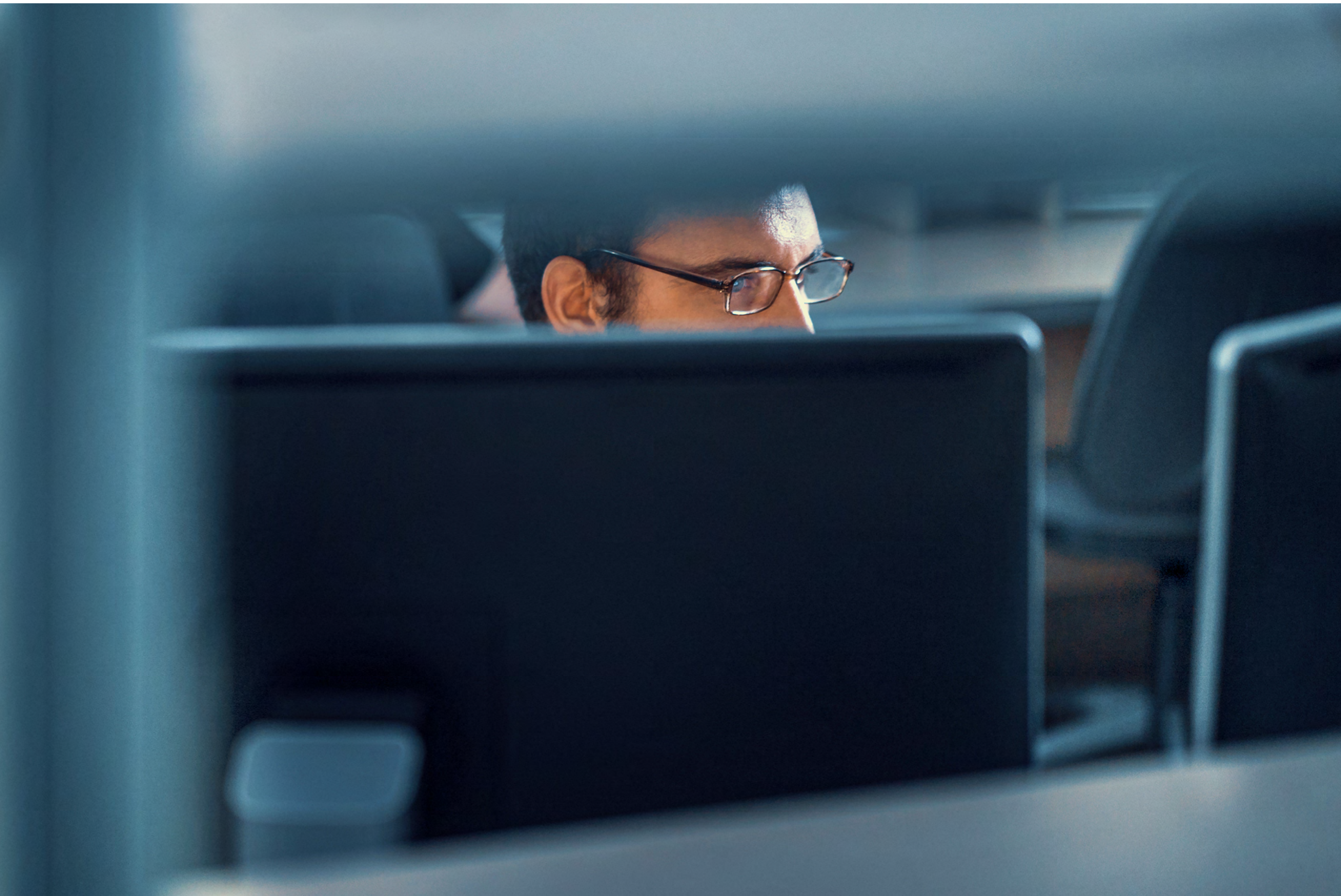
opentext™ | Cybersecurity

Brochure

Insider Threat Survival Guide

Essentials for Outwitting Your Adversaries



Insider Threats at a Glance

In 2022, insider threats have become more numerous, more expensive to remediate, and more varied, according to research from the Ponemon Institute.[1] Two-thirds of companies (67%) respond to more than 20 insider-threat incidents per year.

- Negligent employees and contractors are the largest source of insider threats, accounting for 56% of all incidents.
- Imposters posing as insiders through stolen credentials is the fast growing threat, accounting for 18% of all incidents.
- The average company spent $15.4 million each year to monitor for, respond to, and remediate insider threat incidents.

In April 2021, hackers used a stolen username and password of an employee at the United Nations to access proprietary project-management software and then compromised other servers in the network.[2] In June, a ransomware group convinced an employee at game maker Electronic Arts to provide a login token for the company network, leading to the reported theft of 780 GB of data, including source code for the company's Frostbite graphics engine and internal development tools.[3] And, at the end of the year, the FBI arrested a former developer for network technology firm Ubiquiti for stealing data and leaking information about a breach of the company's cloud data storage in December 2020, resulting in a $4 billion loss in market capitalization for the firm.[4]

Widely considered to be the most damaging type of cyberattack, insider threats have evolved over the past decade to become more numerous and varied. The average company now responds to more than 20 incidents each year, spending an average of $15.4 million to handle and recover from breaches caused by a variety of insider threats, including negligent workers, malicious employees, and imposters using stolen credentials.

Preparing for insider attacks, intentional or otherwise, before they happen can significantly reduce detection and response times and limit damage. Insider threats differ from external threats, requiring different training, policies, processes and tools to detect, assess, and respond to intentional and unintentional insider threat activities. Companies should prepare now, because one incident can cost millions.

Preparing for insider attacks, intentional or otherwise, before they happen can significantly reduce detection and response times and limit damage.

The Basics of an Insider Threat Program

An insider threat program requires that key components are in place to work. These basics—including training, processes, and policies—are the framework on which any insider threat program can be built. Each piece of the framework should be considered by a cross-disciplinary group pulled from across a company, including the information-technology department, cybersecurity professions, human resources, and any legal counsel.

As decisions are made regarding the contents of an insider threat program, the group should create a policy document to clarify the elements of the program. Making an official program will enable the group to work across various business silos to ensure that the entire company leadership is on board with the effort.

Policies

The different components of an insider threat program only work when there is a solid policy framework holding the program together. Companies should have specific policies for the storage of important data—where is it stored, how is it protected, and who can access it—as well as how the company can monitor the spread of data and intellectual property.

Monitoring employees is an activity that is fraught with potential pitfalls, so companies should be transparent about how they are monitoring employees, when monitoring is appropriate, and what protections are in place to prevent the abuse of the system. There should be oversight to ensure policy compliance, and mitigation measures against the risk of individuals, who are in charge of monitoring, being compromised.

[1] Ponemon Institute. "2022 Cost of Insider Threats Global Report." **https://static.poder360.com.br/2022/01/pfpt-us-tr-the-cost-of-insider-threats-ponemon-report.pdf**

[2] Turton, William and Mehrotra, Kartikay. "UN Computer Networks Breached by Hackers Earlier This Year." Bloomberg. News article. 9 September 2021. **www.bloomberg.com/news/articles/2021-09-09/united-nations-computers-breached-by-hackers-earlier-this-year**.

[3] Cox, Joseph. "How Hackers Used Slack to Break into EA Games." Vice. New article. 11 June 2021. **www.vice.com/en/article/7kvkqb/how-ea-games-was-hacked-slack**.

[4] Krebs, Brian. "Ubiquiti Developer Charged With Extortion, Causing 2020 'Breach'." KrebsOnSecurity. News article. 2 December 2021. **https://krebsonsecurity.com/2021/12/ubiquiti-developer-charged-with-extortion-causing-2020-breach/**.

Training

Training is important for both employees and security specialists and is essential to lay the groundwork for a good insider threat program.

As attackers continue to up their games in social engineering, employees need to know their role in preventing and detecting malicious insider attacks, and need to be trained in information-security policies to prevent inadvertent mistakes that result in data loss or the theft of an employee's credentials. In addition, employees regularly work with sensitive information, and some—such as programmers and sales people—may develop a sense of proprietary ownership of that information. Companies need to spell out the rules of ownership for information, such as a program code and client information, to prevent misunderstandings that result in data loss.

Cybersecurity professionals, meanwhile, need to be trained in how to detect, respond to, and mitigate insider attacks. The team may consist of technologists and former law enforcement professionals with an investigative background. Because the attacks often look like normal employee activity, companies need to deploy automation and train specialists to tune and triage alerts to find insider attacks amongst the noise of daily activity.

Your industry may have a specific risk profile and need to prioritize certain types of attack. It is critical to identify the appropriate use cases and ensure the right data and training is available to your analysts in addressing such use cases.

Processes

While it is important to have robust access control processes and tools to protect sensitive and proprietary data, the insidious nature of insider threats means bad actors, intentional or otherwise, tend to be authorized users running authorized program and accessing authorized data.

The Center for Threat Informed Defense (CTID) recently published a draft list of 55 MITRE ATT&CK techniques spanning a wide range of tactics related to insider threats. The complexity stemming from different permutations of tactics, techniques and sub-techniques is further compounded by diverse and mutating malware. As attackers get more sophisticated, the number of unknowns in your insider threat landscape explodes. Hence, a holistic approach encompassing access controls and preemptive discovery of behavioral anomalies across all entities (users and devices) and response acceleration is essential.

Given the requisite broad detection coverage and the resulting tsunami of data and alerts, an automated and intelligent process should be put in place to enable your analysts to quickly zoom in on and response to the threats that matter.

Is It Ethical to Have an Insider Threat Program?

By their very nature, insider threat programs are designed to monitor employee activity: What data and sites are they accessing? Are they uploading a significant amount of data? Are they acting anomalously? It is necessary to answer these questions to detect insider threats quickly, but tracking the user outside of the context of threat detection should be avoided.

Ethics are based on transparency, consistency, and utility. Current regulations allow companies to monitor communications on their networks for "legitimate business purposes"—such as preventing insider attacks—but the process should be documented and employees advised of the monitoring to avoid misunderstanding and the possibility of incidents being escalated to legal action. We should keep in mind that attacks stemming from, say, compromised accounts. which are unintentional in nature, and attacks with malicious intent, often have similar or overlapping indicators. So, an insider threat detection system serves to not only incriminate, but also to exonerate.

Companies that are concerned with employees doing personal tasks or "cyberloafing" on company time, should instead look to block sites during business hours.

Establish a Threat-Response Process

Each company needs to develop a process for the triage of potential insider-threat alerts, how to respond to potential incidents, and what steps to take to resolve an incident. Having a well-rehearsed process in place prior to an attack can cut 9 days off the average response and recovery time and save an average of $600,000 per incident, according to a recent survey analysis by Forrester Research.[5]

In addition, documentation is critical. Companies must document any security alert deemed evidence of suspicious activity or of a

[5] Mellen, Allie et al. "The 2021 State of Enterprise Breaches." Forrester Research. PDF report. 9 April 2022. **www.forrester.com/blogs/ breaches-by-the-numbers-adapting-to-regional-challenges-is-imperative/**.

threat, the harmful behavior, and the steps take to respond to the incident. Good documentation helps create a solid playbook as well as a way to internalize the experiences of the security team. Strong and consistent documentation will also head off privacy issues, legal complications, and make certain that every incident is handled in a similar way.

What to Do When You Find or Anticipate an Insider Threat

Following an alert—or a sequence of alerts—that raise the suspicion of potential insider threat activity, the resulting triage and mitigation steps should be documented and consistent. Insider threat response must be a structured process for every single threat that is well documented and always followed. Any indications that the company is treating groups of people differently based on ethnicities or genders could lead to a lawsuit and derail the business's right to legal action for the original infraction.

Sometimes, you may not want to wait for an alert. If you know that a team may be downsized or certain employees may face disciplinary action, you may want to initiate heightened monitoring given the elevated risk of nefarious activities.

The response to a potential insider threat should be prioritized because response activities have different time scales. In the short term, a company should take actions that mitigate the most immediate impacts, such as prevent the further theft of data and any ongoing harm to the company's IT environment. In the long term, specific groups need to investigate the impact of the whole incident, conduct a post-mortem analysis of the performance of the current insider-threat program, and find ways to improve future defenses and response.

Tools for Detecting and Responding to Insider Threats

The tools needed to detect insider threats are different than the tools typically used to prevent and detect attacks by external hackers. While external attackers can mimic an insider once they have breached the network—and certainly, external attackers targeting cloud services with stolen credentials can appear to be insiders—the two groups tend to act in different ways.

Following an alert—or a sequence of alerts—that raise the suspicion of potential insider threat activity, the resulting triage and mitigation steps should be documented and consistent.

External attackers' primary tactics tend to be exploitation of software vulnerabilities, credential stuffing, and phishing attacks against legitimate employees to gain credentials or run code on a local system. All of these tactics are aimed to establish initial access, something that insiders, by definition, already have.

On the other hand, insiders tend to look for ways to covertly exfiltrate data, gain additional privileges and access to out-of-bounds systems, and bypass security controls. The tools deployed by a company to catch insiders should have an awareness of the difference between the tactics of external hackers and internal bad actors or incautious employees.

Early Warning Systems

While end point detection and protection software, next-generation firewalls, and e-mail security gateways will catch the lion's share of external attacks, tools for detecting malicious insiders and employee errors need to focus on behavior. Early warning systems are the first line of defense, allowing companies to have visibility into potentially problematic behavior.

User and entity behavioral analysis (UEBA) systems detect threats by correlating different behavioral signals, creating baseline profiles for different classes of users, and alerting when a user's behavior ventures outside their common patterns. Poor implementations can produce significant false positives and noise through which human analysts must sift, delaying or even preventing the early detection of threats. Modern systems integrate artificial-intelligence and machine-learning features to reduce the amount of human interaction required to triage alerts and minimize the number of alerts.

Data Security

Systems for detecting and responding to insider threats should not only focus on user behavior but also monitor how sensitive data is being used. Any database, for example, whose records are systematically being harvested by an employee should raise a red flag. By focusing on protecting critical data and other assets, companies gain another layer of defense that can add to a defense-in-depth approach to preventing serious impacts from insider attacks.

While encryption is a table stakes for defending data, encryption does not solve most security issues related to insider threats. Encryption protects against data being harvested by making the data unreadable by attackers, but insiders typically already have access to the plaintext information, making encryption a better defense against external attackers, rather than internal actors.

Automated Response

Depending on the level of maturity of a company's security professionals and processes, automated responses can quickly head off suspicious activity. Whether through endpoint protection (EPP) software or through a more comprehensive security orchestration, automation and response (SOAR) system, automating response can save time, speed response, and reduce losses.

Case: Source Code, Databases Stolen by DHS-OIG Acting Branch Chief

In April 2022, a jury found a former acting branch chief of the US Department of Homeland Security guilty of theft of government property, conspiracy to defraud the US government and other charges for their scheme to steal source code from the DHS Office of Inspector General (OIG) to create a commercial version of the agency's case management system, which they would then attempt to sell back to the government. Place on administrative leave in October 2017, Murali Y.Venkata was found guilty of multiple charges for exfiltrating proprietary source code and databases that held the personally identifying information (PII) of federal employees.

Steps to Set up Insider Threat Program

Taking the initial steps to create an insider threat program is not difficult. Most companies have the groundwork already established in their human-resource policies, legal processes, and information-security tools. Yet, bringing those disparate policies, processes, and systems into a single program is the hard part. The resulting program should be well documented with frequent opportunities to insert feedback and lessons back into the process to drive the insider-threat program to maturity.

Step 1: Calculate Magnitude of Impact of Insider Threats

Having ready estimates for the potential damages caused by insider threats will help your team secure the budget needed to bring together an insider-threat program. In 2022, 67% of companies had to respond to more than 20 insider-related incidents, while a third had to mitigate up to 20 incidents. Employee negligence or error caused 56% of all incidents, costing an average of $480,000 per incident, while criminal insiders accounted for 26% of all incidents on average and accounted for $650,000 per incident. Credential theft resulted in the most significant damages and recovery costs, more than $800,000 per incident, but accounted for only 18% of all incidents. However, the rate of credential theft incidents nearly doubled in 2021, a trend that is expected to continue, according to the Ponemon Institute.[6]

> Taking the initial steps to create an insider threat program is not difficult. Most companies have the groundwork already established in their human-resource policies, legal processes, and information-security tools.

From the data, the average company had between 1,000 and 5,000 employees, more than 20 insider-related incidents, and had $15.4 million in costs related to those incidents. Only 12% of companies managed to contain incidents in less than 30 days, while the average incident required nearly three months (85 days) to contain. Using this data, companies should be able to estimate their own potential losses due to insider threats.

Step 2: Evaluate Current Policies

Most companies have policies that pertain to insider-related incidents already in place. However, they often are siloed in different departments, with—for example—human resources having policies for employee misbehavior, information technology having a process for mitigating successful phishing attacks. Knowing what policies your company already has in place is key to kicking off the insider threat program.

Step 3. Evaluate Current Visibility into Insider Threats

Similarly, the toolset and controls available to monitor and prevent workers from inadvertently or maliciously cause damage are equally critical. Companies should evaluate the current security operations centers (SOCs) and their technology for coverage of insider threat techniques. The systems need to able to, at the very least, provide visibility into data-access anomalies, privilege abuse, and changes in employee and device behavior. Better yet, the technology should provide a way to automate a variety of responses.

Step 4. Establish a Holistic Insider-Threat Framework

Using knowledge of the current policies, the available tools, and the most damaging types of attacks, companies should be able to build an initial framework for insider threats that takes an interdisciplinary approach to handling potentially suspicious insider activity.

[6] Ponemon Institute, "2022 Cost of Insider Threats Global Report," p.5.

Employees that mistakenly leak credentials by falling for a phishing attack for example, need to have those credential reset and should be given additional training. Employees that have given notice should be educated on the rules regarding intellectual property and be more closely monitored for anomalous behavior. And, employees status as in-office, remote, or hybrid workers should be part of the evaluation for whether credentials may need additional authentication.

Step 5. Create an Interdisciplinary Policy Group

In conjunction with the initial insider-threat framework, a policy group should be created to evaluate current insider-threat policies and procedures and, if necessary, modify them to account for new information and processes. At the very least, the group should include members from information security, human resources, information technology, the core business group, and the sponsoring executive.

Step 6. Create New Training Materials

With an initial framework in place, the policy group should look to create new training material. Rather than annual training, education efforts should be ongoing. Random phishing tests that lead to educational opportunities will both test employee readiness and further educate workers on the latest risks. Highlighting the benefits of key technologies, such as multi-factor authentication, will lead to greater usage of critical controls and minimize employees' desire to bypass such controls.

Step 7. Determine What Technology Gaps Need to be Filled

The basic technologies needed for a comprehensive insider threat program include:

- **Dashboard for triaging incidents and alerts**—Typically, a security information and event management (SIEM) system is used to satisfy this functionality.
- **Detection of phishing attacks**—E-mail security gateways, endpoint protection systems, and some data loss prevention tools can serve this role.
- **Anomalous behavior detection**—User and entity behavioral analytics (UEBA) systems as well as some network anomaly detection software could satisfy this role.
- **Endpoint detection and response**—To avoid the most costly breaches, EDR can help quickly shutdown an attack or data exfiltration with an automated playbook.
- **Cloud access visibility and controls**—A variety of cloud access controls can help companies gain visibility into how employees are using cloud services and what data is being accessed.

Not Every Industry, or Employee, Is the Same

The most common insider-related incidents vary depending on the industry. Healthcare organizations have a different threat profile than financial institutions, which are different than software vendors. Companies should make sure to create an insider threat program appropriate to their industry's needs and natures.

Companies also need to consider that different employee roles required different treatment under the insider-threat program. Identifying high-risk employees to watch closely is critical. Administrators and privileged users, contractors, workers given layoff notices, and people with access to sensitive data such as human resources or accounting, should all be monitored more closely.

Insider-Threat Programs Are Not Static

Like most processes, an insider-threat program is never complete. Not only will the program change as the company develops more maturity in security processes and knowledge, but threats, regulations, and technologies change over time, requiring re-evaluation of how those factors could impact the program.

Next Steps

For more information on how to get started with an insider-threat program, or how to improve an existing program, see the following resources:

- Stopping insider threats with the ArcSight platform's behavioral analytics
- Guide to protecting source code
- Case study in financial services
- Case study in healthcare
- Case study in online retail
- See it in action—request a demo

Like most processes, an insider-threat program is never complete. Not only will the program change as the company develops more maturity in security processes and knowledge, but threats, regulations, and technologies change over time, requiring re-evaluation of how those factors could impact the program.

Connect with Us

www.opentext.com

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.

763-000010-003 | O | 11/23 | © 2023 Open Text