THE NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

Insider Threat Mitigation for U.S. Critical Infrastructure Entities:

Guidelines from an Intelligence Perspective

Insider Threat Mitigation for U.S. Critical Infrastructure Entities: Guidelines from an Intelligence Perspective

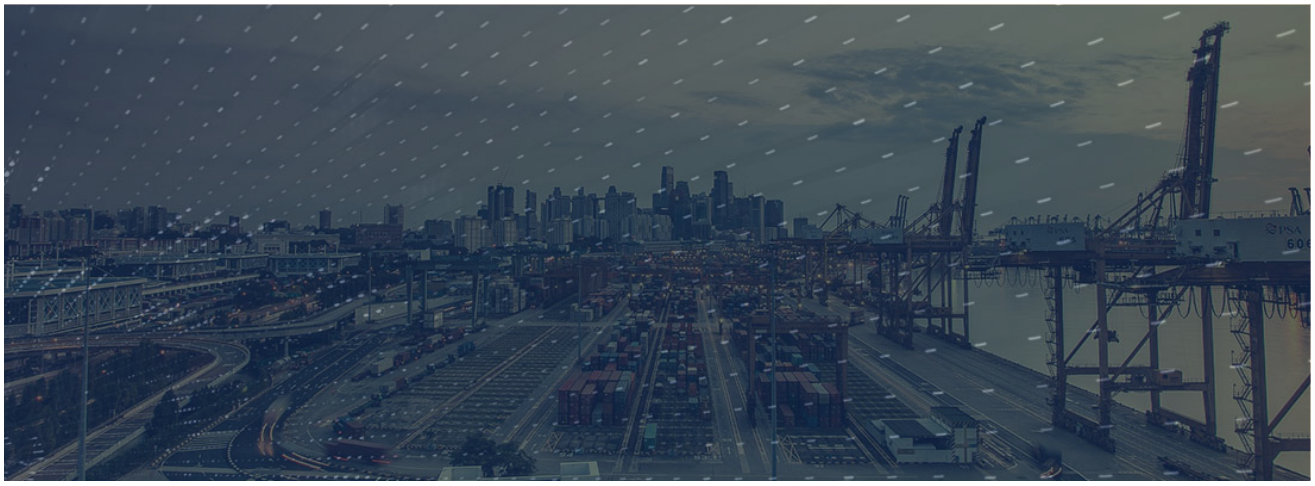
The National Counterintelligence and Security Center
March 2021

Overview

The National Counterintelligence Strategy of the United States of America, 2020-2022 highlights the expanding and evolving nature of threats to U.S. critical infrastructure organizations from foreign state and non-state actors. Foreign adversaries are no longer simply targeting the U.S. government, as was often the case during the Cold War, but today are using their sophisticated intelligence capabilities against a much broader set of targets, including U.S. critical infrastructure and other private sector and academic entities. These U.S. industry and academic organizations are now squarely in the geopolitical battlespace.

Among other activities, foreign threat actors are collecting large sets of public and non-public data about these organizations and their workforces at an unprecedented level. By combining this information with advanced data analytic capabilities and other tools, foreign adversaries are afforded vast opportunities to identify, target, and exploit vulnerable people in U.S. workforces to further their geopolitical interests at America's expense. Their strengths are identifying our weaknesses and our threats are their opportunities.

Given this threat landscape, it is imperative that critical infrastructure entities prioritize and dedicate resources to preempt and/or mitigate insider threats. Insider threats are trusted individuals in an organization who may use their authorized access to facilities, personnel, and information to cause harm to their organization -- whether intentionally or unintentionally.

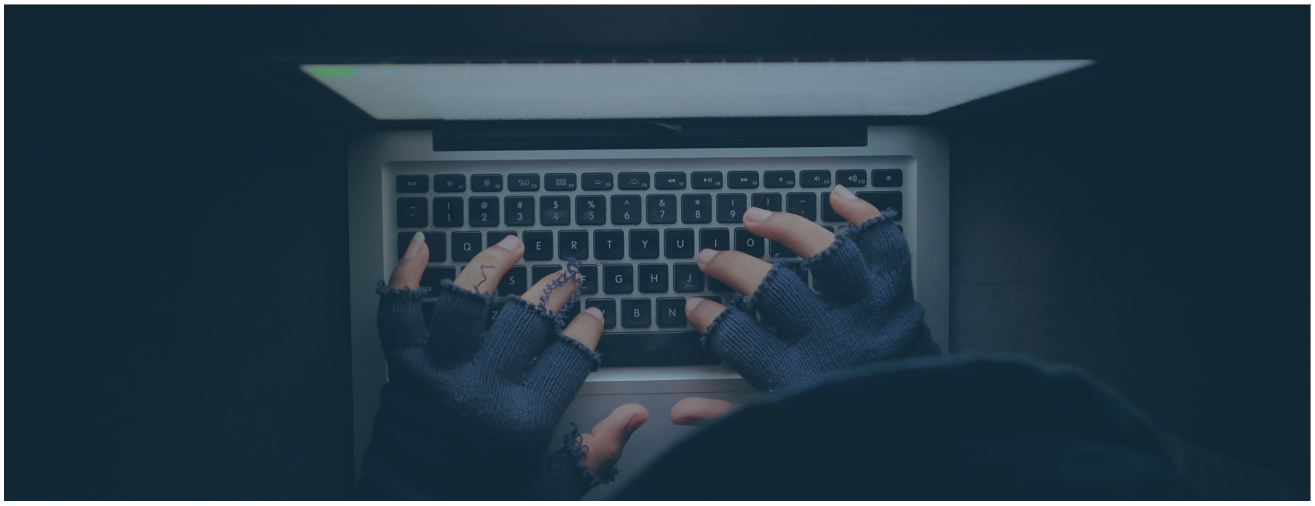


The National Insider Threat Task Force (NITTF) has produced a wealth of standards, advisories, guides, and bulletins to help organizations build effective insider threat programs. Although the NITTF was created in response to compromises of classified information, the NITTF promotes organizational practices that proactively address all insider threats, while protecting the privacy and civil liberties of employees in the workforce. The NITTF model is focused on human behaviors -- seeking to identify anomalous behaviors and address them before significant damage is done to the workforce, the organization, or the mission. NITTF's model is widely recognized across the government and industry as a best practice for protecting all organizational resources.

The National Counterintelligence and Security Center (NCSC) raises threat awareness and promotes practices designed to protect the nation against foreign intelligence threats. Programs and practices that are designed to counter insider threats, while not formal counterintelligence programs, help strengthen the nation's overall counterintelligence posture.

The intent of this report is to raise awareness of the human threat to critical infrastructure, provide information on how to incorporate this threat vector into organizational risk management, and offer best practices on how to mitigate insider threats. This report complements existing NITTF guidance by offering an expanded discussion of how critical infrastructure entities can use insider threat programs that focus on human behaviors to address key vulnerabilities and prevent them from being exploited by adversaries.

Insider Threat



The “Insider Threat” has been part of human history from the origins of civilization. Almost all cultures have historical tales of insider threats. U.S. history is full of anecdotes that highlight the threat faced when a trusted confidant turns. From Benedict Arnold to recent, catastrophic, unauthorized disclosures of classified information, there is a common narrative -- trusted and capable human beings, facing life challenges, change course and ultimately do harm.

Given the resources that foreign adversaries are dedicating to exploit or coopt insiders within organizations they seek to penetrate, insider threats will be an enduring part of the threat and risk landscape for most critical infrastructure entities for years to come.

The solution? Since insider threats are a human problem, they require a human solution. Technology can enable organizations to get a better sense of workforce behavior, particularly in its virtual domains, but the most important resource an organization has to counter insider threats is the workforce itself. To help mitigate these threats, an organization must, at a minimum, achieve two things:

1. Have a program that identifies individual anomalous behavior and the resources to respond.
2. Respond to anomalous behavior in a way that fosters trust and leverages the workforce as a partner.

Target: Critical Infrastructure

Critical infrastructure entities encompass the 16 sectors defined by Presidential Policy Directive 21 (Critical Infrastructure Security and Resilience), including the U.S. electric grid, telecommunications networks, financial institutions, manufacturing facilities, transportation facilities, and hospitals. These sectors feature not only physical assets like roads and fiber, but also the intellectual capital behind them -- the people involved in health care, energy research, food production, green technologies, and many more areas. These individuals are among the primary targets of foreign adversaries who seek to gain access to our critical resources for nefarious purposes.

Witting or unwitting, insider threats within U.S. critical infrastructure entities can cause grave harm to national security and public safety, as well as to individual corporations and state and local governments. Improving ways to mitigate such threats is in the national interest and in the interests of individual organizations.

NCSC and the NITTF, in partnership with the Departments of Homeland Security, Treasury, Energy, Defense, and others, are working to better support critical infrastructure entities in the U.S. private sector; state, city, and local governments; and academia. We encourage critical infrastructure entities to invest in human-behavior-focused insider threat programs that enhance and supplement traditional security practices and are tailored to their environments and unique threats and risks.

How the Risk and Threat Environment is Changing

The U.S. threat environment is changing in ways that require new kinds and levels of attention. U.S. critical infrastructure is both in the geopolitical battle space and the target of extensive criminal activities.

Foreign intelligence threats to the United States have never been more complex or dynamic than they are today. Foreign threat actors have increasingly sophisticated intelligence capabilities and are employing them in new ways to target the United States. Furthermore, these threat actors have an expanded set of targets and vulnerabilities to exploit in order to advance their interests. On a daily basis, adversaries are learning and adapting to our security measures.

Harming U.S. critical infrastructure is one way for foreign adversaries to inflict severe damage on U.S. national security, economic security, or public health and safety. According to the National Counterintelligence Strategy of the United States of America, 2020-2022:

> *"Foreign intelligence entities are developing the capacity to exploit, disrupt, or degrade critical infrastructure worldwide. Their efforts likely are aimed at influencing or coercing U.S. decision makers in a time of crisis by holding critical infrastructure at risk. The decentralized and digital nature of critical infrastructure worldwide creates vulnerabilities that could be exploited by foreign intelligence entities, and they also are targeting the facilities and networks that underpin global energy and financial markets, telecommunications services, government functions, and defense capabilities."*

Given this evolving threat landscape and the fact that much of U.S. critical infrastructure is privately-owned, securing the critical infrastructure is not solely a function of the U.S. Intelligence Community or even the federal government writ large. Solutions must involve the private sector and other stakeholders. There is an unprecedented imperative for public-private collaboration to collectively "raise our game" in protecting U.S. critical infrastructure.

Insider Threats Pose New Kinds of Challenges

Insider threats to critical infrastructure entities are growing. These threats are often less appreciated than remote-access cyber threats and can be more difficult to mitigate.

Insider threats are an increasingly important threat vector to critical infrastructure, both within the context of cybersecurity or supply chain risk, and within the broader risk to security.

Insider threats can cause harm through economic espionage, sabotage, workplace violence, fraud and other misuse of corporate resources. Insider threat activities can involve deliberate actions by insiders working with Foreign Intelligence Entities, or other actions by insiders with malicious or criminal motives. Finally, insiders can also cause harm through simple negligence or carelessness. The current tense ideational-ideological landscape in the U.S. exacerbates these risks, giving some people more motivations and making others more vulnerable to high levels of stress.

Geopolitics in your neighborhood

The interest of foreign adversaries in US critical infrastructure means that geopolitical tensions could affect your company or state/local entity in ways not seen in the Cold War or subsequent periods. It is increasingly true that "you might not be interested in war, but war is interested in you."

It is important to frame insider threats to U.S. critical infrastructure entities in the context of remote-access cyber threats (such as phishing campaigns), which tend to be more prominent in the public view. Critical infrastructure protection discussions have often become synonymous with cyber security discussions, focusing primarily on the battlefield (cyber) and not the threat actor (the human being). Yet, more often than not, there is a human with access who compromises the integrity of our resources.

Critical infrastructure entities will continue to become more reliant on Information and Communications technologies (ICT). There will likely be more interdependencies between ICT elements and thereby more vulnerabilities. Remote-access cyber threats pose continual and serious threats to critical infrastructure entities, but insiders can exploit ICT vulnerabilities without remote-access via the Internet. Even if remote-access cyber protections are highly effective, an adversary may find that an insider is the most feasible means of penetrating an organization.

How the Covid-19 Crisis Affects the Threat/Risk Landscape

The Covid-19 pandemic -- involving public health, safety, and economic insecurity -- is likely to aggravate the threat environment, including insider threats.

The Covid-19 pandemic has caused unprecedented crises of public health, public safety, and economic security for America and nations around the globe. For many U.S. state and local entities, companies, and the individuals who work for them, the pandemic has brought incredible new stresses. These stresses are recognized by Foreign Intelligence Entities as opportunities.

With more individuals working remotely or from home, the pandemic has fostered greater reliance on less-secure information and communications technologies that may be exploited by adversaries, and more interdependencies between elements of these technologies. At the same time, there are potentially greater individual and family anxieties over job security, health, and other issues. A tense national economic, social, and political landscape may serve to further exacerbate these tensions. In short, many employees in the workforce are facing unprecedented stresses at home, have become more isolated from their organizations, and are increasingly reliant upon less-secure information technologies to work.

In this environment, robust and adaptive insider threat programs are more necessary and more difficult. They are more necessary due to the increased salience of insider threat motivations, behaviors, and stresses. Insider threat programs are increasingly difficult in this environment because the crisis puts stress on corporate and government resources, including security programs.

Security as an Evolving Cycle

In the current environment, there is a new imperative for organizations to take stock of their security postures to ensure they match the evolving threat and risk landscape.

Countering insider threats requires a whole-of-organization effort founded on an informed, aware, and dedicated workforce. Fostering a sense of organizational citizenship and promoting a culture of security is critical to addressing insider threats. True organizational security, in both a national security and a business sense, is the responsibility of everyone in the organization.

An effective insider threat program is not merely "a security program," but a sustained employee outreach and awareness effort that promotes a shared responsibility for the protection of the organization and the workforce.

For more than half a century, the U.S. government has promoted the concept of "Operations Security" or OPSEC. At its core, OPSEC involves a risk management cycle that considers adversarial threat (intent and capabilities) when assessing organizational vulnerabilities and implementing appropriate mitigation practices.

With foreign state and non-state threat actors increasingly targeting America's industry and critical infrastructure, it is imperative that industry incorporate foreign adversarial threats into their risk management and business practices and ensure that their workforces are part of the solution, not the problem.

The evolving threat environment should prompt questions among organizations about the extent to which their security posture is well-matched against today's threats. Protections against external physical access and remote-access cyber threats are often more developed than protections against insider threats. Taking stock of one's security posture is a first step toward addressing emerging threats.

- For many organizations, the sheer number and scope of potential threats and risks creates uncertainties over which to prioritize. Frequently, the response is to stick with the seemingly most salient risks -- often involving physical access and remote-access cyber.

- Most organizations have built some forms of security against risks and threats, but these security measures may not match the latest threat landscape. Threats and risks tend to be countered in specialized "stovepipes" -- making an enterprise view difficult.

- For some organizations, a "check the box syndrome" can be in play. Security programs in name only can be seen as better than no programs at all. Such risk framing can contribute to serious security deficiencies.

- Augmenting an existing security structure or creating a new security program is often difficult to resource. Even when sticking with a legacy security posture, it is important to review and assess the posture to ensure it addresses current and emerging threats.

In the evolving threat environment, corporate and government leaders need to be able to answer the following kinds of questions: What is the organization's overall enterprise security posture? What are the most recent investments or organizational changes in security? How could either be mismatched with the current and emerging threat environment? Who in management is in a position to know if there is such a mismatch? Who is accountable for insider threat incidents, responses, or larger security posture mismatches? If such questions cannot be answered based on existing policies and practices, there is likely even more of a need for a security posture review and assessment.

Security posture assessments can help determine if your organization performs "intelligence-like" functions -- the ability to gather and process information relevant to organizational security. Serious security events can be the result of organizational intelligence failure.

To effectively respond to threats, many critical infrastructure entities will need to create a security "intelligence" function or enhance their existing one. Intelligence in the context of the U.S. Intelligence Community refers to the information —questions, insights, hypotheses, data, evidence — relevant to inform U.S. policy decisions. Intelligence in the context of critical infrastructure organizations is information necessary for the successful pursuit of organizational goals and for protection against threats and risks. Key elements of an intelligence function to enhance critical infrastructure security include:

- Creating a security intelligence program to analyze threats and vulnerabilities to personnel, physical, and information disciplines
- Conducting trend analysis of frequent security violations and patterns of "close call" incidents
- Developing a communications plan to educate the workforce of security concerns
- Integrating multiple organizational disciplines (human resources, wellness, Information Technology, etc.) into security planning and operations
- Staying current on internal and external threats (and looking over the horizon)
- Ensuring resources are available for cross-organization learning
- Incorporating full civil liberties and privacy protections into security and intelligence-like programs

For U.S. government insider threat programs, one minimum standard is access to "counterintelligence" information. While a formal counterintelligence program is not likely feasible for many in the corporate world, it is imperative that information about foreign adversarial threats, including intent and capabilities, are incorporated into organizational risk management practices to protect against determined, organized, and well-financed adversaries. Such programs will help protect your organization and its workforce, and, where critical infrastructure is at risk, potentially U.S. national security and public safety. An insider threat program is not a counterintelligence program, but understanding adversarial threats and incorporating them into risk management efforts will help an insider threat program focus its efforts and better prepare the workforce to counter the threat.

Nine Elements of Insider Threat Programs for Critical Infrastructure Entities

I. Recognize that the insider threat is a human challenge

As noted above, the insider threat is a human problem requiring human solutions. The insider threat is the risk that a trusted member of the workforce will use their access to harm themselves, their colleagues, or their organization. Insider threats can be witting -- knowingly inflicting harm -- or they may unwittingly do harm though negligence or carelessness. In the vast majority of documented cases, however, an "insider threat" did not start as a threat, but developed into one over time. In most cases, anomalous behaviors of concern were present before a negative act occurred.

Proactive insider threat programs work to identify risk indicators by focusing on anomalous human behaviors, so early intervention can occur, leading to positive outcomes for at-risk individuals and reduced risk to organizations. These programs facilitate and deploy mitigation response options that protect the organization and its assets while safeguarding the privacy and civil liberties of employees in the workforce.

An insider threat program is not a security program; it is not a cybersecurity (information security) program; and it is not a counterintelligence program. It is a new and unique discipline focused on human behavior -- looking for anomalies, contextualizing them, and facilitating an appropriate organization response. More often than not, the insider threat program is not the responder, it is the facilitator.

An effective insider threat program leverages an informed and empowered workforce to help flag anomalous behaviors so at-risk employees can get the assistance they need before becoming threats to themselves, the workforce, or the organization.

II. Have a dedicated insider threat program

An insider threat program is designed to help an organization and its employees get ahead of workforce problems before they occur. As noted previously, such programs involve sustained employee outreach efforts that promote a shared responsibility for the protection of the organization and the workforce.

The NITTF has extensive materials to help organizations create and advance insider threat programs. The NITTF model is used by the Department of Defense and the Department of Homeland Security (DHS) to address all organizational threats, from unauthorized disclosures to suicides. NITTF's model is recognized by the National Institute of Standards and Technology as a best practice for protecting unclassified information, and by the DHS-housed Interagency Security Committee as a strong foundation for preventing active shooters and other workplace violence.

The NITTF model is scalable and applicable to all types of organizations, both public and private. Within the government, it has been applied effectively across a broad range of organizational missions and constructs, from sophisticated intelligence agencies to small regulatory agencies. NITTF resources are available on the NCSC website at www.ncsc.gov along with links to insider threat resources from other federal agencies.

III. The complexity of insider threats merits specialized attention and requires participation and commitment from the entire workforce

What's in a name?

There is no need to call your program an "insider threat" program.However, what your program is called and where it is placed can impact both its mission and image. If it is placed under security, it will always be viewed as a security program both by leadership and the workforce.

Specialized attention by an organization is crucial for insider threat programs due to the need to mesh different management responsibilities, the inherent ambiguity of human behavior, the complexity of norms and rules for use of information and communications technologies, the sensitivity of computer monitoring, and the nuances of legal and privacy considerations. Broad participation and commitment from the workforce are also essential for insider threat programs. The most effective tool an organization has to identify potential insider threats are employees and managers who are empowered to report anomalies and other issues of concern in the work environment. Mitigating insider threats also requires a sense of co-responsibility among members of the workforce -- between managers and employees, and between different levels of managers. The emphasis on co-responsibility across the workforce is the primary way to offset perceptions that corporate intelligence functions or insider threat measures are treating employees as suspects.

IV. Incorporate components from across the organization in structuring an insider threat program

It is important to identify and partner with stakeholders across the organization to facilitate appropriate insider threat responses, to assess the effectiveness of the program, and to gauge the need for adjustment. Depending on the size and scope of the organization, these stakeholders should include representatives from human resources, security, counterintelligence (or similar function), cybersecurity/information security, internal policymakers, training, and legal, privacy and civil liberties, as well as front-line leaders. Including multiple components of the organization in an insider threat program is essential because information indicating an insider threat can come from multiple sources. Sometimes individual indicators are not considered a problem, but when coupled with information from across the organization, they may reveal an issue.

Stakeholders across the organization all bear the responsibility for organizational responses to insider threats. A successful insider threat program must leverage tools from across the organization to properly address the full spectrum of potential issues. This tool chest must include capabilities well beyond security responses or adverse actions. For success, an organization must also leverage programs to help at-risk employees, such as crisis intervention, employee assistance, financial counseling, peer support groups, and other programs designed to foster organizational citizenship.

V. Designate a top-level senior official to oversee the insider threat program and ensure the counter insider threat mission is promoted across the organization

Experience has demonstrated that U.S. government and industry organizations with effective insider threat prevention and mitigation programs have a designated senior official with access to the organizational head, and a dedicated program office for insider threat advocacy, persistence, and accountability. In its 2019 Insider Threat Program Maturity Framework, the NITTF recommended a single responsible executive as a key element of a mature program.

VI. Effective insider threat programs are attentive to threats and risks to an organization's "crown jewels"

The "crown jewels" of an organization are the information or resources that, if stolen or destroyed, would damage or destroy the enterprise. They are often the materials most sought by outsiders and foreign adversaries. Identifying such crown jewels can help organizations conceptualize the potential for adversaries to target any and all employees who have access to these assets. This common risk management practice can also help focus workforce awareness efforts and help insider threat programs tailor their analysis efforts.

If everyone is responsible, no one is responsible

Insider threat mitigation as a collateral duty is problematic. That said, critical infrastructure entities face decisions on insider threat program structure that could involve multiple designated officials and discrete program offices. For large organizations, there is often need for as many insider threat programs as is needed to both ensure the lateral and upward flow of information and ensure that responsible officials have the authority to take action as needed.

VII. Successful insider threat programs are fueled by an upward flow of insider-relevant information from the workforce

Successful insider threat programs create a process whereby employees are empowered to identify and report to first-line managers, or other supervisors, anomalous behaviors and issues of concern in the work environment. Ideally, the flow is automatic, fostered by a sense of organizational citizenship and trust.

Such flow of information may seem like an employee responsibility, but the conditions for such flow are set by the leadership of an organization -- based on corporate policy, training and

awareness measures, expectations on adverse reactions, adjudication, and the cultural dimensions of trust.

Leadership must set the stage for effective flow by defining: What are the criteria for reporting? To whom? How far up will the flow go? How is information protected? Will employees' privacy and reputations be protected? Employees are more likely to come forward and report concerns within the workforce if these questions are settled. An insider threat program should protect its information and the confidentiality of employees, but the program's practices should be fair and transparent to engender trust among the workforce.

VIII. Technological systems for mitigating insider threats should be integrated with broader programs for detection and deterrence, but are not silver-bullet solutions

An important tool for deterring and detecting insider threats is operating technology that flags anomalous behavior on computer systems or that flags access to specialized locations within facilities. Such technology can provide potent tools for corporate intelligence and insider threat programs.

Foremost among insider threat mitigation technologies is User Activity Monitoring (UAM). This is the technical capability to observe and record the actions and activities of individuals operating on your computer networks in order to detect potential risk indicators and support mitigation responses.

The purpose of UAM differs from that of traditional cybersecurity/information security tools. While both serve important roles in countering insider threats, traditional cybersecurity / information tools tend to focus on information flowing out of the organization. They do not serve the primary function of an insider threat program -- observing human behavior where it occurs. Accordingly, UAM is effective where humans behave most in the virtual world. While there is an inclination to think UAM needs to be in place on an organization's most sensitive networks, the reality may be that open, publicly-connected networks may show human behavior most indicative of a problem.

Even with UAM observing human behavior in the virtual world, the most effective "sensors" for potential insider threats are other employees and managers observing behaviors in the real

world -- assuming they are willing, encouraged and trusted to communicate their concerns. In short, technology is no substitute for creating an organizational culture that fosters robust internal communications to combat insider threats.

IX. Tabletop and red teaming exercises help strengthen insider threat programs

Tabletop exercises, both at the working level and at the executive stakeholder level, are recognized by the NITTF as a key element of insider threat program maturity. They help create rapport across organizational programs, identify potential gaps in policy or procedure, and improve operating practices.

When sponsored and supported by the right levels of management, red teaming or adversary simulation exercises can also identify and explore security threats and risks that may not be obvious or sufficiently appreciated. These exercises often involve deploying a team of subject matter experts posing as adversaries to challenge plans, policies, systems and assumptions of an organization. Red teaming can provide opportunities to share critical information on vulnerabilities across organizational stovepipes, including physical security, data, cybersecurity, human resources, legal, contracting, and others.

What Does Success Look Like?

The first step of successful mitigation is threat awareness. Government and private sector organizations will become more successful in combating insider threats when they develop greater awareness of the consequences of these threats nationwide. Understanding the ways in which insider threats can wreak havoc on organizational reputations, bottom lines, intellectual property, public safety, workplace safety, and U.S. national and economic security are crucial for success in this realm. Insider threats need to be appreciated by leaders, workers, and the general public as much as remote-access cyber threats and they should be considered together with cyber and supply chain threats.

Success will also be realized when insider threat programs across industry and government foster a sense of organizational citizenship and are viewed as a shared responsibility among employees. As a new discipline that is distinct from, but related to, traditional security and counterintelligence programs, insider threat programs need stakeholder buy-in from employees so they can serve as trusted means to facilitate appropriate organizational responses. Insider threat programs also need senior-level support, engagement, and appropriate resources.

Finally, instead of responding retroactively to new risks posed by new technologies and new uses, organizations should anticipate those risks and build protections against insider threats early on. Programs to deter, detect and mitigate insider threats need to mature and evolve to the point where they are not considered unnecessary costs, but essential to the mission success of an organization and its ability to maintain organizational integrity and safety.