WHITE PAPER

Combating the Insider Threat

Guidance from NIST and the National Insider Threat Task Force

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

Insider cybersecurity threats are much more prevalent than most of us realize. IBM estimates that 60% of all cyber-attacks are perpetrated by those with insider access[1]; McAfee cites enterprise insiders as a major source of Personally Identifiable Information (PII) sold on the dark web[2], particularly in the healthcare industry; and at least two-thirds of major corporations reported insider threat incidents in 2016[3] ranging from file theft and destruction to selling passwords and deliberately sabotaging critical systems. Over 40% of U.S. government agencies report such incidents every year[4]. It's a serious—yet incredibly overlooked—risk.

Employees turn malicious for a variety of reasons. Some are disgruntled and respond by acting out electronically against their co-workers and employers. Others have personal or financial problems outside of work that trickle into the workplace and manifest themselves in destructive behaviors, including those who may be bribed or otherwise financially incentivized to sell credentials or other information. Others are simply thrill-seekers who might enjoy file theft or system sabotage—as research in cyber psychology shows, we're likely to behave more recklessly online than we are "IRL."

There are many aspects to addressing and combating these insider threats within both the private and public sectors[5]. Much like anything in security, there is no "silver bullet" that will instantly and irreversibly thwart all risk. Instead, securing an enterprise against insider threats involves a comprehensive and multi-pronged approach that includes monitoring, active threat identification, training, a corporate security culture and more.

While organizations vary in their approach and prioritization of insider threat prevention, best practices are continually evolving as the nature of threats evolve. Organizations such as NIST and the National Insider Threat Task Force are just two resources that are continually evolving guidance on the topic. In its latest revision (Rev 5) of Special Publication 800-53, NIST provides a mapping of security controls for implementing an insider threat program, applicable for both Classified and Unclassified environments. NIST's Cybersecurity Framework is another tool that enables senior leaders in particular to frame and ultimately manage their enterprise insider threat risk.

The National Insider Threat Task Force, established under Executive Order 13587, recently updated its *2017 Guide: A Compendium of Best Practices to Accompany the National Insider Threat Minimum Standards* that specifically focuses on six major categories of the U.S. government's National Insider Threat Minimum Standards: Designation of a Senior Official(s); Program Personnel; Access to Information; Employee Training and Awareness; Monitoring User Activity on Networks; and Information Integration, Analysis, and Response[6].

While nothing is ever perfect, these and other insider threat guidance sources indicate that when properly integrated, the use of a few basic insider threat program building blocks can form a powerful combatant to insider cyber threats.

User Activity Monitoring

User activity monitoring is one of the basic building blocks of any insider threat program. So, why user monitoring? Certainly, employees don't like being included in their own organization's threat profile, and it may be equally uncomfortable on the management end. "Surveillance"[7] in the workplace is also a contentious issue in and of itself, whether tracking email conversations, device logs, or Internet search histories. Nobody likes being distrusted—particularly on paper (and in code).

Combating threats from inside an enterprise, however, is impossible if you're not looking for them in the first place. Just as passing on a perimeter firewall would be negligent in the face of external hackers, so too would be skipping over user monitoring. This may raise some complicated questions, but user monitoring programs are necessary.

First, organizations should monitor employees' Internet behavior on a patterned basis all the while looking for strange activity. Data analytics is helpful in this regard. If you observe any outliers, such as connecting to unknown or foreign IP addresses, those incidents should be flagged and reported. The same goes for when employees log on remotely; if an accountant who never works from home begins sending data requests in the middle of the night, something might be awry.

NIST CSF-Insider Threat

Identify	Protect	Detect	Respond	Recover
Asset Management	Prevent Incursions	Detect Infections	Contain Infestation	Return to Normal
• Asset Management • Governance	• Asset Control • Awareness and Training • Data Security • Information Protection Processes & Procedures	• Anomalies and Events • Security Continuous Monitoring • Detection Processes	• Analysis • Mitigation • Improvements	• Recovery Planning

Attributable Events Indicating Violations of System/Target:

» Malicious code detection
» Unauthorized local device access
» Unauthorized executable
» Unauthorized privilege access
» After-hours privileged access
» System reboot/reset
» Disabling the audit mechanism
» Downloading to local devices
» Printing to local device
» Uploading to local devices

Fig. 2 Credit: CNSSI 1015, Appendix B, p. 42 of ODMI Guide
www.dni.gov/files/NCSC/documents/nittf/NITTF-Insider-Threat-Guide-2017.pdf

Security teams should also watch for strange downloads and file transfers as well, particularly for users who have access to PII[8] and other sensitive enterprise information (i.e. classified data, financial data, or intellectual property documents). As you investigate these incidents and pinpoint their causes, use this information to improve your monitoring and analytics.

Volumes of activity can similarly provide valuable insight. It's certainly true that some users may work remotely or visit strange IPs as part of their job. But sudden or dramatic increases in that activity itself (like excessive printing, file downloading, and after-hours access) should set off alarm bells. And again, this monitoring should run on a mix of technical and human work. For instance, if you set a printing threshold that employees know about, it would take a human observer to notice that an employee is printing just under the threshold every single night.

User monitoring still carries over to after an employee's departure. In addition to "freezing" old accounts (so login attempts won't work), place flags on old credentials as well. Employees who are laid off or terminated may choose to sell their usernames and passwords online or attempt to sabotage company systems from afar. This type of activity should be actively monitored for.

Of course, all of this monitoring isn't too helpful without rapid-response capabilities. Being able to quickly terminate IP connections, lock down accounts and end file transfers mid-execution are all essential to not just detecting—but preventing—insider threats in real time.

Further, it's critical to document any insider threat evidence collected through this monitoring. In order to prove an employee to be an insider threat—and potentially prosecute them in a court of law—there needs to be clear, meticulously-kept evidence. This is another value added by monitoring.

So, remember: as with most cybersecurity threats faced by a modern enterprise, threats don't just need to be identified and flagged, they need to be quickly and aggressively combated by the entire organization. It's just another part of a comprehensive security posture.

The Technology

While monitoring cyber behavior is vital to combating insider threats, it won't stand on its own—systems, applications, data, devices and other digital services should be technically secured and monitored against malicious insider activity as well. This poses a number of challenges.

Traditional defense mechanisms fail against insiders. Perimeter firewalls, intrusion detection systems and multifactor authentication standards are meaningless against an adversary who has active and legitimate access to systems and information. They are already inside the cyber boundaries laid by conventional security software, which increases the likelihood of slipping through the cracks and causing considerable harm.

Further, even if we do monitor the activity on a user's account, there are challenges in discriminating between normal and abnormal behavior so change management is critical. The integrity of the files is critical for true network situational awareness. If an encrypted file is read dozens of times a day by an accounting team, will the system notice if someone outside of accounting decrypts the file? What about a malicious[10] insider *within* accounting—would they be detected? How do we distinguish between legitimate file transfers and non-legitimate ones? What about using USB sticks legitimately (i.e. backing up presentations for a business trip) versus maliciously (i.e. installing malware on company systems)?

Continuing in this vein, ideal policy solutions to these problems may be impractical. For instance, it might be convenient to block all Internet downloads including email attachments, but this last point would massively impair organizational communication. It might also be desirable on some level to prevent employees from bringing their own devices[11] into work—but again, this may result in the same inconvenience; imagine a visual design company prohibiting iPads. (Some policies, such as banning USB sticks, might in fact be possible.)

In short: insider threats are complicated not just from a monitoring perspective, but from a technical security perspective as well. Employees should be treated equally, though this makes it hard to know who (if anyone) is a malicious insider. As a result, we need robust IT protections and robust risk mitigation protocols to complement other defenses.

Support from IT Security Solutions

Focus heavily on user access control. Set default account privileges to the minimum needed for daily tasks, and then adjust those privilege baselines between departments and roles. IT staff will likely need higher permission levels than accounting personnel, to use just one example, although they likely shouldn't have access to client financial information. Similarly, if an employee needs elevated access for a temporary project (i.e. security testing), their access should be revoked as soon as the project ends; their increased privileges should be officially documented; and this should then affect how their activity is monitored—both logistically and rigorously.

Encrypt data with industry-grade protocols, mitigating the potential damage caused by an employee stealing information or selling credentials. Block file deletion in almost all circumstances, and make sure heavy backups and redundancies are in place. If a single angry IT employee[12] can irreversibly delete critical business documents... that's asking for trouble. Similarly, place clear restrictions on who can modify which files and under what circumstances. Identity-based access control, true change management and the ability to record an unauthorized action are the best defense for all around risk management and mitigation.

Prohibit users from running non-whitelisted executables, particularly when they're loaded off of CDs or thumb drives. Block strange IP connections and known malicious websites, restrict Internet downloads, prevent remote printing (i.e. sending documents from work to a device at home), and prevent unencrypted remote logins to your system. Additionally, don't let users modify network logs, prevent employees from disabling or altering antivirus programs, and don't make multifactor authentication an option that users can turn off. These will only strengthen enterprise security against malicious insider behavior.

Again, establish robust monitoring protocols to flag such incidents. Security and management personnel need real-time information in order to quickly contain insider threats, and only well-refined feedback loops will ensure this fact. After employees are terminated, for instance, immediately deactivate their login credentials. If employees switch jobs or departments, re-evaluate and reclassify their digital privileges. If contractors need system access, rigorously monitor and scrutinize their cyber behavior—and so on and so forth.

We could continue on about technical protections against insider threats, from purchasing forensic toolkits and malware removal software to conducting system audits and creating "honeypots" to trap both technical and nontechnical threats. It should be clear, though, that without a completely-integrated approach to insider threats, enterprise organizations will fail to achieve a robust cyber security posture. Security needs to be a holistic effort.

Aligning Human Behavior to an Insider Threat

While "regular" insiders may turn malicious for a variety of reasons, rarely do these causes originate in cyberspace; instead, it's often the physical world that produces the trigger. It is therefore essential to monitor employee behavior outside of the cyber domain to better inform threat mitigation. (Many insider threat programs refer to this portion as "continuous and persistent surveillance.")

Technology lowers the barrier to malicious insider activity. Stealing files on a USB drive, for instance, is less intimidating than stealing folders from a filing cabinet, just as posting credentials on a website is easier than breaking into a locked office. Our risk perceptions are also fundamentally skewed in the cyber domain; because we lack a cyber lexicon and a historical understanding of cyberspace, our ability to reason logically and rationally is seriously inhibited the moment we're in front of a screen. Those already at risk for physical malicious behavior are at an even higher risk for its digital counterpart, and those who normally might not act out can now pose a threat.

Solutions for Preventing Insider Threats

Monitor for issues outside of the workplace, taking note of family and personal problems, medical issues, financial challenges, and social media posts that are outside the norm. Supervisors, HR professionals, and counterintelligence/security staff in particular should pay attention to gradual changes in home and life situations. When a change is noted, this behavior will put the subject into a higher risk category for additional monitoring.

Don't forget: when it comes to insiders, it's more often a slow shift towards malicious behavior than a sudden "snap." Financial problems are particularly relevant, as they (obviously) affect an employee's risk of accepting bribes or selling information online—and tend to come on gradually. However, the same could be said for personal issues like divorce, medical issues like a sick family member, or workplace disciplinary issues like a poor performance review. Insider threats are motivated by a complex variety of reasons, but the causes are more observable than we might think.

Begin this monitoring as early as the hiring process. Job candidates with histories of impulsive or destructive behavior should immediately raise flags during the search process. Particularly when it comes to cyber, perpetrators of malfeasance or misbehavior are quite likely to repeat that behavior. Pay similar attention to contractors, about which there may be less directly available information.

Also, monitor for employee issues within the workplace. Are employees disgruntled? Do they argue with co-workers? Are they suddenly underperforming or missing deadlines? Are they inexplicably absent for prolonged periods of time? These are just some behavioral warning signs that something may be wrong.

The same diligence applies to changes in employment status. Demotions, transfers, pay deductions and terminations all temporarily elevate a given employee's risk. Remember that an insider doesn't actually have to be getting fired for them to pose an active threat; the mere perception of termination, demotion or the like can be enough for an employee to act out. It's quite common for employees leaving a company to take destructive action before their last day (i.e. stealing proprietary information or trade secrets).

Of course, saying "monitor insiders" without clear feedback and reporting mechanisms is pointless. So: clearly communicate and consistently enforce security policies[13] and controls. Educate employees on cybersecurity, paying close attention to how you frame related issues. IT employees will understand secure cyber behavior quite differently than the marketing team. Similarly, employees' understanding of security's importance will be different—the former, from a technical or risk management perspective, and the latter, from a public relations angle, to give just one example.

Along with this framing, don't focus too heavily on the risks posed by insiders. While you should educate employees on this issue, excessive repetition of this fact will only foster distrust and undermine attempts at a security culture[14]. Instead, draw attention to how employees can fight this threat; positively frame the need for awareness and assistance, and actively involve them in your cyber defense. After all, it's often one insider who will notice another's strange behavior.

Make reporting protocols robust, well-known, and confidential—and even consider the cost-benefit of anonymous reporting. As reports come in, ensure that technical and human security protocols quickly kick into gear. Meticulously document your investigations and evidence collection, paying special attention to corporate policies and relevant statutes and regulations. And react quickly and responsively to contain active threats. Integration is critical in this respect.

Reporting doesn't just have to be of specific incidents, like someone using another's computer while they're away from their desk. Employees should also be able to report unusual behavior in general. Ego and self-image issues are an important component of the insider threat profile, so arguing with co-workers or strange mood swings are also relevant to this facet of cybersecurity. Remind employees: what they might not think is relevant might, in fact, be very important.

Insider threats to the modern enterprise are a serious risk, but have been considerably overlooked. Government agencies and companies alike must combine technical and human monitoring protocols with regular risk assessments, human-centered security education and a strong corporate security culture if they are to effectively address this threat. When it comes to cybersecurity, situational awareness, change management, constant vigilance and total adaptability are a must. The good news is that the NIST Cybersecurity Framework and other industry resources now provide much needed guidance for organizations seeking to escalate the priority of their insider threat programs.

To learn more about how Tripwire can help protect your business from insider threats visit tripwire.com/products/

References

1 www.ibm.com/security/campaign/guardium-insider-threats

2 www.mcafee.com/us/resources/reports/rp-health-warning.pdf

3 www.accenture.com/us-en/insight-cybersecurity-digital-trust-2016

4 www.symantec.com/connect/blogs/despite-increased-focus-government-insider-threats-not-declining

5 www.tripwire.com/state-of-security/security-data-protection/insider-threats-main-security-threat-2017/

6 Guidance for interpreting these areas and meeting the government's requirements are provided in the *2017 Guide: A Compendium of Best Practices to Accompany the National Insider Threat Minimum Standards*

7 Since certain states prohibit employers from electronically monitoring employees without giving prior notice, relevant state laws should be reviewed prior to engaging in employee monitoring activity and/or policy. For more information on workforce privacy, go to: www.shrm.org/resourcesandtools/tools-and-samples/toolkits/pages/workplaceprivacy.aspx (login required)

8 www.tripwire.com/state-of-security/latest-security-news/240000-federal-employees-pii-potentially-exposed-in-dhs-data-breach/

9 Since certain states prohibit employers from electronically monitoring employees without giving prior notice, relevant state laws should be reviewed prior to engaging in employee monitoring activity and/or policy. For more information on workforce privacy, go to: www.shrm.org/resourcesandtools/tools-and-samples/toolkits/pages/workplaceprivacy.aspx (login required)

10 www.tripwire.com/state-of-security/latest-security-news/240000-federal-employees-pii-potentially-exposed-in-dhs-data-breach/

11 www.tripwire.com/state-of-security/security-data-protection/cyber-security/u2f-next-generation-2-factor-authentication/

12 www.tripwire.com/state-of-security/security-awareness/the-malicious-insider/

13 whatis.techtarget.com/definition/BYOD-bring-your-own-device

14 www.tripwire.com/state-of-security/latest-security-news/fired-employee-demands-200k-exchange-unlocking-data/

15https://en.wikipedia.org/wiki/Security_policy

16 www.tripwire.com/state-of-security/security-awareness/sherlock-holmes-infosec-crowd-5-steps-becoming-security-awareness-mastermind/

Tripwire is a leading provider of security, compliance and IT operations solutions for enterprises, industrial organizations, service providers and government agencies. Tripwire solutions are based on high-fidelity asset visibility and deep endpoint intelligence combined with business context; together these solutions integrate and automate security and IT operations. Tripwire's portfolio of enterprise-class solutions includes configuration and policy management, file integrity monitoring, vulnerability management, log management, and reporting and analytics. **Learn more at tripwire.com**

The State of Security: Security News, Trends and Insights at tripwire.com/blog
Follow us on Twitter @TripwireInc » Watch us at youtube.com/TripwireInc