exterro®

WHITE PAPER

Best Practices for Insider Threat Mitigation

Detecting and mitigating against insider threats is one of the most difficult challenges for companies, organizations, and governments. This is partially due to the fact that insider threats is a very misunderstood problem, filled with many assumptions that are in some cases inaccurate or untrue.

This guide provides insights into best practices that have been learned from challenges people have encountered while developing, managing and enhancing their Insider Threat Programs (ITP). This guide will serve as an accurate and in-depth resource for understanding and mitigating insider threats.

Tips For Your Organization's Insider Threat Mitigation Program

Always assume that serious insider threat problems already exist in your organization.

Effective communication and collaboration with key stakeholders across different departments (security, HR, IT or network security, etc.) is critical to insider threat detection and mitigation. A lack of communication between key stakeholders can lead to blind spots and the inability to create an accurate snapshot of potential and actual insider threats.

Familiarize yourself withindustryreports to gauge your organization's susceptibility to insider threats.

An insider threat can be anyone with the right access, intentions and motivations to fulfill their objectives. It does not matter what the size of your organization is. Every organization is susceptible to insider threats. Most industry surveys and reports are focused on computer or network insider threat related incidents, and leave out other very damaging areas such as insider threat fraud.

Additionally, since the definition of insider threat can vary, *how* insider threat incidents are categorized and reported can lead to inaccurate reporting.

There is a consensus among insider threat mitigation (ITM) experts that many insider threat incidents are not reported. Why? An organization that prosecutes an employee will most likely appear in public court records. Some organizations, especially businesses do not disclose publicly or pursue criminal charges for this reason. What types of insider threats should you be on the lookout for? See the list for examples.

Be aware of unintentional insider threats.

Unintentional insider threats can be just as costly and damaging as Malicious Insider Threats.

In 2018 McKinsey & Company reviewed the VERIS Community Database. The database contains about 7,800 publicly reported breaches from 2012 to 2017, to identify the prevalence of insider threat as a core element of cyber attacks. The research found that 50% of the breaches studied had a substantial insider threat component. What's more, it was not mostly malicious behavior. Negligence and co-opting accounted for 44% of Insider related breaches.

Examples of insider threats:

- New employees bringing in stolen information from their previous employer
- An outsider with connections to an insider in the organization
- Employee threats (includes contractors and trusted business partners)
- Disgruntled employees or job jumpers
- Divided loyalty or allegiance to U.S. or terrorism espionage (national security, economic, industrial, corporate)
- Data theft, data destruction, information technology sabotage
- Embezzlement, fraud, theft
- Insiders who are unwitting, ignorant or negligent
- Phishing (credential theft—cyber criminals become insiders)
- Cyber criminal—insider threat collusion
- Nation state sponsored insider threat
- Insider threats during mergers & acquisitions
- Company down sizing, reorganization
- Workplace Violence (bullying, sexual harassment)

Think of an insider threat program as Security 2.0

Creating an insider threat program is a new appraoch to insider threat mitigation but it's not necessarily new. Focus on reevaluating and improving the security culture and posture of the organization through positive incentives and encouraging employees to take security more seriously. Has the organization considered implementing a Security Vulnerability Rewards Program?

Insider threat mitigation involves the whole organization

Insider threats are an organizational and human problem that must be addressed from the top of the organization on down. There are many different factors that contribute to the insider threat problem and understanding these factors is essential for ITM. The policies, procedures and business processes of various departments (security, human resources, IT or network security, etc.) must be evaluated to ensure they are robust and effective for mitigating insider threats.

Get employee buy-in

Employee buy-in is essential for an ITP. Employees should understand the importance of the ITP, it's purpose, and how it protects everyone (employee safety, organization survivability, etc.) Organizations should communicate the ITP to the workforce via a formal ITP policy and employees must be made aware of their responsibility to report employee behavioral indicators of concern in a secure and protected manner.

Benchmark, improve and update

Managing an ITP is continuous process. An ITP needs to adapt and adjust to an organization and its security culture. You may need to tweak or enhance your ITP periodically to ensure it is robust and effective. Conducting benchmarking and an ITP maturity assessment against other organizations ITP, is a very good way to see how well your ITP stacks up against others.

Consult with Legal

There are many laws related to employee privacy, monitoring and legal considerations or concerns for ITP's. It is very important that your organization consult with an attorney that specializes in "legal considerations" for ITP's. Ensure your organization has legally sound processes and procedures to collect, integrate and analyze various data sources for potential or actual insider threats.

NDAs and Codes of Ethics

All individuals managing or supporting an ITP should sign a Non-Disclosure or Code Of Ethics Agreement specific to the ITP. Also the ITP Manager and those supporting the ITP Working Group (ITPWG), should be given appointment letters. These appointment letters should clearly define the roles, responsibilities and lanes in the road for individuals supporting the ITPWG.

Don't rely solely on background checks

Background checks are a point-in-time snapshot of an employee. Gathering and analyzing internal data sources is very important for insider threat detection. Equally important is knowing what external data sources are also available to create the big picture of potential or actual insider threats.

To be more proactive in detecting and mitigating Insider Threats, many organizations are using post-hire solutions that allow the employer to continuously monitor an employee for indicators of concern. With these solutions, organizations can proactively identify employee risk and preemptively address a problem before it escalates.

Network Security and Employee Monitoring ≠ an ITP

Relying on just user activity monitoring, behavioral analytics, SEIM and DLP tools for insider threat detection, is a reason organizations still have insider threat incidents. Insiders can use other methods for data exfiltration that these tools won't detect.

Also, only focusing on employee network behavior ignores a large portion of the employee work-life picture. External employee stress related factors, combined with Internal stress and disgruntlement factors, many times fuel the fire to ignite the employee.

Conclusion

It's important that you don't underestimate how damaging an insider threat incident can be to your organization. Below are a few impacts an incident can have on an organization:

- Financial loss
- IT or network sabatoge, data destruction (downtime)
- Data breach—loss of intellectual property, trade secrets, sensitive business information (PII, customer contacts, etc.)
- Loss of physical assets (computers, inventory, etc.)
- Reputation loss; loss as a leader in the marketplace
- Workplace violence
- Company goes out of business

INSIDER THREAT DEFENSE GROUP

Thank you to Mr. Jim Henderson, CEO of the Insider Threat Defense Group (ITDG), and Founder and Chairman of the National Insider Threat Special Interest Group (NITSIG) who developed this guide.

Conduct remote and covert investigations at every endpoint.

Expose and investigate a variety of criminal and malicious activities, including data breaches, database tampering, inappropriate sharing of confidential company information, deletion of files, wiping of hard drives, or viewing of inappropriate content. Discretion can be critical when conducting investigations, and FTK® Enterprise ensures that employees and teams aren't tipped off as you cull through data.

TO LEARN MORE ABOUT THE EXTERRO FTK ENTERPRISE SOLUTION, REQUEST A MEETING

CLICK HERE

exterro®