INTELLIGENCE INSIGHTS

EXPERT INSIGHTS ON NATIONAL SECURITY DEVELOPMENTS

SEPTEMBER 2020

Human Resources and Insider Threat Mitigation: A Powerful Pairing

PRESENTED BY INSA'S INSIDER THREAT SUBCOMMITTEE

INSIDER THREAT SUBCOMMITTEE

SUMMARY

Trusted insiders do not decide on the spur of the moment to harm their employers by leaking sensitive data, sabotaging computer networks, or committing violence in the workplace. Often, perpetrators exhibit concerning behaviors weeks or months before they act. As the corporate "first line of defense," Human Resources (HR) often has access to information that can help insider threat programs identify these potential bad actors and help troubled employees exit the critical pathway that could lead them to cause damage to the organization or its people. Therefore, engaging HR early and often is key to a successful insider threat program.

To address the human side of the insider threat problem, organizations should integrate their corporate HR functions into an interdisciplinary insider threat monitoring and mitigation approach that acts both proactively and holistically. HR engagement and leadership, together with key stakeholders such as Security, enable a comprehensive program that considers not only technical indicators but also human behavioral factors. Assisting these employees early helps the company reduce susceptibility to insider risks and build and maintain positive employee relationships, leading to talent retention. Through an assessment of the corporate challenges and benefits of creating an HR-enhanced insider threat program, case studies, and recommended best practices, this paper looks to highlight the important role of HR in a successful insider threat program.

INTRODUCTION

INSA defines the insider threat as "the threat presented by a person who has, or once had, authorized access to information, facilities, networks, people, or resources, and who wittingly, or unwittingly, commits acts in contravention of law or policy that result in, or might result in, harm through the loss or degradation of government or company information, resources, or capabilities; or destructive acts, to include physical harm to others in the workplace."[1]

The definition includes two provisions of note. First, it explicitly refers to a human being, emphasizing that the insider threat is a human problem. Second, the definition refers to actions (or failures to act) that may be conducted *wittingly* by a malicious actor or unwittingly by people who act neglectfully or accidentally with no intent to harm the organization; even unintentional insider threats (UIT) could cause significant damage.

In its white paper, "Categories of Insider Threat," INSA describes five types of insider threats that have the potential to damage an organization's interests.[2]

CATEGORIES OF INSIDER THREAT

Following are terms with greatest resonance and most widespread use:*

SABOTAGE | An insider's destruction of electronic or physical property intended specifically to harm his/her own organization or an individual within the organization.

THEFT OF INTELLECTUAL PROPERTY OR NATIONAL DEFENSE INFORMATION | An insider's theft of intellectual property, data, or classified information relevant to national security. This category encompasses the traditional concept of espionage as defined by applicable statutes.

INSIDER FRAUD | Modification, addition, deletion, or inappropriate use of an organization's information, data, or systems for personal gain. Examples include insider trading, embezzlement, and other actions to defraud the organization by an employee, contractor, or trusted business partner.

UNINTENTIONAL INSIDER THREAT | An insider who has or had authorized access to the organization's network, system, physical facility, or data and who, through action or inaction without malicious intent, causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems. Examples include accidental public disclosures of sensitive information, phishing scams, and loss of organizational records and/or electronic media.

WORKPLACE VIOLENCE | Any act or threat or act of physical violence, harassment, hazing, intimidation, or other threatening disruptive behavior that occurs at a work site.

**From Intelligence and National Security Alliance (INSA), Categories of Insider Threats, October 2019. At www.insaonline.org/wp-content/uploads/2019/10/INSA_WP_Categories_of_Insider_Threats-1.pdf.*

Trusted insiders who commit crimes do not just "pop-up." Rather, in most cases, a person's behavior changes over time, generating warning signs that may be recognized by the organization along with stressors or precipitating events that underlie the concerning behaviors.[3,4] Therefore, it is not sufficient to conduct insider threat screening only at the hiring stage or during infrequent periodic background checks. Instead, there is a need for continuous evaluation (CE) of all individuals and for assessments that address technical indicators (network usage), physical security indicators, and human behavioral factors that help identify individuals who are at the highest risk.[5]

In short, insider threats are not just hired; they are grown. HR is typically responsible for the initial vetting of job applicants, but all stakeholders – particularly management, HR, Security, and the business unit in which the employee works – must pay attention to human and organizational factors, including external and internal stressors that give rise to insider threats. To achieve this higher level of maturity in insider threat programs, HR must be a valued and engaged stakeholder in the insider threat process.

By considering the human side of the insider threat problem, these key stakeholders can better address the problem proactively and holistically. The aim of a comprehensive insider threat program is not just to identify potential "bad actors" but also to help employees through difficult times, enabling the company both to reduce its susceptibility to insider risks and to retain talented personnel in whom the organization has invested time and resources.

In this white paper, we will discuss the value of integrating HR into an interdisciplinary insider threat monitoring and mitigation approach; we outline recommendations for implementing solutions along with examples of best practices that enable faster and gentler outreach, an understanding of corporate/other resources, and more comprehensive assessment of employees. We conclude with a discussion of the benefits of adopting this holistic approach to insider threat mitigation.

BACKGROUND

Often, insider threat perpetrators exhibit concerning behaviors weeks or months before they act.[6] For example:

- In 2015 a disgruntled Canadian Pacific Railway IT systems administrator who had been suspended for insubordination – and notified he would be fired – sabotaged important company data by using his company laptop to access and delete important company files and lock administrative accounts; he then deleted associated audit logs and wiped the hard drive of his laptop before returning it.[7,8] The company could have eliminated the employee's ability to commit such harm by dismissing him immediately or by removing his access to critical data as soon as he was suspended.

- In September 2016, Navy contractor Aaron Alexis went on a shooting rampage at the Washington Navy Yard, killing twelve people and injuring three. The perpetrator's previous arrests, as well as several examples of disturbing behavior in the weeks leading up to the shootings, presented opportunities for HR officials to intervene – either by assessing his behavior and offering assistance, or by limiting his access to the facility.[9]

These and many other examples expose concerning behaviors and other non-technical indicators that generally fall within HR's purview, but HR lacked the necessary empowerment or insider-threat perspective to act. Such cases highlight the need for greater coordination between HR and insider threat program stakeholders—especially HR and Security.

Understanding the relationship between HR and Security requires an appreciation of the role of the human factor in the assessment of insider threats. All too often, organizations rely on technical collection abilities provided by the IT staff, forgetting that this data approach is a tool, not a solution. A more complete picture of the insider threat is best obtained through a coordinated effort by Security and HR to examine associated behavioral as well as technical indicators.

THE CRITICAL PATHWAY

Insider threat behavior seldom occurs in isolation. Personal and work-related factors such as family stressors, health issues, financial difficulties, and work-related stressors may act as triggers for inappropriate behavior. Shaw and colleagues[10,11] describe a critical pathway including personal, professional, and financial stressors that can result in disgruntlement and concerning behaviors—e.g., violations of policies, rules, or even laws—as the individual responds to these stressors. These concerning behaviors provide early warning of insider threat risk. In some cases, insensitive reactions or excessive sanctions by management may exacerbate or accelerate the insider threat. If recognized and addressed appropriately, the risk might be mitigated. The Critical Pathway model describes a series of events that flow from these stressors, which act as precipitating events that lead to concerning behaviors. If recognized early, these behaviors provide opportunities for the organization to address and mitigate potential threats *before* they act—i.e., to take proactive steps "left of boom."

Among the variety of personal pressures that can increase insider threat risk are financial stress, criminal arrest, court outcomes or being on a watch list, health/medical issues, and family crises such as divorce. The insider threat director of a leading government contractor stated that 90 percent of reports concerned credit issues and debt. A survey by CareerBuilder indicates that one in four employees, regardless of position or salary, are unable to cover their expenses each month.[12] Figure 1 illustrates some of the other financial stressors that affect employees, which include saving for college and retirement, medical bills, and elder care. Some stressors are byproducts of negative behaviors and should be of concern, and some (such as substance abuse) may also be detected by law enforcement activity or organizational drug testing. While a single stressor is not indicative of an insider threat, risk is increased if concerning behaviors are observed in the context of one or more stressors. All too often, the organization is completely unaware of the stressors because the employee does not seek help or the stressors are outside of the organization's purview, such as a reduction in the employee's family income due to the loss of a partner's job.

LEADING FINANCIAL STRESSORS[13]

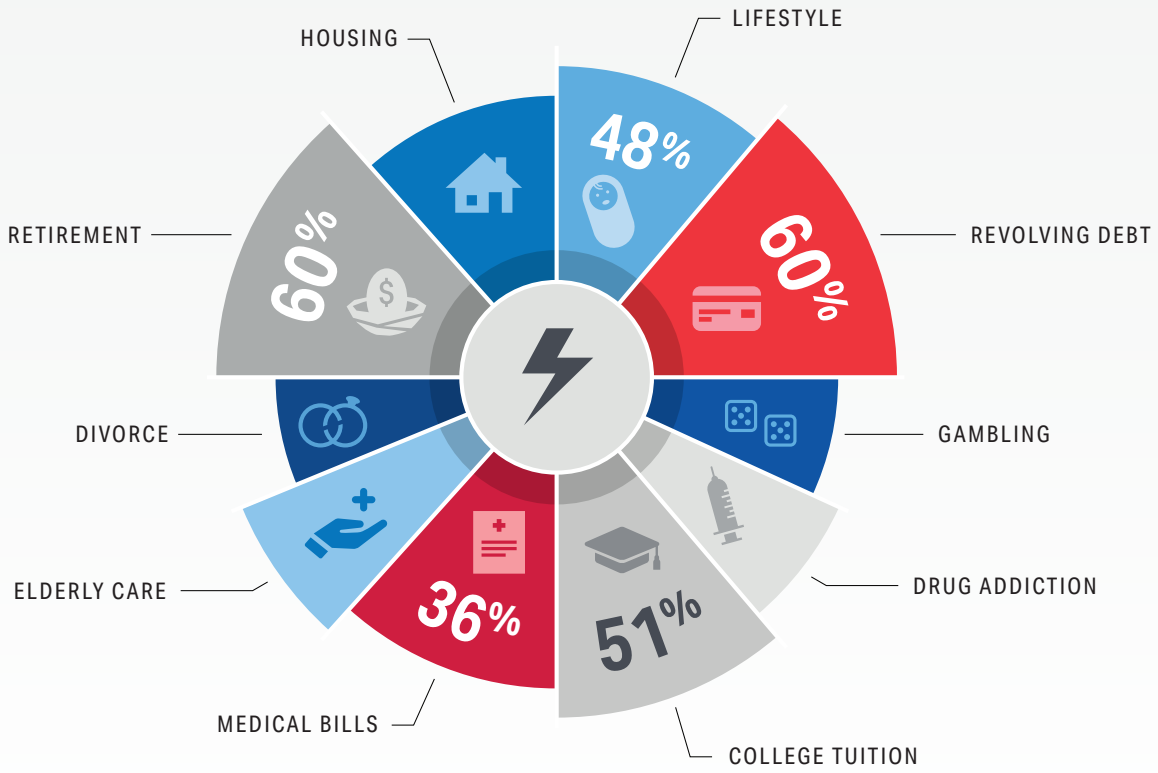

Figure 1

"The challenge in mitigating the insider threat is to devise an early warning strategy to better align organizational resources with the struggling or at-risk employee so that appropriate support or mitigation actions may be taken proactively to reduce or eliminate the risk."

In addition to these personal issues, work policies or practices that produce stress or worker dissatisfaction can increase the likelihood of both malicious and unintentional insider threats. The challenge in mitigating the insider threat is to devise an early warning strategy to better align organizational resources with the struggling or at-risk employee so that appropriate support or mitigation actions may be taken proactively to reduce or eliminate the risk.

KEY STAKEHOLDERS

Despite the availability of standardized rules and guidance across government and industry, insider threat programs vary significantly in structure and operational capability. The 2011 release of Executive Order 13587 initiated action by the federal community and created the National Insider Threat Task Force (NITTF). While the reporting structure varies between federal and industrial programs, the core makeup of insider threat working groups remains essentially the same as they focus on reporting the criteria contained in the 13 Adjudicative Guidelines.[14] In this paper we focus on the relationship between HR and Security and how their coordination promotes the "whole person concept"[15] in assessing threats, which takes into account the combination of adjudicative variables and their seriousness, frequency, motivation, and likelihood of recurrence.

Key stakeholder organizations, particularly HR and Security, approach the insider threat problem with different perspectives based on their respective missions. While both disciplines work with people, their approach is quite different. Security focuses on the protection of the organization's facilities, technology, information, and the workforce from internal and external threats, undertaking extensive planning to identify risks and prevent incidents. HR provides centralized personnel data management and analysis from the development of the position description, through recruitment, performance reviews, retention, travel, and benefits to the completion of employment. However, while relevant personnel data may be reported and collected for the purposes of insider threat identification, this information is not typically shared with and analyzed by security until after an incident.

ADDRESSING THESE CHALLENGES

"HR needs a seat at the table right up front. Need to be part of framing metrics beyond just security to measure for both who is a threat, struggling or vulnerable and how to address. Need to focus on insider risk as business metrics. Cost to hire, cost to train, cost over time of their contributions, cost to mitigate, cost to fire, cost of doing nothing."

FORMER FORTUNE 100 HUMAN RESOURCES SENIOR EXECUTIVE, MARCH 18, 2020.

SUPPORTIVE ENVIRONMENT

Between the two HR functions of hiring new employees and out-briefing departing employees, significant company resources can be brought to bear by an informed and engaged HR team to support employees. Most organizations focus on understanding their employees through their work. Simply put, they depend on monitoring physical access, cyber access, digital communications, and other tools focused on finding negative or concerning activity. What can get lost in this security-focused effort is the well-being of the employee.

"Positive intervention is what is needed (e.g., deal with employee conflict, manager issue). EAP can ensure support in place for an employee whose personal issues are flowing into [the] workplace. For the most part, employees want to do the right thing. They just often do it in a very wrong manner."

DIRECTOR, INSIDER RISK MANAGEMENT PROGRAM, A FORTUNE 500 COMPANY

In many cases, the first signs that an employee is troubled come from co-workers who notice behavior or comments that appear suspicious, concerning, or atypical. Employees need to understand their organizations' policies on reporting of suspected insider threats and how to recognize suspicious behaviors. They should know how and whether to report the information to HR, Security, or other offices, depending on company policy.

Many organizations have employee assistance programs (EAPs) that can provide counseling, financial advice, or other support to employees facing personal challenges. Such programs can help divert a troubled employee from the critical pathway that can lead to destructive behavior. Widespread awareness of EAPs can make staff more likely to report concerns about a co-worker, as such reporting could be seen as an opportunity to help the co-worker get assistance rather than as a call for disciplinary action. Promotion of EAPs by Human Resources staffs could help remove the stigma associated with reporting concerning behavior by colleagues.

EFFECTIVE AND TIMELY MITIGATION

When reporting happens, the organization must understand and support mitigation recommended by the insider threat program. Reporting may be undermined as a result of the following three missteps: if it comes too late to enable effective support, when actions are taken without a full understanding of circumstances, or when people slip through the cracks because HR's insights were not leveraged. For example, false positives (which can reflect a rush-to-judgment without fully understanding the circumstances) can produce unfortunate, unintended consequences in the loss of quality employees who leave after being unjustly accused of wrongdoing.

An interdisciplinary insider threat initiative comprised of HR, Security, management, and other stakeholders is best equipped to address insider threats with a whole-person perspective, providing employee assistance where appropriate for troubled individuals.

"No matter where the insider threat program sits within an organization, it needs to be managed by governance between all key pillars within a firm. HR is one of those components."

SENIOR LEADER, ONE OF AMERICA'S FOREMOST MANAGEMENT CONSULTING FIRMS

ORGANIZATIONAL SELF-ASSESSMENT

The interdisciplinary insider threat initiative should review organizational factors that potentially exacerbate risk. This can include periodic review of management practices, policies, or issues of poor work planning/control that contribute to stressful or unproductive work environments—all of which are factors that may increase the potential for insider threats to develop. Such internal reviews should seek to identify possible "triggers" in the workplace that can drive unproductive behaviors, such as a toxic work environment, controversial policies, or a lack of effective employee assistance to deal proactively with personal or professional challenges.

"We've had our proactive, robust program in place for six years. Our data reflects 50% of our leads for actions that were brought to our attention based on HR data."

COUNTERINTELLIGENCE OFFICER, FORTUNE 100 COMPANY

TRUSTED WORKFORCE

HR is also a critical player in setting and supporting an environment of trust. The advent of the federal government's Trusted Workforce (TW) 2.0 will introduce a new approach in addressing insider malicious behavior. Under the TW 2.0 vetting doctrine, the security clearance adjudicative process evolves to include not just event-driven data but also the behavioral aspects that define the "Attributes of Trust." This shift in addressing underlying behaviors completes the linkage required to address insider threats more effectively. This approach is informed by the Critical Pathway model[16] to address counterproductive work behavior,[17] which can serve as a behavioral baseline for both the insider threat and Personnel Vetting programs.

To fully benefit from setting a trusted work environment, employees must also trust their employing organizations. HR can directly facilitate that dynamic by ensuring employees are more comfortable in seeking help when stressors build and by incorporating early warning triggers that alert the organization about relevant external and internal data before they become a security risk. The concept of trust can be supported by HR's ability to pick up patterns of concerning behaviors that can be securely shared with the employee's direct leadership to inform a helpful conversation around organizational options.

BENEFITS

Engaging HR early and often is key to a successful insider threat program. While insider threat programs have access to technical data sources that can detect potential insider threat activity, HR programs have first-hand knowledge of an employee's behavior, personal circumstances, and performance levels. The intertwining of the two can provide a strong whole-person approach to mitigating insider risk.

As an example of such close engagement, a leading university research laboratory has created an insider threat program that is "joined at the hip" with HR to "soften" the organization's interactions with potential insider threats. HR notifies the insider threat program prior to critical events, such as involuntary terminations, which enables the insider threat program to prepare HR for specific concerns. This exchange of insights allows HR to effectively reduce the chance of provoking a negative reaction from the departing employee.

BENEFITS TO HR PROGRAMS

Close collaboration between HR and insider threat programs can facilitate interventions that prevent or mitigate potential insider threat incidents. A strong partnership between HR and insider threat programs can help advance HR professionals' ability to effectively conduct employee onboarding, off-boarding, and performance/behavior evaluations and actions. This will also help ensure the insider threat program develops and analyzes risk indicators that focus on the "whole" of an employee.

Among the benefits to HR resulting from closer coordination with Security and insider threat programs are:

Identifying Risks. HR manages data that are key for insider risk modeling and analysis. However, many HR departments do not include a data analysis component. While applying appropriate privacy protections, the insider threat program could add HR-specific data types – for example, onboarding and behavioral indicators HR captures during employment – to its risk modeling. Combined with other risk indicators collected by the insider threat program, these risk models could provide HR with insight into employees who may benefit from intervention. For example, many organizations perform employee climate surveys, and HR often manages this data. insider threat programs could recommend concepts and questions for inclusion in such surveys that could provide a more complete picture of employee wellness. In aggregate, these results can help pinpoint risks in specific departments or identify sources of employee stress.

A more informed hiring process. An insider threat program's involvement in vetting, or input to the policies governing vetting, could prevent problematic hires before they join the organization in the first place. Key risk data arising from initial vetting and background checks in the pre-hire screening process can provide "early warning indicators." According to the *Common Sense Guide to Mitigating Insider Threats* published by Carnegie Mellon University's CERT Program, "An organization's approach to reducing its insider threat should start in the hiring process. Background checks on prospective employees should reveal previous criminal convictions, include a credit check, verify credentials and past employment, and include discussions with prior employers regarding the individual's competence and approach to dealing with workplace issues."[18] In describing a major success story for HR-Security stakeholder coordination, one of our interviewees, as Director of the Insider Risk Management Program at a major aerospace firm, noted that their hiring managers have contacted their insider threat program with questions on potentially risky or "odd" information they received when reviewing potential candidates. This early assessment of potential risk allows HR to make a more informed holistic assessment of the candidate.

A more informed understanding of employee support needs. Beyond the onboarding of a new hire, HR needs to remain fully integrated with the insider threat program's actions throughout an employee's career. While HR can adequately support some problems on its own – for example implementing Employee Assistance Programs and addressing employee wellness – advanced involvement with insider threat programs can help HR better understand how to guide a troubled employee through tough times and away from the critical pathway.[19] According to CERT, "Employees with issues need a way to seek assistance within the organization. Employees must be able to openly discuss work-related issues with management or HR staff without fear of reprisal or negative consequences." For example, one company with a proven insider threat program also utilizes relevant CE findings to allow their HR program to engage personally with the employee at risk, providing accommodations or help if needed. This company has developed emotional wellness plans, building in part from insider threat observations and including details on who and how to engage with the employee in order to best assist them.

A more informed approach to HR education and training programs. Insights into employee behavior could help drive HR education and training programs to ensure that staff receive information that is relevant to their experience in the organization.

A more informed approach to performance management. Collaboration between HR and insider threat programs will provide HR professionals with insights into employee behavior that allow them to more effectively engage in performance management. If Security observes an employee exhibit in counterproductive behavior, for example, it can work with HR to address these concerns in discussions with that employee's management team or in an employee's performance review. Such intervention may facilitate an end to the employee's concerning actions before they cause damage to the organization.

BENEFITS TO INSIDER THREAT PROGRAMS

A strong partnership between an organization's insider threat program and HR can yield many benefits:

Identifying concerning behavior and performance issues. HR is in the best position to track concerning behaviors and performance issues identified by management or co-workers. Information available from performance evaluations, such as decline in performance, as well as complaints about employees can be shared with the insider threat program to warn about potentially disgruntled or troubled employees.

Fostering constructive collaboration. HR can assist Insider Risk Programs throughout the investigative process as well. For instance, a senior industry executive notes that HR often notifies its insider threat program counterparts on precipitating events that could cause disruption. Conversely, the insider threat program will often go straight to HR to deal with an issue they found through their triage process. This collaboration allows HR to utilize its established relationship with the manager to build rapport and assist in the risk assessment. If the insider threat program is going to interview an employee, they ensure that HR is aware and/or involved to certify that all appropriate steps are taken in case further (or punitive) action results. This partnership has raised awareness within the company, to the point that involving the insider threat program is a natural part of HR processes and conversations.

ORGANIZATIONAL BENEFITS

Companies invest significant resources in their employees' success. By integrating HR into insider threat programs, they can protect these investments by providing positive incentives to employees, instituting policies that protect the company and its employees, and taking proactive actions to prevent potential insider threat events.

Among the benefits are:

Positive incentives. Positive employee incentives may improve morale and productivity, increase employee satisfaction, and ultimately decrease the likelihood of insider risk. Examples of positive incentives managed by HR include fair alignment of compensation internally and with industry standards, transparent criteria for promotions and awards, regular employee orientation and mentoring, EAPs, and professional development programs. The insider threat program can use its understanding of potential risks to support HR's design of these programs.

A better understanding of organizational vulnerabilities exposed by insider threat investigations. Ongoing investigations generate insights into the types of projects, data, and facilities that may be at heightened risk from employees seeking to engage in theft, espionage, or sabotage. These insights can help Security, Information Technology specialists, and others better protect the potential targets of nefarious behavior.

Balancing privacy and security. Collaboration between HR and insider threat programs can help ensure the company's critical assets remain secure while protecting employees' privacy and civil liberties. Privacy protections – for example, limiting who can access information on employees' network usage – would increase employees' confidence in the organization and encourage employee engagement with the insider threat program. According to an official from one large company, collaboration between HR and insider threat staffs enabled HR to see how often employees stole corporate Intellectual Property (IP). This company's insider threat program worked with HR to improve the way it communicated departing employees' obligations to protect IP during off-boarding discussions, transforming a five-page legal document to a single color-coded slide that made important information easier to discern. The insider threat program saw fewer data exfiltration incidents from departing employees after working with HR to make these changes.

Gaining support of union leadership. Communicating the benefits of whole-person and supportive employee risk-monitoring strategies can help secure the support of union leadership and members. According to one industry expert, the prevailing myth is that the insider threat program "can't do anything" because "it's too difficult to work with the union." The reality is often that the insider threat program simply needs to become educated on the particulars of the union contract and engage with union leadership on how to work with them. Common issues include consent to monitoring, limits on investigative activities, and prohibitions on interaction with bargaining unit employees without a union representative present. Through effective collaboration, an insider threat program can improve its understanding of employees, and a labor union can help its members take advantage of employee support programs.

CONCLUSIONS

HR is not only inextricably linked to a comprehensive insider threat program, but also the best equipped functional area to maximize insider threat programs. Some of the most robust insider threat programs utilize HR resources as the first line of defense in support of an early warning strategy because of their insights into, and advocacy for, troubled employees. The "first-in" HR team's more complete view of the individual enables it to mitigate risks quickly compared to a supervisor or security team member who lacks this information. Engaging HR prevents reactive and hasty conclusions originating from technical monitoring or post-exploit forensics. In many cases, HR is also the most knowledgeable of organizational programs and resources to help the potential insider threat find an off-ramp from the critical pathway.

REFERENCES

[1] *Intelligence and National Security Alliance, "Explanation of INSA-Developed insider threat Definition," December 3, 2015. At https://www.insaonline.org/wp-content/uploads/2018/10/INSA_InsiderThreat_definition-Flyer.pdf.*

[2] *Intelligence and National Security Alliance, Categories of insider threats, October 2019. At https://www.insaonline.org/wp-content/uploads/2019/10/INSA_WP_Categories_of_Insider_Threats-1.pdf.*

[5] *Lindy Kyzer, "Periodic reinvestigations are out, continuous vetting is in for security clearance holders," Government Executive, March 11, 2020. https://www.govexec.com/management/2020/03/periodic-reinvestigations-are-out-continuous-vetting-security-clearance-holders/163695/*

[6] *Eric D. Shaw & Lynn F. Fischer, Ten Tales of Betrayal: The Threat to Corporate Infrastructures by Information Technology Insiders: Analysis and Observations. Monterey, CA: Defense Personnel Security Research Center, TR 05-13, September 2005. At https://www.dhra.mil/Portals/52/Documents/perserec/tr05-13.pdf.*

[7] *U.S. Department of Justice, "Former IT Employee of Transcontinental Railroad Sentenced to Prison for Damaging Ex-Employer's Computer Network," press release, February 13, 2018. At https://www.justice.gov/opa/pr/former-it-employee-transcontinental-railroad-sentenced-prison-damaging-ex-employer-s-computer.*

[8] *United States of America v. Christopher Victor Grupe, Indictment, CR-1790-PJS/DTS, U.S. District Court, District of Minnesota, April 11, 2017. At https://regmedia.co.uk/2018/02/14/grupe.pdf.*

[9] *Intelligence and National Security Alliance, Legal Hurdles to Information Sharing, January 2020. At https://www.insaonline.org/wp-content/uploads/2020/01/INSA_WP_Legal-Hurdles_FIN.pdf.*

[10] *Eric Shaw, Kevin G. Ruby, Jerrold M. Post, "The Insider Threat to Information Systems," Security Awareness Bulletin, 2:98 (1998), pp. 27–47. At http://www.pol-psych.com/sab.pdf.*

[11] *Shaw and Sellers.*

[12] *"Living Paycheck to Paycheck is a Way of Life for Majority of U.S. Workers, According to New CareerBuilder Survey," press release, August 24, 2017. At http://press.careerbuilder.com/2017-08-24-Living-Paycheck-to-Paycheck-is-a-Way-of-Life-for-Majority-of-U-S-Workers-According-to-New-CareerBuilder-Survey.*

[13] *Graphic from IFEBP, Financial Education for Today's Workforce: 2016 Survey.*

[14] *Adjudicative Guidelines for Determining Eligibility for Access to Classified Information," 32 CFR 147. At https://www.govinfo.gov/content/pkg/CFR-2012-title32-vol1/xml/CFR-2012-title32-vol1-part147.xml#seqnum147.1*

[15] *Tom McMurtrie, "insider threats: Taking a Holistic Approach to Protecting Agency Data," Federal News Network, December 27, 2017. At https://federalnewsnetwork.com/cybersecurity/2017/12/insider-threats-taking-a-holistic-approach-to-protecting-agency-data/.*

[16] *See Eric Shaw and Laura Sellers, "Application of the Critical-Path Method to Evaluate Insider Risks," Studies in Intelligence, Vol. 59, No. 2 (2015). At https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-59-no-2/pdfs/Shaw-Critical%20Path-June-2015.pdf.*

[17] *For a discussion of counterproductive work behaviors, see Intelligence and National Security Alliance (INSA), Assessing the Mind of the Malicious Insider: Using a Behavioral Model and Data Analytics to Improve Continuous Evaluation, April 2017, pp. 5-6. At. https://www.insaonline.org/wp-content/uploads/2017/04/INSA_WP_Mind_Insider_FIN.pdf.*

[18] *Software Engineering Institute, Carnegie Mellon University, Common Sense Guide to Mitigating insider threats, Sixth Edition (CMU/SEI-2018-TR-010), December 2018. At website: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=540644.*

[19] *Shaw and Sellers.*

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

ACKNOWLEDGEMENTS

INSA expresses its appreciation to the INSA members and staff who contributed their time, expertise, and resources to this paper.

INSA MEMBERS

Vinny Corsi, *IBM; Insider Threat Subcommittee Chair*

Julie Ard, *Noblis*

Kris Brost, *AC Global Risk*

Frank Greitzer, *PsyberAnalytix*

Mike Hudson, *ClearForce*

Daniel McGarvey, *Alion Science & Technology*

Kim Mix, *Leidos*

Kathy Schwab

Sue Steinke, *Perspecta*

INSA STAFF

Suzanne Wilson Heckenberg, *President*

John Doyon, *Executive Vice President*

Larry Hanauer, *Vice President for Policy*

Peggy O'Connor, *Director, Communications and Policy*

Caroline Henry, *Marketing & Communications Assistant*

Megan Anderson, *Intern*

Rachel Greenspan, *Intern*

ABOUT INSA

The Intelligence and National Security Alliance (INSA) is a nonpartisan, nonprofit trade association dedicated to advancing collaborative, public-private approaches to intelligence and national security priorities. Through the application of industry expertise, leading-edge academic research and commercial best practices, INSA seeks to make the Intelligence Community more effective and efficient. Our 160+ member organizations and its 4,000+ individual and associate members include senior executives and intelligence experts in the public, private and academic sectors.

ABOUT INSA'S INSIDER THREAT SUBCOMMITTEE

INSA's insider threat Subcommittee researches, discusses, analyzes, and assesses counterintelligence and insider threat issues that affect government agencies, cleared contractors, and other public and private sector organizations. The Subcommittee works to enhance the effectiveness, efficiency, and security of government agencies and their industry partners, as well as to foster more effective and secure partnerships between the public, private and academic sectors.