions
- Lacks defined roles and responsibilities
- Largely reactive activities with minimal to no formal prevention strategy

Outcome:

- Higher risk of insider threat
- Delayed response in the event of an insider breach

Repeatable

Characteristics:

- Leverages existing security processes or functions to prevent insider threat, with no formal insider threat program
- No formalized training for employees or vendors
- Underdeveloped procedure communication strategies

Outcome:

- Limited detection capabilities
- Inconsistent ability to respond, depending on the nature of incident
- Inadequate consequence management procedures

Defined

Characteristics:

- Formal insider threat program 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 that incorporate insider threat event handling
- Formal consequence management procedures in place
- Defined program governance with buy-in by key stakeholders
- Dedicated insider threat resources
- Developed training curriculum for employees and vendors
- Lacks full understanding of the organization's critical assets

Outcome:

- Enterprise-wide awareness of insider threats
- Increased ability to detect insider threats through traditional information security technologies such as data loss protection, endpoint monitoring, etc.
- Operational efficiency realized through coordinated efforts by all stakeholders
- Consistency in how assets are monitored and protected
- Uniformity in how incidents are handled
- Some critical assets more exposed to insider threats than others

Managed

Characteristics:

- Key performance indicators in place to assess program effectiveness
- An iterative approach that provides continuous improvement
- Strong information governance disciplines underpinning the insider threat program
- Some risk indicators developed to monitor critical assets
- Leverages data analytics technologies, such as behavioral analytics, to identify hidden relationships and motives

Outcome:

- Comprehensive understanding of the organization's critical assets and their related risks
- Enhanced ability to monitor and mitigate insider threats
- Continuous improvement as the program evolves over time
- Captures previously missed signals predicting potential insider threats
- Measurable reduction in insider threat incidents

Optimizing

Characteristics:

- Insider threat program fully integrated into the enterprise risk management strategy
- Increased focus on proactively defending and responding to insider threats
- Big data infrastructure that provides access to and integrates all required data sources across the organization
- Expanded suite of risk indicators leveraging the big data platform, advanced data analytics technologies and organizational knowledge

Outcome:

- Significant decrease in insider threat incidents
- Extends benefits of the insider threat program into other business imperatives, such as risk management, compliance, internal controls and talent management
- Enhanced defensibility of the organization's internal controls and risk management capability
- Timely response to litigation and regulatory requests for data

A strong insider threat program is effective in preventing, detecting and mitigating insider threat.

EY's Insider Threat Program Framework

EY's Insider Threat Program Framework helps organizations develop an integrated risk management program to protect their critical assets against insider threats. It offers a data-driven approach to manage insider threat risk while taking advantage of the advanced analytical tools and information governance disciplines.

The framework leverages the work of the US and UK Computer Emergency Response Teams, the Intelligence and National Security Alliance, the National Institute of Standards and Technology, and the Center for the Protection of National Infrastructure. A global team of EY professionals, who possess extensive background and knowledge in counterespionage, forensic investigation, data sciences, information security and enterprise risk management, developed this framework. We created it with the assumption that the insider threat program should be fully integrated with the organization's existing corporate security and cybersecurity programs. Insider threat needs to be part of enterprise-wide risk management considerations, aligned with organizational risk priorities.

An insider threat program is far more than a technical program. Given the nature of insider threats, the human element is just as important as the technology. The human consideration needs to be embedded in every aspect of the insider threat program, from policymaking, monitoring and escalation procedures to consequence management.

There are eight steps to building a successful insider threat program

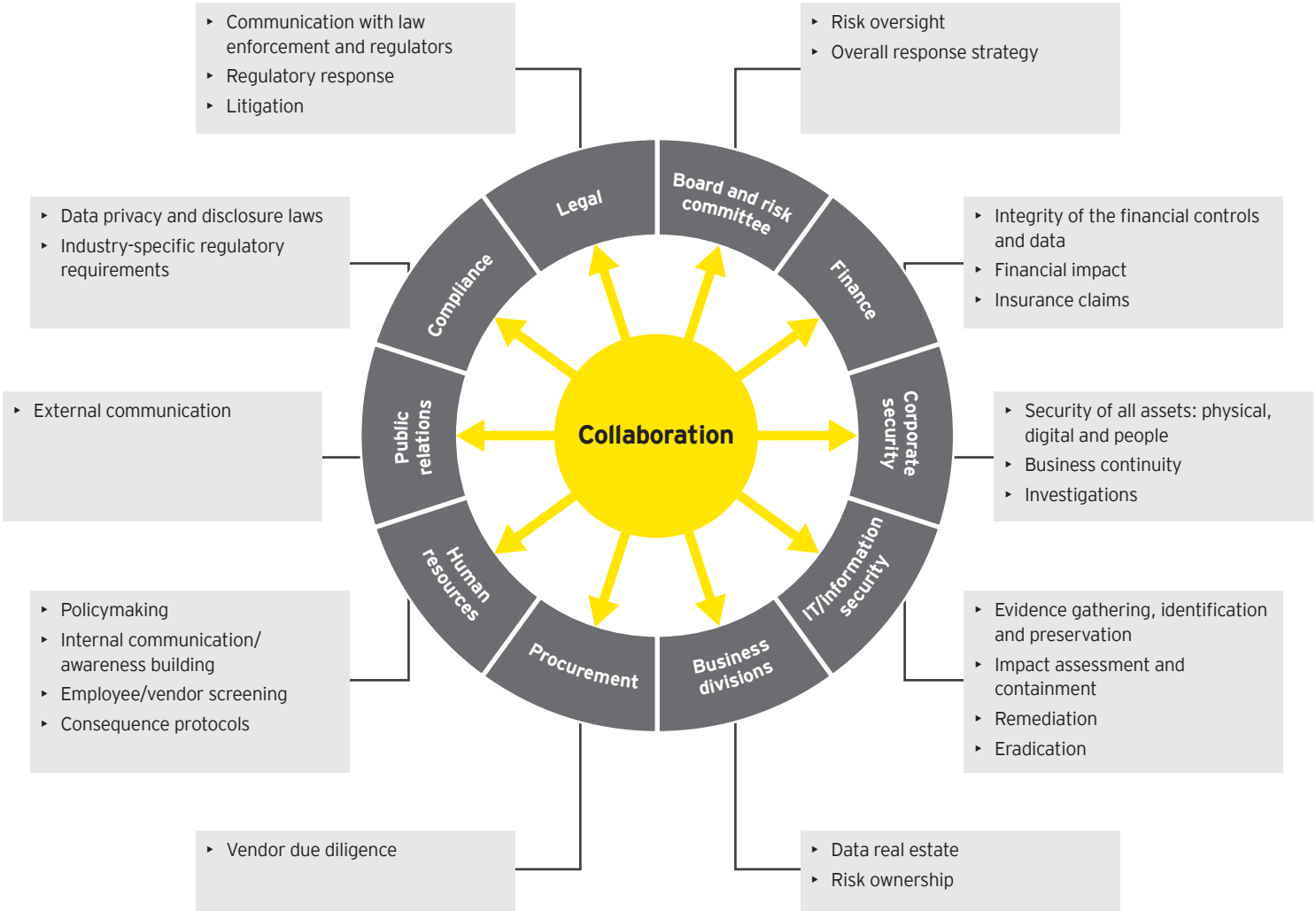
They are:

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 threats are 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. Screen employees and vendors regularly, especially 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 threats and their related risks

Prepare to develop an integrated insider threat program via cross-functional collaboration

When developing an insider threat program, organizations should start with a clearly defined governance model, through which stakeholders collaborate to identify critical assets, risk indicators, relevant data sources, compliance requirements, cultural concerns and privacy implications. The success of an insider threat program depends on the support and participation of its stakeholders. The stakeholders need to develop constructive working relationships to manage risk from within. Keys to success include clearly defined and easy-to-follow policies, succinct communication protocols, and rigorous training curriculums.

Collaboration is fundamental to success



In developing the insider threat program, we work closely with the organization's legal counsel to comply with industry- and geography- specific data protection and privacy regulations. We use technology to address data integrity, security and privacy concerns. For example, our professionals anonymize/encrypt data to protect privacy in transit and at rest without affecting our ability to analyze data. We also help organizations strike the right balance between privacy and security through communications about the insider threat risk and the objectives of their insider threat program. These communications require transparency in order for employees to understand the program objectives and overcome privacy and other cultural concerns, while leaving certain elements confidential to prevent malicious insiders from circumventing security controls.

Sample activities to start an insider threat program

	Plan and collect	Review and analyze	Develop strategic framework
Key activities	▸ Identify program owners 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	▸ Evaluate the effectiveness of existing relevant policies and processes ▸ Examine corporate hiring and screening procedures ▸ Determine the requirements and scope for each component of the program (e.g., internal communication, training, employee and vendor screening, consequence management) ▸ Identify and catalog "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 (UBA) models	▸ Formalize program objectives and obtain buy-in from 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 relationships between relevant policies and processes and develop integration plans ▸ Develop or refine behavioral analytics models based on defined insider threat detection strategy

Information governance is one of the key means used to protect data assets

Digitization has led to the arrival of big data and the explosion of new data assets that are becoming more valuable — and more vulnerable. Information governance is paramount to protect critical data assets from insider threats. It provides business intelligence to help configure security controls, which improves risk management and coordination of information management activities. A solid information governance foundation helps organizations adopt a risk-based approach to protect their most valuable assets, while instilling sound data management hygiene.

1. Adopt a risk-based approach
2. Identify physical locations of your critical data assets
3. Advocate user access management hygiene
4. Establish business rules of information management

Advanced forensic data analytics is becoming an indispensable tool to detect insider threats

Applying advanced data analytics techniques, we are able to help organizations objectively analyze insider behaviors and generate risk rankings within the insider population. Data analytics also helps to enhance the information security posture by making it more difficult to work around the security controls than the traditional signature-detection methods.

Raw data

Terabytes of event data collected daily

At a rate of thousands of 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 behaviors

Create a risk-ranking score system

Anomaly detection through machine learning + Linguistic analysis + Assessment of "indirect" indicators = Risk ranking

77% "Internal fraud" risk, an area that has long been managed using forensic data analytics, was ranked as the top use case at 77%.

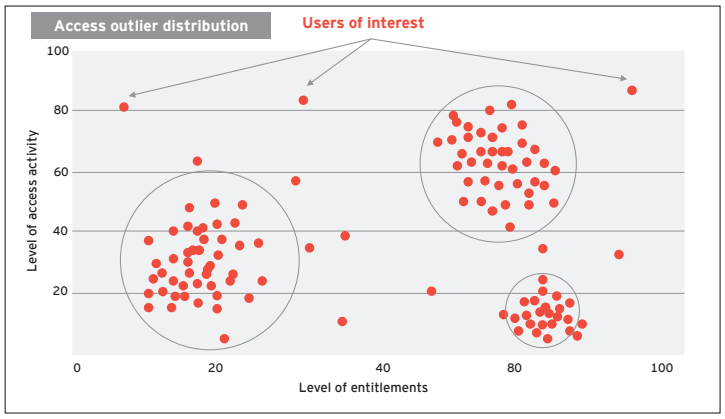
70% "Cyber breach or insider threat" is the second-highest risk area, where 70% of respondents are using forensic data analytics.

Source: EY 2016 Global Forensic Data Analytics Survey

UBA is by far the most commonly used data analytics technique in managing insider threat risks. Via natural language analysis and sentiment analysis, UBA focuses on emotional or evaluative content of text communications. It takes a holistic and human view of multiple data sources, including emails, HR data and web-browsing activities, combining them to tell us not only what is happening, but also how and why it is happening. UBA is also used in predictive/preventive analysis to highlight sentiment patterns that match those that have previously been linked to theft or misconduct. It allows organizations to sample threat vectors, such as emails to competitors, secretive emails, large volumes of file deletions or copying to a USB drive, and categorize an employee's risk levels using a risk-ranking score system.

> **" By 2018, at least 25% of self-discovered enterprise breaches will be found using user behavior analytics."**
>
> *Best practices and success stories for User Behavior Analytics, Gartner, 2015*

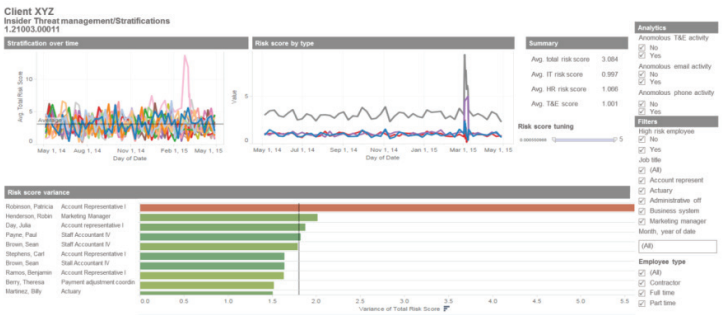
UBA with outlier analysis can help identify red flags that are outside of the security baseline. The outlier analysis can be further enhanced via risk scoring to identify the risk areas that warrant in-depth investigation. Natural language processing is frequently used to monitor email and instant messaging communications to detect emotive tone and sentiment, risky topics and named entities.



As the adoption of advanced data analytics increases, we foresee that insider threat programs will draw on the capabilities of speech recognition and computer vision. While both technologies have been in existence for some time, using them to proactively manage insider threat risk is still minimal. Computer vision uses facial recognition and license-plate scanning to automatically sift through security video footage and detect employees in the wrong place at the wrong time — indicating potentially malicious behaviors. Speech recognition can enhance findings from call center monitoring, where calls are monitored for off-script, negative emotion or threat words, using phonetic text, speech-to-text transcriptions and emotion detection.

Manage risk alerts in interactive visualization tools

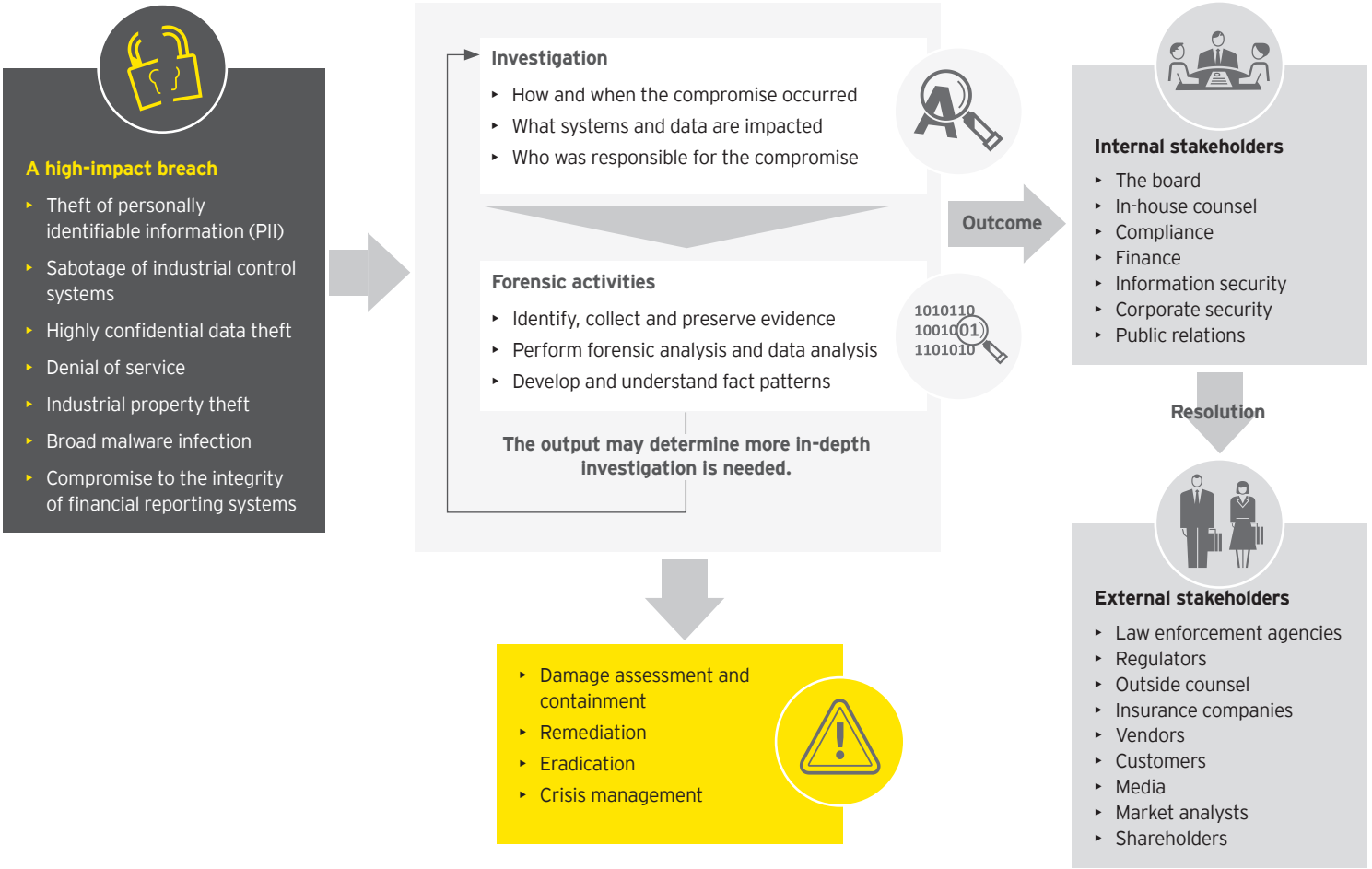
Visualization is a powerful data analytics technique for identifying anomalies that are only evident when taking into account the multi-dimensional data attributes, especially in the intersection of structured and unstructured information. Using visualization technologies, we can display anomalies, or risk alerts, through dashboards, reports and workflow diagrams to help companies effectively monitor and respond to alerts — including a full contextual picture of the events and actions generating the alerts. With the benefit of a holistic view of alerts displayed on a common time dimension, overlaid with contextual market data and a news feed, users can drill down into any alert using an extensive and customizable list of filters and functions. To improve organizational response to insider threats, we develop individualized dashboards and reports to help stakeholders focus on their responsible areas and take appropriate actions quickly. The ability to personalize risk analysis also strengthens control environment by limiting sensitive and high-risk information to the relevant stakeholders only.



Respond and recover with a breach response program

While there are nuances between external and insider breaches, the negative impacts are similar and should therefore leverage the same response program in anticipation of a major breach. The more an organization is prepared for a major breach, the more likely that its impact can be reduced. While the organization strives to build as strong an insider threat program as possible, it must also develop a breach response program that considers both insider and external breaches.

What and who is involved in a high-impact breach?



Legal concerns

Implementing an insider threat program cannot be successful without careful consideration of the legal and regulatory implications.

Insider monitoring must comply with a proliferation of new state and national privacy legislation:

- In the United States, the Electronic Communications Privacy Act allows employers, under certain provisions, to monitor email and other electronic communications of their employees.
- In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) limits how employers may collect, store and use electronic data. Some provincial governments in Canada have opted out of PIPEDA in favor of stricter privacy laws.
- The Member States of the European Union, in compliance with the European Convention on Human Rights, adhere to privacy laws under the Data Protection Directive. A draft of the European General Data Protection Regulation (GDPR) was recently finalized and will supersede the Data Protection Directive in 2018.
- The United Kingdom has its own privacy restrictions, described within the Data Protection Act 1998 and the Regulation of Investigatory Powers Act 2000. It will be subjected to the GDPR when it comes into force in 2018.
- The member economies of Asia-Pacific Economic Cooperation (APEC) endorse the APEC Privacy Framework.

Companies dealing with multinational matters encounter added complications that may prevent them from coordinating data transfer activities across borders. For example:

- EU-US Privacy Shield — On October 6, 2015, the European Court of Justice invalidated the Safe Harbor Framework on the basis that the European Commission had not appropriately evaluated whether the US maintains "essentially equivalent" protections of EU citizen data. The EU-US Privacy Shield was announced in early 2016 by the European Commission and US Department of Commerce as a replacement for the Safe Harbor Framework. The agreement intends to protect personal information of EU citizens to EU standards when it is sent to the US.
- China state secrecy laws — Firms doing business in China must contend with China's state secrets laws, which enable state control of sensitive technical or commercial information. Compliance with these laws, which can also create difficulties in complying with US regulations and disclosure requirements, makes it challenging to gain a universal view of corporate data.

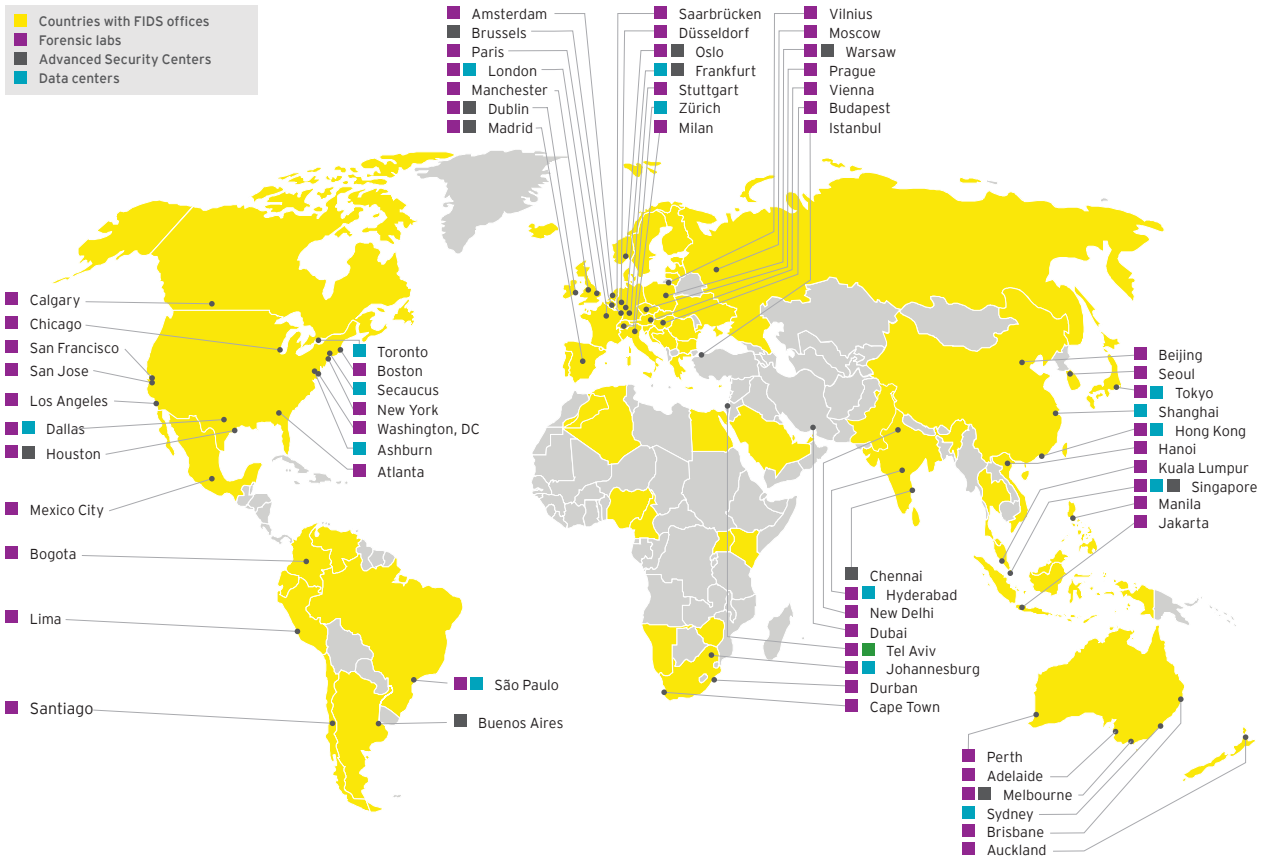
Why EY?

Our Fraud Investigation & Dispute Services (FIDS) team draws from a wide range of industry-focused professionals who have extensive experience in conducting complex, multinational investigations. They come from a variety of backgrounds, including counterintelligence, law enforcement, military, regulators, academics and commercial, with competencies in law, data sciences, linguistics, psychology, computer science, forensics and investigation.

Our services

- Insider threat program:
  - Current and future state assessments
  - Program and policy development
  - Awareness campaigns and training
  - Risk indicator development and data modeling
  - Response and investigation
  - User behavior analytics implementation
- Information governance:
  - Data carve-outs
  - Storage reclamation
  - Insider threat prioritization
  - Legacy backup tape retirement
  - Data disposition consulting
- Cyber breach response management:
  - Impact assessment
  - Litigation support
  - Support for parallel proceedings
  - End-to-end eDiscovery engagement support
  - Cyber investigation
  - Cyber forensics
  - Data recovery and remediation
  - Cyber and network security insurance claims
- Forensic data analytics:
  - Surveillance and behavioral analytics
  - Digital forensics and investigation
  - Anti-fraud and compliance risk analytics

Global presence



EY | Assurance | Tax | Transactions | Advisory

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 4,500 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. And 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.

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

EYG No. 02095-161Gbl
BSC No. 1604-1910400

ED None

ey.com