THE INSIDER THREAT: DETECTING INDICATORS OF HUMAN COMPROMISE

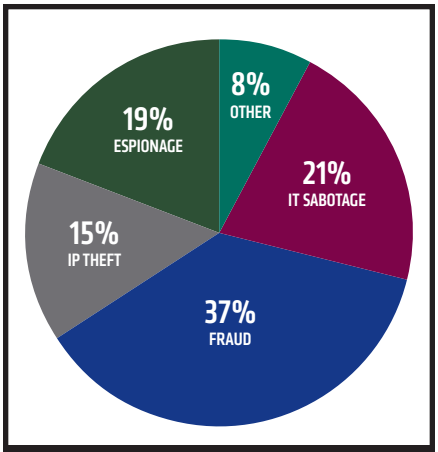
◆ Your organization's greatest asset is also its greatest risk. The employees, contractors and trusted business partners you rely on to keep your organization running can also cause the most damage. A malicious insider can use authorized credentials to do unauthorized things, bring your network down or repeatedly steal data from your organization without being detected. ◆

The malicious insider's motivations can vary, making them unpredictable. The CERT Insider Threat Center has done extensive analysis of the intentions of the perpetrators of insider related cybercrimes and identified four primary goals to their actions:

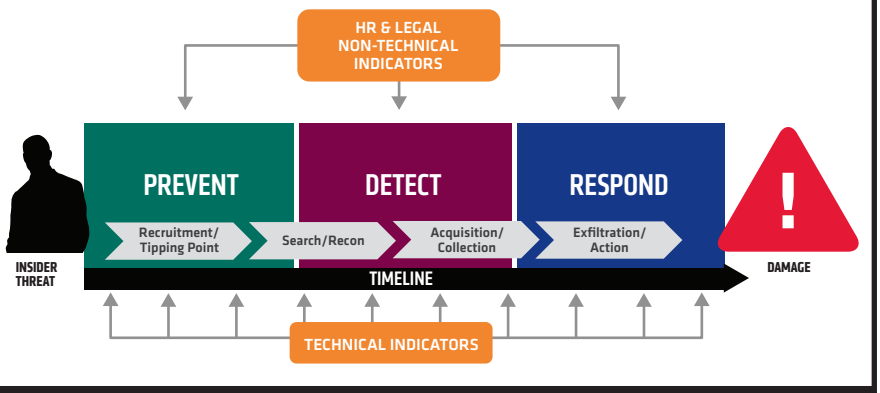
1. Fraud
2. IT sabotage
3. Espionage
4. Intellectual property theft

THE INSIDER THREAT KILL CHAIN

Understanding an insider's intentions provides us with clues in terms of risk indicators of a potential incident. It's rare that an insider chooses to act out randomly, as insider attacks are usually pre-meditated or follow an event that motivates the person to act. Former FBI CISO Patrick Reidy devised what he



◆ **FIG. 1** *CERT breakdown of insider crimes in the US.*



◆ **FIG. 2** *The Insider Threat Kill Chain—attack progression and defense.*

termed the "Insider Threat Kill Chain" modeled after the "Cyber Threat Kill Chain" coined by Lockheed Martin.

The "Insider Threat Kill Chain" deals specifically with a trusted insider—someone who uses authorized credentials to do unauthorized things—versus a remote adversary trying to gain access. The four phases of the Insider Threat Kill Chain consists of Recruitment/Tipping Point, Search & Reconnaissance, Acquisition & Collection and finally malicious Exfiltration & Action. On the defensive side, the actions evolve as the malicious phases progress. The first step is Prevention, where training, security policies and Human Resources plays a critical role, then as the employee moves to actually commit malicious/criminal acts we move into the Detection phase, followed by the Response phase if data is compromised or damage is inflicted on the network.

RECRUITMENT/TIPPING POINT

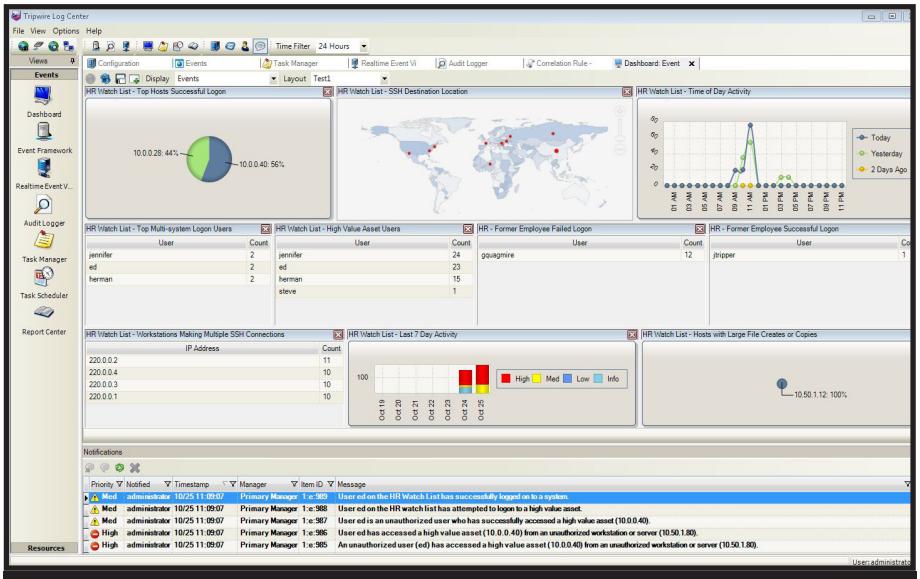
The first phase of the Insider Threat Kill Chain is the Recruitment or Tipping Point. This is the point where the insider turns from good to bad. This can be a case where an employee is passed over for a promotion, or reprimanded by Human Resources for some action. It can also be when an outsider recruits an insider, usually with financial incentive, but also the promise of employment with a competitor.

At this phase the indicators of potential compromise are slight, or at least difficult to detect. An organization's Human Resources and Information Technology teams need to establish clear lines of communication. Any events such as employment termination, resignation, reduction in force, etc. need to be clearly communicated to IT with policies in place to revoke access. Employees who will stay on before exiting the company or those with recent disciplinary actions against them should be monitored or added to an "HR Watch List" through integration with Active Directory or other centralized authentication management systems.

Tripwire® Log Center® provides the ability to add additional logging and monitoring of activities by these users on your network. In addition, regardless of HR status, you'll want to add more detailed logging for any privileged accounts on your network that have access to critical systems or sensitive data.

SEARCH & RECONNAISSANCE

Once an insider has turned bad, the next phase is to begin to search out where they can find data, or weaknesses they can exploit to cause damage to the network if their goal is IT sabotage. Monitoring employee access to sensitive data such as ERP, CRM and marketing



◆ **FIG. 3** *HR Watchlist dashboard creation.*

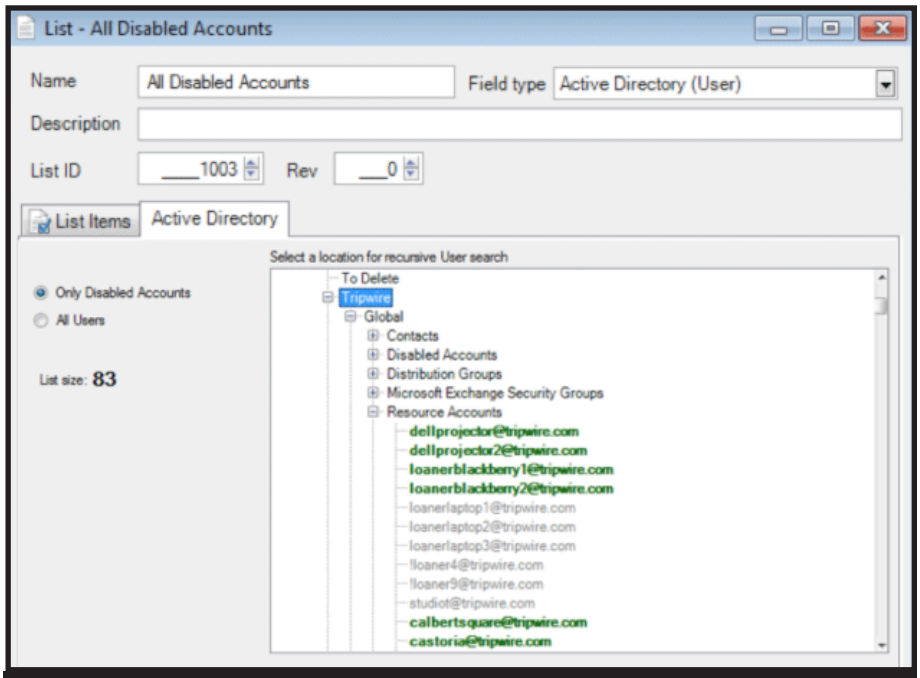


FIG. 4 *Tripwire Log Center Active Directory integration.*

automation systems and database is critical, particularly with employees that have been flagged as high risk. If one of these employees attempts to access systems they are not authorized to access, these failed login attempts can provide an indicator of the insider's intentions.

Tripwire Log Center integrates with operating systems, servers, databases and security/network appliances to aggregate and correlate log and event data, providing you with visibility into what high risk and/or privileged employees are doing on your network.

THE PRIVILEGED INSIDER

When it comes to the technically savvy insider who has privileged access and technical knowledge, they are in a position to do a great deal more damage. They may actively seek configuration and application vulnerabilities in your systems, seeking out ways to further escalate their privileges and access. Many times they will use vulnerability scanning tools to identify weaknesses inside the network, or may modify configuration files to provide a back door into systems after they have left the company.

The Tripwire IP360 vulnerability management (VM) solution provides organizations with the ability to see what the hacker or malicious user with privileged access would see if they were to scan your network from the inside, by continuously monitoring and reporting on system and application vulnerabilities. The Tripwire Enterprise security configuration management (SCM) solution provides visibility into configuration vulnerabilities and changes made to files. The tight integration of Tripwire Log Center with Tripwire IP360 and Tripwire Enterprise provide visibility of insider actions, identifies weaknesses that they could use against you and makes these events actionable with real-time alerts, automation and reporting.

ACQUISITION & COLLECTION

Once the malicious insider has identified data sources they usually begin to collect data in a single location. Flagging large file creation and copies on hosts by suspicious users can provide a key indicator that data is being collected for exfiltration. If this activity is followed by a remote connection to a server outside the organization, or data is copied to removable media device against security policies, you'll want to trigger an alert and report on the incident. In addition to alerting, you'll also want to automatically disable accounts and access to the system to mitigate potential data leakage.

Tripwire Log Center in combination with Tripwire Enterprise can detect these file creation and copying anomalies, and provides the mechanism to alert and initiate actions to take defensive measures to decrease the potential for damage. Tripwire Log Center also provides the ability to monitor connections that are made outside of the organization, as well as identify common ports used for file transfer protocols (such as SSH, FTP or Terminal Services/RDP).

EXFILTRATION & ACTION

When you're able to detect data exfiltration or IT sabotage attempts before they occur, it's still not usually the end of the story. Additional data needs to be collected for forensic purposes, as well as to track what the user did before and after the incident since additional data and systems may have been compromised.

Tripwire Log Center provides the Advanced Log Auditor for this purpose. It empowers investigators to drill through and replay attacks, as well as trace all actions of the perpetrator. Tripwire Log Center's advanced log

collection agent ensures high resiliency so that no logs are lost. It also encrypts and compresses logs for efficient archiving and quick retrieval.

If the malicious insider did cause damage, Tripwire Enterprise provides tools to quickly remediate systems back to a known trusted state. It also provides historical tracking of changes made to system configurations for further forensic analysis.

CONCLUSION

Managing the risks an insider threat poses to an organization requires a combination of people, process and technology. Although it may seem like an impossible task to mitigate damage caused by insider, there are usually indicators that can identify potential risk before an incident occurs. By aligning communication and policies between Human Resources and your IT department you can implement controls to reduce risk and detect incidents before they cause damage. With Tripwire's combined set of security controls you can monitor your environment for events of interest in real-time, track configuration changes and identify vulnerabilities before they are exploited.

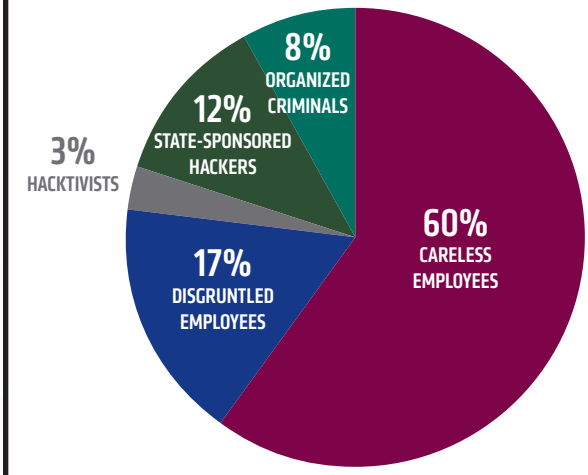


FIG. 5 *Poll results of June, 2014* Dark Reading *visitors responding to "What do you consider the greatest security threat to your organization?"*