Managing insider threats

Why you need a proactive approach to protecting information assets from authorized users with malicious intent

32%

of respondents said insider crimes are more costly or damaging than incidents perpetrated by external adversaries.

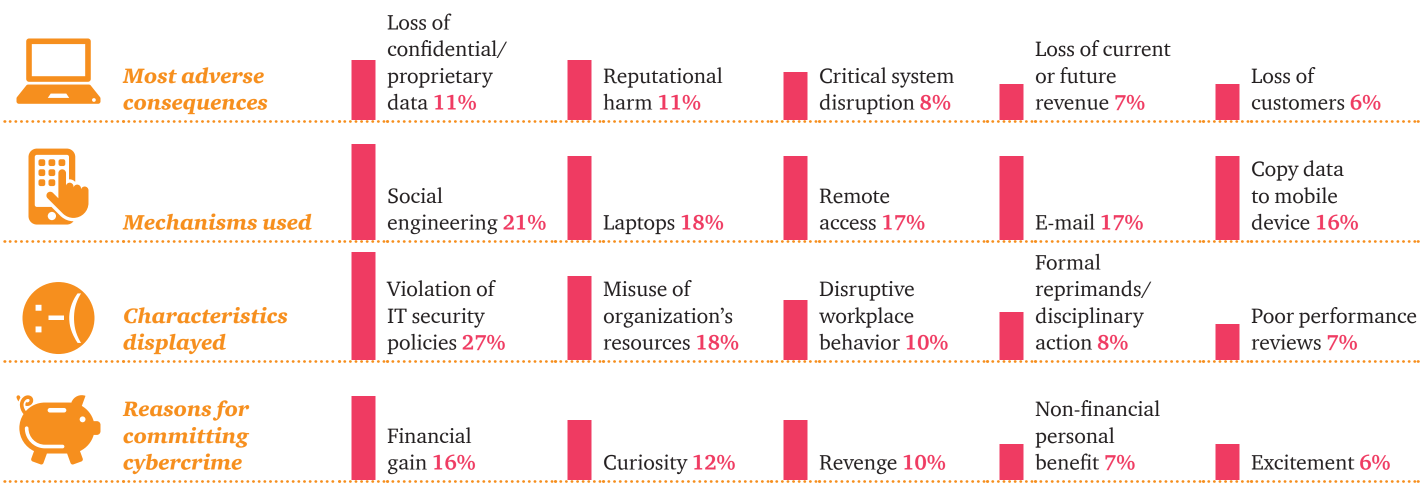
When it comes to cybercrime, incidents caused by external actors dominate news headlines. But senior executives know that security breaches by insiders—employees and business partners with trusted access—can be even more damaging. Yet the majority of businesses are unprepared for these insider threats.

Consider this: Almost one-third (32%) of respondents to PwC's 2014 US State of Cybercrime Survey said insider crimes are more costly or damaging than those committed by external adversaries, yet less than half (49%) say they have implemented a plan to deal with internal threats.[1] The lack of a formal insider risk-management strategy seems shortsighted, given that 28% of survey respondents detected insider incidents in the past year.

While current and former employees are the source of most insider compromises, trusted business partners can also commit or unwittingly facilitate cybercrime, as high-profile government-contractor data leaks and retailer breaches have so unequivocally proved. Third parties and business partners with trusted or authorized access can be a particular risk because most organizations do not adequately assess their cybersecurity practices. In fact, only 44% of respondents to the PwC cybercrime survey said they have a process for evaluating third parties before they engage in business operations with them, and just 31% include security provisions in contract negotiations with trusted vendors and suppliers.

[1] 2014 US State of Cybercrime Survey, co-sponsored by CSO magazine, CERT Division of the Software Engineering Institute at Carnegie Mellon University, PwC, and the US Secret Service, March–April 2014

Figure 1: The causes and consequences of cybercrime committed by insiders*



*A current or former employee, service provider, authorized user of internal systems, or contractor

Source: 2014 US State of Cybercrime Survey, co-sponsored by CSO magazine, CERT Division of the Software Engineering Institute at Carnegie Mellon University, PwC, and the US Secret Service, March–April 2014

Why insider threats are so insidious

Insider threat actors often have an advantage over external adversaries because they have authorized access to data and systems, and therefore have no need to breach security controls. Even insiders with access to the network, but no authorized access to certain types of systems and data, are more likely to understand the organization's competitive environment. They also may know exactly where to look for the company's most valuable information, including customer lists, pricing strategies, and research and development initiatives currently in progress.

Often employees have access to intellectual property and trade secrets that are very valuable to external threat actors. Recently, for instance, employees of US-based agribusiness companies allegedly provided samples of valuable bio-engineered seeds and their gene sequences to criminals who planned to sell them to a Chinese business. One of the US companies said the theft resulted in the loss of at least five years of research and a minimum of $30 million in revenues.[2] When workers have access to data this valuable, the temptation of financial gain can become a significant motivation.

Most employees start a job with honest intentions and typically become a threat as a result of subsequent personal financial difficulties, job dissatisfaction, interpersonal conflict, workforce reductions, or to secure a more lucrative position with a competitor. Case in point: An employee of an oil and gas company, after learning that he would soon be terminated, shut down the organization's network servers and deleted critical data. As a result, the company was unable to fully communicate for 30 days and had limited access to data and applications, resulting in a loss of more than $1 million.[3]

Others may react against ideological differences with the organization or perceived corporate wrongdoing. One need only consider the 2013 leak of a massive trove of government surveillance data by an ideologically disillusioned defense contractor to understand the potential for enormous damage.

Rogue employees often exhibit telltale behaviors before they commit a crime, such as erratic work schedules, drops in performance or attendance, or uncharacteristic comments made to co-workers. Sometimes these signs are even apparent to outside clients, third parties, and external threat actors.

That is an invitation to external adversaries such as nation-states and organized crime groups, which sometimes target vulnerable employees to help steal or gain access to sensitive data. When doing so, they often identify employees who are experiencing financial problems or are obviously looking for new opportunities for employment or financial gains.

Former employees can be equally useful to external threat actors. In 2014, for example, two US-based engineers were convicted of trade secret theft and economic espionage against an American chemical manufacturer. The engineers paid former employees of the manufacturing company to provide the information, which they then sold to state-owned Chinese companies.[4]

[2] FBI, *Chinese National Arrested for Conspiring to Steal Trade Secrets*, July 2, 2014

[3] US Attorney's Office, *EnerVest Computer Attack Draws Four-Year Federal Sentence*, May 20, 2014

[4] FBI, *Two Individuals and Company Found Guilty in Conspiracy to Sell Trade Secrets to Chinese Companies*, March 5, 2014

Figure 2: Insider threat influencers, motives and behaviors

External influencers

Foreign government intelligence agencies

Criminal enterprises

Activists

Competitors

Motives

- Personal financial distress or greed
- Notification or fear of layoff
- Job disgruntlement or revenge
- Interpersonal work conflict
- Steal data for monetary gain
- Access critical operational systems to extort data for financial gain
- Obtain access to systems to transfer funds
- Disrupt critical systems for ideological reasons
- Expose perceived wrongdoing

Behaviors

- Use authorized access to systems and data rather than physical access
- Commit crimes while onsite rather than off premises
- Operate during regular business hours rather than off-hours
- Exporting structured data to unstructured files on work computers, network shares, or external media
- Attaching files to personal, Web-based Email
- Use of USB storage devices
- Printing of critical data in bulk
- Installation of unauthorized software on work computers
- Drop in performance and/or attendance
- Uncharacteristic comments made to co-workers

What companies should do

Minimizing and managing crimes committed by inside actors will demand that organizations develop and execute a specific insider-threat management program that is aligned and integrated with their business, cybersecurity, and data-protection strategies. The basic building blocks to such a program are: **identify** what is most valuable to you and a potential insider threat; **protect** against insider threats; **detect** when threats manifest in your organization; **respond** to limit their potency and potential damage; and **recover** to restore your environment to a better state.

It's important to understand that insider risk cannot be managed by the IT, information security, or corporate security business functions alone. Nor can technology itself forestall insider threats. Effective management will require a disciplined, risk-based, cross-functional approach that includes IT, information security, corporate security, human resources (HR), legal, audit, and other stakeholders. It will also demand participation from appropriate lines of business, as well as finely tuned data privacy policies.

Fortunately, the U.S. government has made strides in providing guidance for companies in cybersecurity, including integrating insider threat management into cybersecurity strategy. Until recently, U.S. government guidelines for creating an integrated security strategy have been disjointed and limited. That changed with the publication of the National Institute for Standards and Technology (NIST) Cybersecurity Framework, a set of voluntary guidelines for risk-based cybersecurity. While the voluntary NIST Cybersecurity Framework targets critical infrastructure providers, we believe it offers advantages for organizations across industries for its stated goal of improving risk-based security. Implementation of the guidelines can facilitate a strategic shift from reactive compliance to a more effective, proactive risk-centric approach to cyber threats and vulnerabilities.[5]

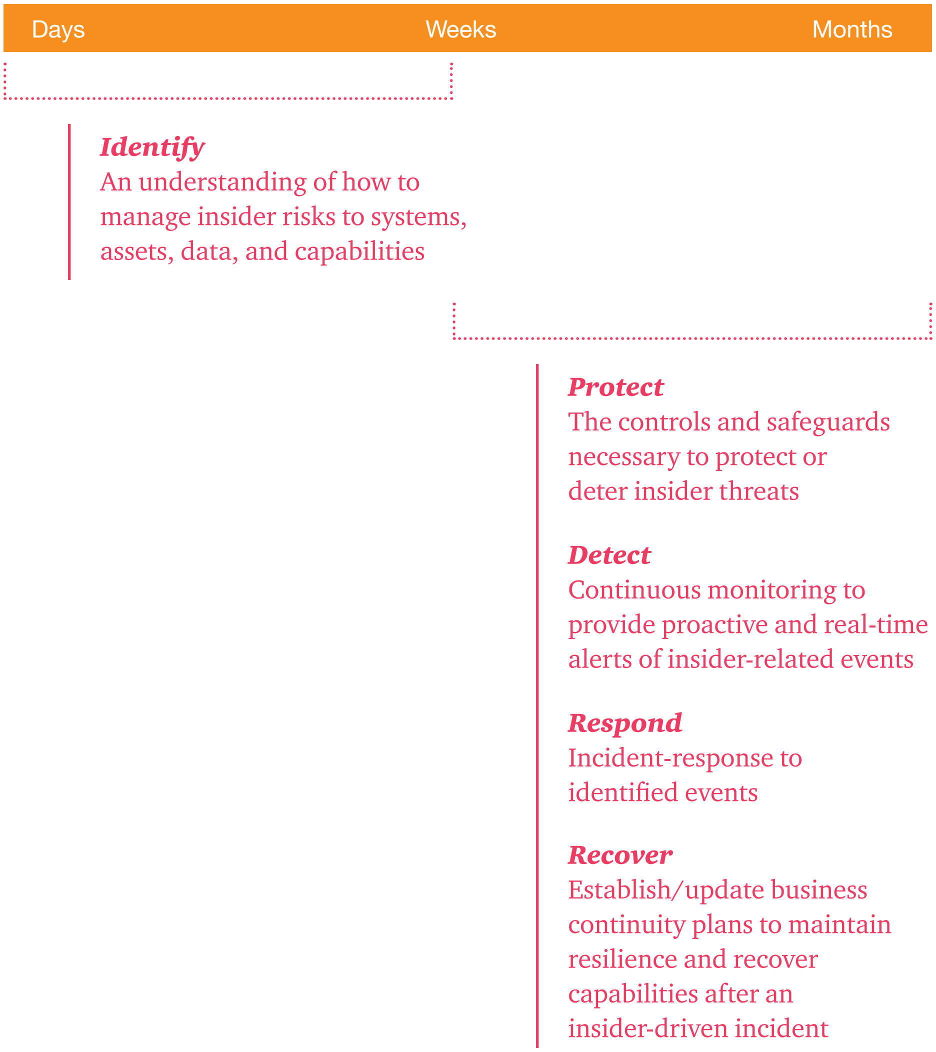
The framework lays the groundwork for additional benefits, including effective collaboration and communication of security intelligence among executives and industry organizations, potential improvements in broad enterprise risk management, reduced legal exposure, and even enhanced regulatory compliance. These elements are all essential to managing insider threats to sensitive data and systems.

[5] PwC, *Why You Should Adopt the NIST Cybersecurity Framework*, May 2014

Building an insider program

Organizations can use a phased approach to build an insider threat management program over time which is compliant the NIST framework functions of: Identify, Protect, Detect, Respond, and Recover.

A phased approach to an enhanced insider threat program



Identify
An understanding of how to manage insider risks to systems, assets, data, and capabilities

Protect
The controls and safeguards necessary to protect or deter insider threats

Detect
Continuous monitoring to provide proactive and real-time alerts of insider-related events

Respond
Incident-response to identified events

Recover
Establish/update business continuity plans to maintain resilience and recover capabilities after an insider-driven incident

Areas of focus

Identify

- Governance
- Risk management
- Human resources
- Physical security
- Ethics & compliance
- IT asset & user credential management
- Existing security monitoring technology

Protect

- Access controls
- Awareness and training
- Location of sensitive data
- Policies

Detect

- Response plan
- Event classification
- Monitoring technologies
- Event classification
- Threat intelligence
- Trade secret movement
- Computer usage

Identify

The first element of the Framework enables a company to develop an organizational understanding of managing insider risk. It focuses on processes that help corporations understand the business context of information security, resources that support critical business functions, and related insider risks. This knowledge can help the organization focus on and prioritize security efforts that are consistent with its risk-management strategy and business needs.

To get there, senior executives and business leaders should first identify and agree upon what constitutes the organization's high-value data and systems—typically, those that most directly support critical business functions—and who is responsible for protecting these assets against insider threats. Attaining consensus among executives, business-line leaders, and product managers on what priorities to apply to which valuable assets will be critical. A senior leader who is visible and accountable to the C-suite will be necessary to gain buy-in, drive change, and set roles and accountability for managing insider risk.

Beyond knowing what data and systems are valuable to the company, it is also important to understand what would be lucrative to criminals. One way to do so is through the use of external threat-actor profiles to help identify the types of adversaries that are likely to target the organization, including those with a history of using third parties like contractors or suppliers to steal information. These profiles also can help clarify why adversaries might threaten a business, how they might do so, and what systems they are likely to target. Understanding these external threats also will help reduce the possibility that outside criminals will target and recruit employees and contractors.

Key questions to ask

Which systems, if disabled, would create the most business risk?

What data, if stolen or corrupted, would result in serious business risk?

How is protection of these high-value assets prioritized?

Protect

After high-value data has been identified, organizations should pinpoint where the information assets are stored across the enterprise and determine who has access to them. All authorized users should be identified by job function and geography. It may also be worthwhile to perform some level of cyber due diligence to establish a benchmark, then determine if any of these users are currently behaving maliciously or suspiciously.

Compiling a set of technical and nontechnical insider-risk indicators will be essential. These indicators should be based on an understanding of how insider threat actors target sensitive data, what telltale signs or evidence would expose their actions, and how the organization will respond. Technical indicators are related to how insiders use their computers and network access; nontechnical indicators constitute verbal and nonverbal human behavior. Identifying the risk indicators that are relevant to the individual and job role will help determine the technology needed to monitor computer and network usage, how to configure that technology, and the HR, legal, and ethics policies that should be implemented.

For many businesses, it may be advantageous to perform deeper background screening to identify employees with privileged access who may be predisposed to illegal activity. Often, this enhanced background due diligence will be necessary only for a subset of employees. In addition to considering the risk potential of individual employees, evaluating insider risks by job role and access associated with that role can help predict and reveal insider risks.

Organizations should also assess a variety of controls and components that, taken together, provide the foundation for an insider-threat management program: access control tools, policies and processes, employee training and awareness, and detection and monitoring tools and analytics. Corporations also should review their decision-support processes to enhance detection and response of incidents, management hiring decisions, and contract assessment. At the same time, effective third-party management can set expectations and contribute to informed, efficient risk-based decisions that can help avoid additional threats.

Employees and managers form the backbone of an effective insider-threat management program because they are often in a position to first notice suspicious behavior or risk indicators. As a result, instilling a "see something, say something" mindset among employees and managers can help detect—and even deter—insider threats. Most organizations have existing information security and ethics training programs that can serve as effective channels to communicate precautions and indicators. These programs also can help instill a sense of personal responsibility and ownership that may help prevent incidents.

Technology, of course, also plays a role. Companies have invested in myriad cyber- and information-security solutions over the last 15 years, and many of these can be calibrated and integrated with other tools to better manage insider threats. Technology solutions and processes can include host- and network-based monitoring, data loss prevention, background investigations, forensic interviews, training programs, and decision-support processes. These tools can produce a staggering amount of information, and as a result threat analytics tools will be essential to provide context and insight into real-time security alerts and broad threat patterns. Analytics also can ultimately help organizations prioritize and drive security operations and investigations.

Finally, evaluation and updating of corporate policies designed to monitor and control computer and network use can help organizations carry out a more rigorous risk assessment.

Detect

Enhancing existing technologies and deploying new tools to monitor computers and networks can greatly improve an organization's ability to manage and reduce insider risks.

Effective detection of insider incidents will require that organizations identify anomalous activity in a timely manner and understand the potential impact. Doing so will demand that incidents are analyzed to understand the methods and targets compromised, and that event data are aggregated and correlated across the enterprise. It also will be necessary to conduct vulnerability scans, and continuously monitor network activity of users.

Once deployed and fine-tuned, companies should integrate these technologies into a broader threat-intelligence platform that leverages nontechnical risk indicators from other business functions such as HR, ethics, and corporate security. Managing and monitoring these technologies and intelligence-correlation mechanisms will be a discipline that may require a dedicated and highly skilled team.

It may also be necessary to update and refine certain policies, including the following:

- Periodically remind employees that online behavior is electronically monitored, and obtain signed acknowledgement and consent to this policy.
- Control the use and type of USB storage devices (e.g., external hard drives, thumb drives, encrypted, serialized, etc.).
- Control USB ports on computers.
- Control access and transfer of data from databases.
- Implement controls regarding removal of hard copies of sensitive documents from company premises.
- Tightly control Internet access of users who have access to high-value data and the capability to transfer electronic funds.

Organizations that implement and enforce strong policies—and educate employees about these policies—can create an environment in which workers are less likely to commit cybercrime.

Respond

Continuous monitoring of high-value data, systems, and activities across the enterprise will require a dedicated team to scrutinize and correlate the activity of users with privileged access.

Monitoring and correlation should be performed in tandem with continuous analysis of risk indicators provided by corporate security, ethics, and HR. For some organizations, it may be necessary to risk-rate and assess users based on their access to sensitive information or specific role in the organization. Ongoing monitoring, regular background due diligence, and re-certification of access rights should also be considered for these users. Remember that many insiders become malicious only after they are granted authorized access.

Containment and mitigation of insider incidents will hinge upon a tested response plan. This plan should be executed immediately after detection, and leaders should communicate to employees their roles in response activities. Incidents should be categorized according to the response plans, and alerts from detection systems should be analyzed. In doing so, organizations may find new insider vulnerabilities that should be documented as risks.

Part of the response phase should be a carefully considered intervention plan and methodology for dealing with suspected insider threats. Risk indicators will not always yield "smoking guns," and a heavy-handed approach can potentially create risk where none previously existed. It can, for instance, result in unsubstantiated allegations, indiscreet inquiries, and other actions that erode morale or alienate employees. This can be equally or more damaging than insider threats.

Recover

As part of recovery, an insider threat-management program should be tightly linked with a corporation's business continuity planning process. This will help maintain resilience—especially among the workforce—and recover capabilities affected by the threat. The NIST Framework and other risk-management approaches emphasize the importance of information sharing, feedback, and incorporating lessons learned to improve planning and communications in all five phases.

The lessons learned should be incorporated into the existing response playbook. These updates, along with recovery activities, should be communicated to employees so that they understand how the business responds to insider incidents—and that it takes insider threats seriously.

Organizations also should include reporting of incidents to law enforcement agencies in their recovery plans. That's a process that many businesses do not carry out. PwC's 2014 US State of Cybercrime Survey found that only 12% of organizations that had detected insider cybercrimes notified law enforcement officials.

Unethical employees who get away with criminal acts without legal ramifications may commit similar crimes at their next job. By not reporting criminal activity, there will be no public record of wrongdoing, making it difficult for the next employer to identify risk during pre-employment background checks.

Questions the Board should consider

Who is in charge of insider threat management?

How many detected security incidents are attributed to insiders?

What is the impact of insider incidents?

How thorough is our policy for responding to insider incidents?

What departments or functions are involved in handling insider threats?

How do we assess potential and existing employees and third parties for insider risks?

How do we monitor employees for malicious activity?

How do we monitor business partners for compliance with our security practices?

What are other companies doing to manage and mitigate insider threats?

Should the company reveal to its workforce, shareholders, and regulators the existence of an insider threat-management program?

An integral component of your risk management practice

A well-designed and effectively implemented insider-threat management program won’t eliminate internal risks, but it can help reduce the likelihood of compromise and mitigate the damage of incidents. It is increasingly critical because internal crimes are often more costly than the high-profile exploits of hackers and organized criminals. Insider crimes also can be precisely targeted and more damaging since internal threat actors are likely to know where valuable information resides and how to access it.

To be truly effective, top executives and the Board should actively support and participate in the insider-threat management program. Top-down support can also help improve regulatory compliance and ensure that appropriate safeguards are in place to mitigate legal action that may result from an internal breach.

Given today’s elevated threat environment, it’s no longer possible to protect all data at the highest level. But implementing a well-designed insider-threat management program and fusing it with existing security practices can help organizations more effectively detect and rapidly respond to internal risks, a capability that is integral to an effective cybersecurity practice.

www.pwc.com/cybersecurity

Contacts

To have a deeper conversation about managing insider threats, please contact:

Sean Joyce
Principal
sean.joyce@us.pwc.com

Shane Sims
Principal
shane.sims@us.pwc.com

Neal Pollard
Director
neal.a.pollard@us.pwc.com

David Burg
Principal, US and Global Cybersecurity Leader
david.b.burg@us.pwc.com

Michael Compton
Principal, Cybersecurity Strategy and Operations
michael.d.compton@us.pwc.com

Peter Harries
Principal, Health Industries
peter.harries@us.pwc.com

John Hunt
Principal, Public Sector
john.d.hunt@us.pwc.com

Mark Lobel
Principal, Technology, Information,
Communications and Entertainment
mark.a.lobel@us.pwc.com

Gary Loveland
Principal, Consumer and Industrial
Products and Services
gary.loveland@us.pwc.com

Shawn Panson
Partner, Risk Assurance
shawn.panson@us.pwc.com