COVER STORY | BY VAL LeTELLIER

ILLUSTRATION BY VIKTOR KOEN

As workforces shift towards telework, leaders need to reorganize their insider threat toolbox as they look for new ways to detect warning signs and mitigate potential incidents.

AT HOME WITH THE INSIDER THREAT

INSIDER THREAT MITIGATION IS NEVER EASY.

The number of incidents and the financial cost of insider theft, fraud, sabotage, and workplace violence are on the rise. Technical countermeasures like behavioral analytics address only part of the problem and are increasingly expensive, complicated, and difficult to integrate. The move to reduce overhead and increase morale by allowing employees to work remotely means additional challenges. The U.S. Bureau of Labor reports that roughly 15 percent of the workforce was almost fully working remotely, mostly in management, sales, and finance before the coronavirus pandemic began. A far greater percentage work remotely for part of their job.

To make matters more complicated, the spread of the COVID-19 coronavirus prompted many organizations to quickly implement remote work programs without the lengthy prelaunch planning, design, and testing processes normally followed. While these programs were meant to address a temporary crisis, it is highly likely they will boost the already significant remote worker growth seen in the last decade. It is also highly likely there will be security events—including insider attacks or vulnerabilities—not fully considered in organizations' haste to launch these programs.

With more employees working from home, client sites, and the road, an amorphous "digital fence" grants insiders greater responsibility but also less direct oversight. Within this new paradigm, conventional insider risk early warning resources are degraded. Specifically, valuable insights gained from regular face-to-face observation and engagement by managers, colleagues, and clients become limited.

A new strategy is therefore required to address early warnings in this environment, one that counteracts the natural tendency for remote workers to be "out of sight, out of mind." Instead, this requires a different form of management, placing greater weight on understanding employees and the critical events affecting them. To underpin this new strategy, new tactics are needed to identify, assess, and react to anomalous activity, new vulnerabilities, and threats.

THE PARADIGM SHIFT

The first step to developing a borderless insider threat strategy is understanding what is lost when shifting to remote work. Employee observation and workplace cohesion are at the top of the list.

Observation is significant because independent behavioral assessment has traditionally been a highly valuable resource for identifying malicious behavior. Essentially, fellow employees and managers have historically played a large role in identifying threats. This early warning resource is considerably degraded when exposure is limited to email, conference calls, and occasional meetings.

> *Essentially, fellow employees and managers have historically played a large role in identifying threats.*

Social and professional group cohesion is important because in all workforces, the building of authentic relationships between workers creates a satisfying bond between the employee, the manager, and the organization. This bond is widely beneficial to job satisfaction, morale, and productivity, and it also enhances organizational resiliency to insider attacks. Cohesive groups tend to have higher levels of trust and emotional unity, often looking out for each other.

While degradation of employee observation and cohesion independently represent significant challenges to an insider threat program, when combined they create a paradigm shift in the insider risk environment.

This paradigm change is not going unnoticed. In an OpenVPN survey of 250 IT leaders—from managers to C-suite executives—more than half said they believe that remote employees pose a greater security risk than onsite employees. More than one-third of respondents had already experienced a security incident because of a remote worker's access.

Regarded as a leading center of insider threat study, Carnegie Mellon University's Software Engineering Institute (SEI) CERT National Insider Threat Center lists 21 insider threat mitigation best practices in its latest annual *Common Sense Guide to Mitigating Insider Threats* technical report. The dislocation and decentralization of workers greatly challenges executing five of those best practices—clearly document and consistently enforce policies and controls; monitor and respond to suspicious or disruptive behavior; anticipate and manage negative issues in the work environment; structure management and tasks to minimize insider stress and mistakes; and establish a baseline of normal behavior for both networks and employees.

Simply put, enforcing security policies and determining then monitoring behavior baselines of remote employees is demanding. Worse, the lack of organizational cohesion can create or exacerbate negative issues, increase stress, and prevent timely and appropriate responses to suspicious or disruptive behavior.

These new challenges are particularly evident when examined through the prism of the insider threat kill chain, the path an insider takes toward an attack.

Starting with the first step of temperament—or the inner nature of the insider—security leaders should consider employees' personalities. It is crucial to note that the difference between an insider leaning towards "self-destruction" instead of "self-healing" can push an employee towards incidents like insider attacks. Indicators of this type of personality can include violent tendencies, psychological imbalance, vengefulness, and more.

The second stop on this journey is an event or certain stressors that trigger an emotional shift, like a personal or professional crisis.

The third stage is conflict, where the insider is dissatisfied with a superior, coworker, or perhaps even the entire business, likely generating a resentment that builds and builds throughout the remainder of this kill chain.

Determination is the fourth phase, where the insider becomes singularly opposed to perceived enemies. This often displays as increased risk-taking, open hostility, social withdrawal, or identification with violence.

During the fifth stage, preparation, the insider will prepare by performing reconnaissance, acquiring any necessary materials, or penning a manifesto.

Lastly, we arrive at the attack, where the resentment comes to a head.

With on-site employees, the environment where this process occurs is largely—if not entirely—under a leader's control or supervision, and an insider's movement through the kill chain provides opportunities for those close to a potential attacker to recognize behavioral changes. With remote workers, control of the organizational environment is minimized, and observation of overall employee behavior is far more difficult.

THE CENTRAL TRUTHS

When developing a borderless insider threat strategy, it is important to understand the central truths relevant to your effort. Given that insider threat mitigation within a remote workforce is just now starting to be studied, these truths lie in the general body of insider attack and remote work studies. By finding them, certain lessons learned become evident.

There are significant opportunities for stopping insider attacks. Generally, these incidents are not impulsive in nature. The insider takes considerable time before acting, regardless of the motivation, and slow progression from idea to action means that they almost always expose themselves to some degree through observable changes in attitude and behavior.

Humans are quite good at spotting insider threats. People naturally create behavior baselines for everyone they know and have a sixth sense for deviations. Unlike algorithms, people can instantly evaluate actions within context, then quickly and accurately judge when something is amiss.

A common first sign of a growing problem is an insider's decreased engagement or withdrawal from interaction with colleagues, managers, and clients. This usually reflects a growing preoccupation with matters besides work. These are often significant personal or professional events an organization will want to assist the employee with, potentially avoiding negative impacts upon the workplace's productivity and perhaps safety.

While a significant event can trigger the kill chain, it is worth noting that there are critical stages of an insider's life particularly relevant to threat mitigation—notably, the ages between 35 and 45 years old. The apex of the symbiotic relationship between personal and professional lives, these are the ages marked by reevaluation of life choices and goals, potentially leading to divorces or career changes.

Given the fluidity of situations, triggers, and reactions, insider threat programs must be proactive. Continuous evaluation enables this, mitigating risk early in the kill chain. While organizational culture, employee privacy, and funding constraints often prevent firms from incorporating this methodology, a different decision might be made if organizations understood that it would enhance employee welfare and morale. Early warning signs met with understanding and assistance turn employees from liabilities to examples of a

CATEGORIZING INSIDER ATTACKERS

There are five distinct categories of insider attacks. Each attacker's profile is developed from commonly seen personality characteristics and critical events that negatively affect them.

Intellectual property/sensitive data theft

These insiders want to benefit themselves or others by stealing valuable data or materials, either working alone or with an outside malicious actor. Common personality characteristics include entitlement, narcissism, antisocial behavior, and a desire for control. Usual precipitating events include a negative personal financial event, failed promotion effort, poor performance review, unfulfilled career aspirations, resignation, or termination.

Insider fraud

These attackers seek personal gain through their actions. Typical personality characteristics include egotism, entitlement, privilege, and self-importance. Common precipitating events include significant additional expenses, negative personal financial events, and unmet career or lifestyle aspirations.

Sabotage

These insiders strike out against an organization with the intent to harm its functionality. Common personality characteristics include anger, vengefulness, vindictiveness, disengagement, and destructive behavior. Typical precipitating events include confrontation with management, poor performance review, failed promotion effort, demotion, workplace embarrassment, and termination.

Workplace violence

These insiders move against the organization to cause bodily harm to its people. Prevailing personality characteristics are aggression, emotional detachment, confrontation, disengagement, strain, and a lack of remorse. Common precipitating events include negative family or relationship events.

Unintentional insider threat

These insiders lack malicious intent but become a threat through negligence and/or outside manipulation. Common personality characteristics include being flighty, unfocused, disorganized, scatterbrained, stressed, and strained. Common precipitating events include new personal or professional distractions.

positive and caring security culture, increasing overall job satisfaction, retention, and productivity.

DEVELOPING A STRATEGY

Enterprise risk managers should consider several factors, methods, and goals in constructing effective remote insider threat strategies.

There are controllable insider environmental factors, and there are uncontrollable factors. With remote workers organizations might not control the environment, but they can control the personalities they work with through the initial hiring decision. By truly understanding who is hired in the first place, organizations can avoid significant problems in the future. Of course, more robust preemployment screening for those seeking positions of greater responsibility and trust is warranted.

Whether it's a potential new hire or an established employee, "whole person" and "whole threat" methodologies can be very effective for insider early warning. The whole person approach is contextual and psychosocial, using personality, environment, and precipitating events to identify insider risk. A whole threat approach addresses the common root causes that result in in different attacks, including data theft, fraud, sabotage, and violence. These methods leverage common sense and objectivity to understand the trusted insider personalities relevant to the organization, as well as the precipitating events and corresponding tripwires that can turn those personalities towards malicious action.

Data will invariably support detection methods, and public data is extremely valuable as an early warning resource. Historically, public records data shows that all but a few malicious insiders exhibited indicators of nefarious activity prior to their ultimate discovery. Ultimately, legal and proper usage of public data can help identify insider threat behavior before attacks occur, especially from those in positions of greater access, responsibility, and trust.

All insider threat strategies must consider the evolving nature of data usage, storage, transmission, and security. While data can deter an attack, it is also a new end point. Since the data classification and segregation considerations for remote workers merit an entire separate examination, a few select practices are worth noting. First, widescale adoption of cloud infrastructures has created new vulnerabilities as sensitive data is stored globally and accessed by increasing numbers of employees, partners, and customers. An important first step in addressing these vulnerabilities is using secure applications, locking down identities, and monitoring how identities use applications.

Second, risk managers should consider ways to shift their focus from the network to the data itself. In a zero trust environment, the data object is persistently protected, at rest and in motion, from data creation to consumption and through to destruction. Emails and files are encrypted before they leave the sender's computer and only decrypted (with multi-factor authentication) when they reach the destination, keeping data protected wherever it is accessed, used, transmitted, or stored.

APPLY INSIDER RISK BEST PRACTICES

Many of the best practices to mitigate risk within the on-site workplace are relevant to the off-site workplace, and several become even more important:

Create an empowered stakeholder team. Put simply, an insider risk program should be crowdsourced by including representatives from the C-suite, legal, human resources (HR), information technology (IT), administrative, financial, compliance, security, and the general employee population. Supported by a senior-level champion, this team can help implement cross-organizational communication and information sharing. HR should have a significant role on this team, because often it is the primary office addressing anomalous employee behavior and voluntary/involuntary departures. The dispersed nature of the remote workplace reinforces the need for a broad and empowered stakeholder team that cuts across organizational siloes.

Determine the remote worker security program goals. Using the stakeholder team, set the goals needed to know, understand, and help remote employees. Focus on realizable achievements, match the organizational culture and resources, determine what is not achievable, and create milestones for desired progress.

Advertise your program. Using the stakeholder team, demonstrate transparency by clearly stating what is being done and why. Provide opportunity for questions and recommendations. All of this will help avoid claims of hidden agendas. This is particularly important in the remote workspace. By creating effective anomalous behavior reporting mechanisms and highlighting the co-dependency of employee and organizational success, remote employees will become stakeholders in the program. By explaining that the program is meant to provide early warning of employees who may need assistance from the organization, the program will likely be viewed as positive rather than punitive.

Identify critical assets and access holders. Generally, this list is significantly longer than most risk managers realize. In the remote workspace, critical data is often being handled in an uncontrolled environment where an organization has only a limited ability to monitor for security policy adherence and ensure the data remains with only those whom you designate.

Technicians or vendors with access to client-site spaces or networks housing critical data or material are often overlooked in the risk equation. Newsworthy examples include alarm technicians who use their privileged access to facilitate bank robberies, pharmaceutical sales representatives who sell products on the black market and replace the originals with placebos, and postal service carriers who hoard or destroy large quantities of mail.

Determine the most harmful insider attack. Certain organizations are more susceptible to certain insider attacks. The remote workplace is particularly susceptible to fraud (by exploiting access to client sites), sabotage (by destroying or altering company products), and unintentional access (by allowing unauthorized personnel access to sensitive data). Identifying the most harmful insider attacks enables the creation of a watch list of the most relevant insider profiles. Employees fitting these profiles may merit additional monitoring for exposure to "tipping points" that move a predisposed insider personality to harmful action.

Assess insider early warning capability. Focusing on remote workers with privileged access or authority, apply the attacker mentality and red teaming to understand the way a malicious remote insider will probably attack the organization, and how early in the insider kill chain anomalous activity will be identifiable and by whom.

Data will invariably support detection methods, and public data is extremely valuable as an early warning resource.

Ask how robust the screening of potential hires is; to what degree are personality, organizational fit, and remote work conditions considered; and to what degree are the backgrounds of potential hires investigated.

Consider the strength of the cohesion between managers and remote workers and between workers, as well as which policies for engagement include regular personal contact—virtual or otherwise—that allow remote employees to feel part of a larger cohesive group. Look at the workforce's understanding of insider threat red flags and how to report and respond to them. Assess whether leaders know about individuals who fit attacker profiles and if they recognize triggers that could start the kill chain. After looking within, similarly analyze outsiders that have a certain level of trust—such as vendors, subcontractors, and anyone with privileged access to the organization or its assets.

Identify all available early warning sensors. Especially in a remote work environment, insider threat early warning is a team sport requiring a host of human and technical sensors. HR can highlight performance and behavioral issues, IT can highlight network anomalies, and security can highlight policy violations. Line managers and employees can provide firsthand observations of unusual behavior.

Develop realistic and effective remote work security governance. Employees' access to critical data or materials should be limited, ideally dependent upon roles, information types, and need-to-know principles. Authentication, secure communication, encryption, personal device usage, data and device storage, and employee monitoring are all areas that organizations may need to consider and draft effective policies for. Auditing and accountability for compliance must be administered, along with periodic refresher training.

Create insider threat awareness. Develop an appreciation for the use of profiles and indicators as part of an insider early warning system. Train leadership and staff to understand that behavior and behavioral observations matter in preventing insider attacks, including in the remote workspace. Teach them about insider personality types, the impact of precipitating events, and how to spot indicators of a negative response to an event. Teach them how to use the anomalous behavior reporting mechanisms available to them. Make it a core managerial responsibility to pay attention to workers for the value it creates in wellness, productivity, and assessment.

To reduce employee ambiguity, personal judgment calls, and missed indicators, consider establishing a mandatory requirement for employees to report security violations.

Have a response plan. While responses to an insider risk indication are dependent on the situation and the organization, there are a few notable best practices to consider. First, predetermine lines that, if crossed, require further action. Second, maintain an objective perspective of the situation, starting with the premise of innocence and using observation as a starting point for further information collection (not judgment). Finally, predetermine the status that—if achieved—prompts the end of monitoring.

The intent is to focus on employee welfare. This will enhance morale, positively reinforce stakeholder buy-in, coworker reporting, and overall program success.

Ensure a continuous and adaptable process. As with most security programs, conduct continuous evaluation, tabletop exercises, and red team exercises, and solicit and incorporate constructive employee feedback and recommendations into future plans and programs.

VAL LETELLIER HAS A DEEP UNDERSTANDING OF HOW INSIDERS ARE CREATED, MANAGED, PROTECTED, AND DISCOVERED, EARNED FROM TWO DECADES OF RECRUITING FOREIGN SOURCES AND PENETRATING INTELLIGENCE TARGETS FOR THE CIA. HE LEADS THE ASIS DEFENSE & INTELLIGENCE COUNCIL'S INSIDER THREAT WORKING GROUP AND IS A MEMBER OF THE INSA INSIDER THREAT SUBCOMMITTEE.