As organizations take careful measures to protect their critical assets from external risks, they often remain vulnerable to threats from inside their organizations. By studying behavioral changes and detecting routine variations and hidden relationships, companies can more effectively manage insider risk. The insider threat behavioral spectrum (the Spectrum) describes the four key stages of an insider attack. It offers insight into the causes of insider threat and provides guidance on implementing controls to prevent and detect malicious breaches by insiders.

Legal, Compliance and Technology Executive Series

Understanding the insider threat behavioral spectrum

Of special interest to:
- General counsel
- Outside counsel
- Chief legal officer
- Legal technology executives
- Chief compliance officer

Catalyst stage
Expression stage
Preparation stage
Execution stage
Catalyst stage

Adverse events in an employee’s life may be the impetus for them to steal information or engage in other harmful acts. In fact, Carnegie Mellon University researchers concluded that 70% of individuals stole at least some intellectual property 60 days or fewer before their termination (whether forced or voluntary), and 57% of the cases of insider IT sabotage involved an attack within 60 days of the insider’s termination from the organization. The percentage of departing employees who steal intellectual property may sound surprisingly high. Remember that IP theft might range from more common acts such as taking contacts or copies of documents that an employee created to the less common theft of customer lists, product designs, etc.

Expression stage

Catalyst events usually cause the individuals to alter their work behaviors. While excessive time off, odd working hours and increased job search activities can be masked, employees who are insider threats may demonstrate public behavior that signals a problem. For example, prior to illegally disclosing nearly 750,000 protected documents to WikiLeaks, former United States Army soldier Chelsea Manning’s coworker stated during testimony that Manning “punched me in the face unprovoked and displayed uncontrollable behavior that was deemed untrustworthy.”

Preparation stage

In many cases, insiders will not act on impulse. They will take steps to collect information of interest prior to any action. For instance, to collect the information he stole, Edward Snowden used a web crawler to search for data that may be of interest to him. Most of the preparation activities do leave digital footprints that may be detected early.

Execution stage

Companies usually employ limited monitoring of authorized personnel, which can make it easier for an insider to commit fraudulent or criminal activities.

When a frustrated former employee of a global financial institution anticipated termination in 2013, he transmitted codes that erased network configuration files, resulting in a loss of connectivity to approximately 90% of all of the bank’s networks across North America.

Use analytics for better prevention and early detection

Many of the actions in the expression and preparation stages are not easily detectable by traditional, signature-based methods because authorized access to sensitive information does not normally trigger alerts. Behavioral analytics is designed to help associate activity anomalies with conduct patterns to identify the risk of employee malfeasance.

By integrating data relevant to each stage of the Spectrum, companies can use analytics to identify catalysts of discontent, expressions of frustration, hallmarks of preparation and obvious elements of execution. For example, there may be indicators aligned with the catalyst stage within HR records or ethics hotline records. Logs from knowledge management systems or databases may reveal searches for information of interest that would be seen during the preparation stage.

Good policymaking can preempt risky behavior

While advanced data analytics techniques can help organizations objectively evaluate insider behaviors and enhance their security posture, they are not enough. Organizations should combine the use of technology with well-defined policies, consistent communication and training, and routine due diligence.

Standardizing onboarding, background screening and employee separation procedures will also offer opportunities for mitigating harmful activities. For example, having a uniform employee separation process mandating a certain level of security review upon termination might stop a disgruntled employee from conducting IT sabotage or data theft.

It is a best practice that organizations conduct routine employee screening (as permitted by privacy regulations), particularly for those who have privileged access to critical assets, to detect changes in their behaviors or situations that can lead to insider threats. Someone filing for personal bankruptcy or involved in litigation may have a greater incentive for stealing corporate secrets. As a result, the lack of recurring screening may put a company at risk.

Promote insider threat awareness

As organizations gather more data about the behavioral patterns of risky insiders, they should use the findings at each stage of the Spectrum to create training that generates awareness and insights about insider threats. The training should prepare employees to identify risky insiders and address them before the risk escalates. By providing examples of indicators seen in each phase (expressions of anger, physical violence, changes in work patterns, working odd hours, increased interest in areas not aligned to current job assignments, etc.) and highlighting tools for dealing with them (supervisor notification, hotline, etc.), organizations can help employees deal with insider threat behavior. The curriculum can be delivered through case studies, group exercises or personalized trainings to reinforce the messages and, ultimately, the organization’s defenses.

Conclusion

It is vital to promote a culture of collaboration to effectively mitigate the risk of insider threats. To build enduring safeguards, organizations can consider having policies and training curriculums in place, developing repeatable and consistent monitoring processes to identify potential threats, and using a broad range of data sources to gain a thorough understanding of the risk environment.

These efforts are most successful when done in coordination with a cross-disciplinary team that includes legal counsel to address privacy, data protection and cross-border data transfer concerns, human resources to achieve proper pre-employment screening and procurement to certify that third-party vendors are thoroughly vetted.

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 approximately 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.

© 2018 EYGM Limited.
All Rights Reserved.

EYG no. 00791-181Gbl
1712-2512839

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