The Enemy Within: Deterring & Detecting Insider Threats

Produced by the Research & Information Support Center

November 13, 2018

Introduction

Some of the most damaging cybersecurity threats do not originate from malevolent external actors, but from organizational insiders and third parties, whether malicious or negligent. One high-profile recent report attributes more than 50 percent of security incidents to insider threats, while 28 percent of data breaches are insider driven. However, these figures likely reflect the low end of how damaging insiders can be to an organization, as organizations often do not disclose insider actions externally.

It is often extremely difficult for organizations to detect and thwart an employee with legitimate access. On the other hand, an organization can often detect or control outsiders' attempts to access data, either physically or electronically, and can mitigate the threat of outsiders stealing company property. Insiders, however, have a knowledge of systems and data and can operate with minimal scrutiny, which enables them to inflict substantial damage. Insiders may steal solely for personal gain, for revenge, or for the benefit of another organization or country. Employees may also take proprietary information when they believe they will be terminated or are searching for a new job. Domestic or foreign business competitors or foreign governments attempting to acquire proprietary information and trade secrets illegally have recruited or placed spies into targeted companies. Consequently, the internal theft of intellectual property is an increasing threat to organizations and can go unnoticed for months or even years.

To reduce the risk from insider threats, organizations need to turn security inside out, building a strong security culture with organization-wide collaboration and employee buy-in. The following report describes the threat posed by insiders, highlights the importance of physical security personnel cooperating with information technology (IT) teams, and advocates a three-pillared approach based on deterrence, detection, and mitigation.

Who are Insider Threats?

An insider threat is a person within an organization – a current or former employee, third party contractor, or business partner – who has or had authorized access to an organization's networks systems, data, or premises, and uses that access to compromise the confidentiality, integrity, or availability of the organization's information or systems, with or without malicious intent. Insider threats include fraud, intellectual property (IP) theft, corporate espionage, and IT infrastructure damage. Due to the insider's legitimate access and knowledge of organizational networks and data, this is one of the chief security threats to the private sector. The proliferation of sensitive data, excessive access to data, complex technology, growing demand for sensitive information, and lack of employee awareness all exacerbate the threat posed by insiders.

Know Your Enemy and Yourself

Not all insider threats are malicious; some incidents result from honest mistakes or careless actions. However, all of the following actors could be considered insider threats.

Malicious actors may be:

- Disgruntled: this person, who either quits or is terminated, takes information with them when leaving an organization. They do this to elevate their standing at a new employer, help a new employer outperform their previous organization, or to sabotage their previous employer.
- Entitled: this person takes information or work-related products with them that they believe belongs to them and should be able to keep. The intent may not be malicious, but the act is intentional and can be damaging.
- Planted: this person is planted or recruited by an outsider, whether a state-sponsored actor, organized criminal group, or rival organization. These individual, who may act out of greed, ideology, or divided loyalty, look to steal data and intellectual property for their handler while remaining employed.
- Advanced Persistent Threat (APT): this is a state-sponsored external group that can masquerade as an insider. APTs use stolen user credentials, unbeknownst to the authorized credential holder, to emulate an insider and mask their movements, while identifying and exfiltrating desired information.

ONLINE TRAINING RESOURCES

National Counterintelligence and Security Center:

- Insider Threat Training

Center for Development of Security Excellence:

- Insider Threat Awareness Training
- Establishing an Insider Threat Program for Your Organization
- Insider Threat Toolkit

Non-malicious actors may be:

- Negligent: this person loses equipment or documents or falls victim to social engineering, like a phishing email. Negligent employees are the most common threat; according to a 2016 survey, they were reportedly responsible for 68 percent of security incidents. In addition to falling for phishing emails, these employees also exhibit weak password security or bad password sharing practices.
- Inadvertent: this person unintentionally transmits data that they should not have. This could include sending an email with personal information to an incorrect address or distribution list.

Other actors:

- Third parties: these contractors and vendors pose a significant threat because they have access to an organization's network and information. They can cause security incidents through both malicious and inadvertent actions.
- Privileged users: these individuals have a trusted role in an organization and can use their access to maliciously attack. Outside actors target these users because of their extensive access, through which they could unwittingly become a threat due to negligent actions.

According to a 2018 survey, organizations indicated that the insiders that posed the biggest security threats were regular employees (56%), privileged IT users or admins (55%), and contractors or security providers (42%). As there are a wide array of potential threats, there are a variety of motives or personal

factors that drive these insiders to commit a malicious act against their organization. These motivations include money, revenge, ego, job uncertainty, ideology, emotional instability, divided loyalty, coercion, or simple negligence. No matter who the actor is or what their motivation may be, there are a number of steps that organizations can take to deter and detect the threat and prepare to respond. Failing to prepare properly will make mitigation and remediation more costly.

CASE STUDY: EXPLOITING THIRD PARTIES

In November and December 2013, intruders stole data from more than 40 million credit cards and the personal information of 70 million customers from approximately 2,000 Target stores via compromised point-of-sale systems. While this data breach provides a number of information security lessons, the initial intrusion of the Target network succeeded through a third-party vendor security lapse.

Two months prior to the breach, a malicious phishing email containing malware was sent to a Target HVAC and refrigeration vendor. The vendor's system was then compromised by a banking Trojan, enabling the hackers to steal credentials to access Target's online vendor portal. Due to network segmentation vulnerabilities, the hackers were able to gain access to other parts of Target's network, including locations with sensitive data. The attackers used their network access to install malware into point-of-sale devices, which read and recorded the information on scanned payment cards.

The cost of the breach was significant. Target executives, including the CEO and CIO lost their jobs, and the company spent hundreds of millions of dollars to refund money stolen from customers, replace affected cards, and settle numerous lawsuits, all because the exploitation of a negligent third party initiated a series of events that culminated in a substantial and costly data breach. To avoid falling victim to a third party vulnerability, organizations should avoid publicizing lists of vendors, limit vendors' system knowledge or access, restrict outside access unless coming from an approved network or VPN, require multi-factor authentication for vendor log-in, and train third parties on vulnerabilities like phishing and outdated software.

The Cost of Insiders

Not only do insider threats pose a security risk to organizations, but the damage resulting from their actions can be extremely costly. According to a 2018 report on the cost of insider threats, 159 benchmarked organizations reported 3,269 insider incidents over a 12-month period. The average total cost of insider security incidents was more than $8 million, with costs including monitoring and surveillance, investigation, escalation, incident response, containment, post-incident analysis, and remediation. Negligent insiders, the most common threat identified in the report, had the highest average annual cost ($3.81 million) of the three analyzed threat categories, but the lowest average cost per incident ($283,281). Attacks resulting from stolen credentials, the least common threat vector identified, had the highest average cost per incident ($648,845) but the lowest average annual cost ($1.96 million).

Incidents resulting from malicious insiders had an average per incident cost of $607,745 and an average annualized cost of $2.99 million. These costs reflect the impact and probability of events, as insider negligence is the least expensive type of incident, per event, but happens with more regularity, while infrequent credential compromise has the largest impact.

However, beyond these costs, organizations must assess the other consequences and costs that follow an incident: the cost of lost sensitive, personal, or financial data or intellectual property; the installation of malware; lost revenue from disrupted business productivity; cost of damaged equipment or assets; legal or regulatory costs; and diminished brand reputation and consumer trust. The potential costs and consequences that result from insider attacks far outweigh investment in an insider threat program.

Developing an Insider Threat Program

Insider threats are difficult to prevent because with legitimate physical and electronic access, malicious actors have already bypassed initial access controls. Insiders know the networks they are accessing, and it is difficult for security personnel to determine if users are accessing information for legitimate job functions or for malicious purposes; actors can therefore cover their tracks and go undetected for long periods. One report concluded that it took an average of 73 days to contain an insider incident, and only 16 percent of incidents were contained in less than 30 days. However, organizations can take a number of steps to minimize the threat and prepare a proper response.

An initial step to protecting an organization against internal and external risks is to develop a clear and documented set of information security policies and procedures. An organization-specific, risk-based security policy should incorporate an insider threat program, which should be actionable, sustainable and seek measurable results. This program should approach security holistically, as insider threats are a "people problem," not an IT problem; it should include actions to deter, detect, and mitigate threats. The program should:

- Identify critical assets and levels of exposure;
- Cultivate lines of communication and collaboration across multiple organizational units; and
- Establish baselines on activities like work schedules and data transfers, determine what is outside the norm, and then identify individuals that deviate from the established boundaries. Draw data from the organization's cross-functional group, including physical security, human resources, legal, IT, medical, and regular employees.

The Role of Physical Security Personnel in Deterrence and Detection

An organization's physical security team is as important as, and a necessary compliment to, technical security. According to a 2018 report on data breaches, 11% of the tactics used involved "physical actions." Other tactics included hacking, social engineering, negligence, privilege misuse, and credential theft, in all of which physical security personnel could play a mitigating role. Neglecting the role of physical security in insider threat programs leaves a significant threat vector unprotected; a holistic security approach can identify risk indicators before a costly incident occurs.

Screen new hires

Physical security teams, working individually and in collaboration with other organizational units, can assume several responsibilities to prevent insider attacks. Security personnel can screen new hires and conduct background checks to identify red flags. Potential insider threat indicators include:

- Substance abuse or addiction issues;
- Financial changes (unexplained wealth or excessive debt);
- Established disregard for security procedures; and
- Disgruntlement with previous employers.

However, pre-employment screening only provides a single snapshot in time regarding an individual's behavior. Some organizations monitor employees on an ongoing basis to look for new indicators, such as an employee being arrested or declaring bankruptcy. While the existence of red flags is not necessarily disqualifying for employment, they could indicate that an employee is under a worrying level of stress, which could serve as the impetus for malicious actions.

CASE STUDY: SPYING FOR A NATION-STATE

Gary Chung was a Chinese-American engineer that worked at Rockwell and then Boeing. Chung worked as a structural engineer on a number of government contracted projects, including NASA's space shuttle program. He also spied for China for nearly 30 years, providing the Chinese government with information on the space shuttle, rockets, and U.S. military jets and helicopters to "contribute to the motherland." During this time, Chung stole hundreds of thousands of unclassified technical documents from his employers and passed them to Chinese handlers.

Chung printed documents of interest to China from his employers' databases, whited out warnings against outside distribution and printer timestamps, re-copied the documents, and took them home in boxes. At one point when the company was moving offices, Chung took dozens of boxes of documents from the office and sent relevant information to the nearest Chinese consulate. Chung also traveled to China for several weeks at a time to meet with his Chinese handlers, under the guise of giving lectures and meeting with academics or researchers.

In 2009, Chung was the first American ever convicted for economic espionage. A number of potential red flags could have alerted security officials to his actions. Chung accessed and printed information from outside of his area of responsibility, carried boxes of documents out of the office, took a several multi-week trips to China, and accumulated wealth -- more than $3 million in assets -- which likely exceeded what could have been expected from his modest salary.

Observe employee behavior

Security personnel and regular employees should also observe the behavior of other employees. The identification of high-risk indicators is a key component to preventing insider threat issues. Behavior that could trigger enhanced scrutiny include:

- Inappropriate information handling: an individual takes sensitive data out of the workplace without need or authorization, inappropriately asks about compartmented information and seeks access to sensitive data, unnecessarily copies material, or disregards security policies for software or hardware;
- Unusual work / travel schedule: an individual remotely accesses networks while sick, on vacation, or at odd hours; works odd hours without authorization or shows enthusiasm for overtime or weekend work when clandestine activities would attract less scrutiny; or takes unreported or frequent overseas travel; and
- Personal conflicts: an individual has excessive debt or unexplained affluence, is overwhelmed by life crises, takes unusual interest in the lives of coworkers, or has an unexplained drop in performance.

Potential insider threats may also be concerned that they are under investigation, and attempt to detect scrutiny. If a person exhibits any of the identified risk indicators, security personnel could conduct a follow-up screening or enhance monitoring of the individual's activities.

Train employees

Employees are an organization's first line of defense, and the key to deterring and detecting insider threats. Educating employees by incorporating insider threat awareness into mandatory organizational training is vital for security. Employees should receive training to understand insider threats, to identify the above risk indicators, and to report observed behavior appropriately. Organizations should internalize the security mantra, "See something, say something."

The workforce should be educated not just on which behaviors are acceptable and which are not, but why specific policies and restrictions are in place. This approach illustrates the techniques and tradecraft that malicious actors may use and alerts employees to behaviors that are outside of the norm. Employers should also train their staff in properly identifying, handling, and protecting sensitive or proprietary information.

Secure facilities

Security personnel, in coordination with IT personnel, can maintain facility security and physical asset management. This responsibility includes identity management and establishing user access controls. Personnel should verify that workstations are secure and monitor information that leaves the facility. Security personnel can work with IT to implement technical restrictions, including prohibiting the use of USBs, external drives, or other device plug-ins, blocking unauthorized Internet downloads, and restricting access to certain downloads.

Disgruntled employees seeking revenge or entitled employees looking for a competitive edge at a new employer may attempt to take data just prior to or at the point termination. To prevent unauthorized data removal, security should restrict the employee's physical and IT access at termination, take ID badges, and escort the individual from the facility. In coordination with IT, organizations should monitor data flows prior to employee departure and remove the individual from email distro lists.

Physical security personnel can work to identify threats before they begin by maintaining disciplined hiring practices, conducting thorough background checks, implementing continuous monitoring, training all employees, and monitoring physical security. All of these steps should be in collaboration with groups from across an organization, including executive leadership, business process owners, and risk management.

Legal implications

When combatting insider threats and implementing a threat program, organizations must design and implement all policies and procedures with careful considerations paid to relevant legal and regulatory frameworks, ensuring they comply with the laws of the jurisdictions in which they operate. Relevant regimes include European Union's General Data Protection Regulation (GDPR), United States' Electronic Communications Privacy Act, and the many laws that protect individual privacy. Organizations must also consider national state secrecy laws, where the state has control of sensitive technical or communications information. These laws, which exist in countries like China and Russia, influence how organizations implement business and security frameworks. The implementation of critical security frameworks is essential for organizations to protect sensitive information, but compliance with all applicable laws remains key.

CASE STUDY: FORMER EMPLOYEE EXPLOITING NETWORK ACCESS

In 2013, Jason Needham quit his job at an engineering firm to open his own company. After he left, he continued to access his former employer's file-sharing network and email accounts for nearly two years, accessing and downloading hundreds of documents, including engineering schematics and project proposals and budgets reportedly worth $500,000. In 2017, Needham was sentenced to 18 months in prison and ordered to pay $173,000 in restitution.

Upon termination, Needham had his credentials terminated. However, he continued to use the compromised credentials of a former co-worker to access an email account, which he used to view other sensitive data. While the employer correctly severed Needham's account credentials, it could have used tools to monitor potentially compromised accounts, implemented multi-factor authentication for logins, or installed data-loss protection technologies to identify an outside IP address that was abnormally accessing the network to download data.

Collaboration with Organizational Partners

A control framework is the set of safeguards, separation of duties, recommended actions, and technology adaptation that the IT side of an organization uses to minimize security threats through deterrence, detection, and analysis. Physical security personnel should work with IT and other security stakeholders in an organization to ensure that a sufficient control framework is in place to mitigate insider threats.

There are numerous technical solutions and best practices for deterring, detecting, and mitigating the threat from both internal and external threats. Deterrence methods, which include establishing security policies and data encryption, should also include access controls. All organizations should implement the principle of least privilege, which is applicable to physical and digital security. Individuals or third parties should not receive access to networks, data, or physical spaces unless it is necessary to perform their job function. With fewer people gaining access, fewer potential malicious actors or negligent employees will have the opportunity to compromise accounts. Enforcement is possible through identity and access management, network segmentation, and activity monitoring.

Detection platforms, which include user monitoring and data-loss protection mechanisms, can alert security personnel to unauthorized data transfers. These mechanisms cover data that is printed, sent via email, and copied to the cloud or removable drives, while physical security retains responsibility for monitoring the physical removal of information. Detection platforms should also incorporate intrusion detection and prevention (IDP). Log management and security information and event management (SIEM) assist with detection and the analysis that occurs in the aftermath of a security incident. Advanced technologies such as predictive Artificial Intelligence (AI) and behavioral analytics support these capabilities and enhance and organization's security posture. The use of deterrence and detection tools can reduce the frequency and cost of security incidents.

Additional Information

Malicious and non-malicious insider threats likely already exist within your organization. Developing a security culture with established policies and procedures to deter, detect, and mitigate those threats will minimize the frequency and impact of security incidents.

However, cyber threats, including insider incidents, are a growing concern. If your organization has a cybersecurity incident, whether past, ongoing, or threatened, you can contact the federal government for assistance. Government agencies have the tools and experience to investigate the potential threat and assist in the safeguarding of your sensitive information. Your organization can report issues to the FBI, DHS, and local law enforcement.

Contact:

- FBI Field Offices
- Internet Crime Complaint Center (IC3)
- Secret Service Field Offices
- National Cybersecurity and Communications Integration Center (NCCIC); NCCIC@hq.dhs.gov; or (888) 282-0870

For additional information regarding insider threats or other information security issues, please contact OSAC's **Cyber Analyst**.