



INTELLIGENCE AND
NATIONAL SECURITY
ALLIANCE



SEPTEMBER 2021

Managing Insider Threats in a Remote Work Environment: *Lessons from the Pandemic*

Presented by

INSA'S INSIDER THREAT SUBCOMMITTEE

Building a Stronger Intelligence Community

EXECUTIVE SUMMARY

Remote work is here to stay. Given that large numbers of government and private sector employees have come to value the flexibility remote work offers, many organizations have taken steps to expand its use. As organizations revise policies and procedures to accommodate wider use of remote work, they must consider new approaches to insider threat programs.

This paper provides observations based on expert-level interviews on how the shift to remote work during the COVID-19 pandemic affected Insider Threat Programs (InTPs) and makes recommendations for mitigating problems created by continued widespread remote work. INSA researchers conducted interviews with security professionals in the U.S. Government (USG) and the private sector.

The widespread use of remote work during the COVID-19 pandemic created enhanced security risks. Isolation and personal pressure created psychological stressors for employees. Reliance on home Internet connections, cloud storage, and new software tools created information security vulnerabilities that could be exploited by outside hackers or malicious insiders. These new challenges required Insider Threat managers to employ creative and proactive mitigation strategies involving information technology (IT) modifications, new analysis and risk assessment capabilities, and enhanced training and awareness programs for officials at all levels.

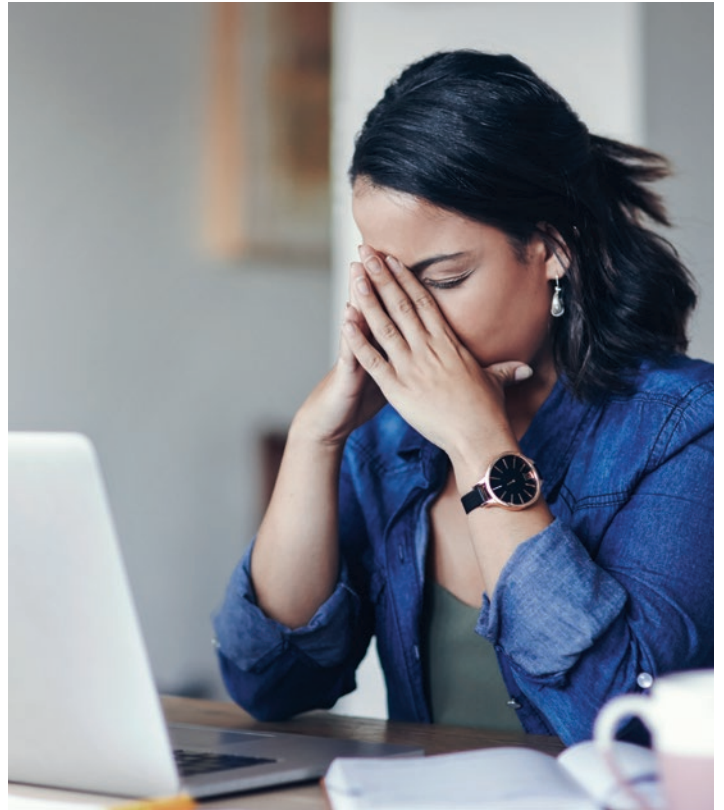
Insider threat risks in a remote work environment can be mitigated through a number of measures on the part of InTP managers, human resources officials, supervisors, and senior leaders. Organizations must clearly define and communicate security requirements, and they must also provide office equipment and other supplies that employees need to comply. All employees should receive enhanced insider threat awareness training, and InT messages should be reinforced through regular employee communications. Managers should be given tools and training to connect with remote staff. In particular, they should be encouraged to engage in regular "wellness checks" with their team members and provide staff with resources – from access to enhanced Employee Assistance Programs (EAPs) to permission to take time away from their computers – to reduce stress, remain connected to the organization, and seek help when needed.

OVERVIEW

The COVID-19 pandemic changed the nature of work, as both public and private sector employers found ways to continue operations with employees working remotely wherever possible. Even those who were fortunate enough to continue working uninterrupted throughout the pandemic experienced isolation and stress. Beyond the workplace, the United States in 2020 and early 2021 experienced racial tensions, civil unrest, and a highly charged presidential election – all on top of a once-in-a-century public health crisis that caused hundreds of thousands of deaths and pushed the public health system to the brink of collapse. These factors contributed to an environment in which all Americans experienced increased stress, fear, and uncertainty.

For employers, these challenges highlight the importance of a strong and adaptable Insider Threat Program (InTP) designed to detect warning signs that an employee might act in a destructive way toward his/her organization and its staff. Such programs became even more critical during the pandemic, as remote work became a virtual requirement for most office workers for more than a year (March 2020 through Summer 2021). Employees' dispersal made it more difficult for supervisors and co-workers to notice changes in employee behavior. As many organizations appear positioned to continue offering work from home (WFH) options even as business operations return to a "new normal," they will need to continue assessing employees from a distance.

This paper provides observations based on expert-level interviews on how the COVID-19 pandemic has affected Insider Threat Programs and makes recommendations on how to mitigate challenges



created by this unique phenomenon. INSA interviews with security professionals in the U.S. Government (USG) and the private sector suggest that the impacts of the pandemic on corporate security and Insider Threat (InT) programs will extend long beyond the health crisis. Nearly all organizations adapted their InT capabilities, controls, policies and practices, which yielded, for many, increased productivity. These new approaches to risk analysis and mitigation are likely here to stay.

THE CHALLENGES



As the pandemic hit and organizations sent their employees to work from home, InTP managers faced the need to monitor workers' behavior from a distance. This new security paradigm presented five key challenges.

CHALLENGE 1

Adapting the Information Technology (IT) Environment

The swift change to a WFH environment for nearly all employees in March was a challenge for both government and industry organizations. Commercial companies that had previously introduced some measure of WFH capability had an easier time deploying it to their entire workforce than organizations – like many federal government agencies – that had virtually no pre-pandemic remote work policies or infrastructure. Such organizations adapted to the opportunities remote work presented, but the rapid implementation of remote work practices often strained their technology, security, and InT capabilities.

Information Technology (IT) and Information Security (IS) departments bore a heavy burden to add capabilities and controls to support secure remote work. The new environment created vulnerabilities and concerns for InTPs that ranged from new logs and alerts that needed to be analyzed to new behavior patterns for individual employees.

In addition, high expectations and significant technical and security risks created a high stress environment for IT and IS professionals trying to deliver solutions. Many were privileged users with accesses that affected the confidentiality, integrity and availability of critical systems. The fact that “superusers” with privileged access were themselves under increased stress increased insider threat concerns. Such employees should be subject to careful user activity monitoring (UAM) and also regularly engaged by supervisors to keep them connected to the organization.

The daily work priorities for many information security and InT professionals shifted away from detecting and responding to threats to delivering new capabilities and adapting to their use. This shift away from threat detection and response temporarily increased the risk of exposure from both external and internal threats. With remote work now fully integrated into most organizations' operations, policies for information and data access should be in place, and InT teams can return their focus to threat monitoring.

CHALLENGE 2

Adjusting to Remote Employees and Teams

All teams reported an increased reliance on additional technological tools and maximizing the use of encrypted emails and audio/video conferencing capabilities to ensure business operations could be sustained. InTP managers conducting investigations had to rely on virtual interviews and engagements, rather than travel and in-person meetings. Several companies reported anecdotally that they did not see a diminution in the effectiveness of their InT programs. One program manager stated: "While we lose the benefit of physical face-to-face interaction, the ease of scheduling and completing virtual interviews increases the number we can accomplish in a short period of time." While it may be easier to schedule larger numbers of interviews virtually, however, interviews not conducted face-to-face may have been less effective or revealing.

Some InTP managers reported that the need to proactively engage stakeholders using virtual tools helped build relationships with other units in the organization. Such efforts increased trust and improved support during investigations. Some corporate entities refined business processes to better integrate Human Resources, legal, and line managers, thereby facilitating information-sharing and reporting. Others improved training and awareness to improve understanding of what an insider threat is, how to identify behavioral indicators, and how to report concerns. More robust inter-departmental collaboration led to reviews of policies that enhanced security; some companies reported taking actions like zero-based reviews on policies related to remote workers' handling of data, computer and network use/access, use of cloud and removable media, and device security, while others reviewed policies on hiring, employee monitoring, and termination.

For the USG, obstacles to face-to-face interaction created opportunities for training and conferences conducted virtually. An excellent example is the Insider Threat Detection and Analysis Course (ITDAC), hosted by the Defense Insider Threat Management

Analysis Center (DITMAC), which cleared a backlog of pending attendees and graduated 85 personnel from across the USG in fiscal year 2020. In contrast, some companies report that training has been less effective due to lack of visual observation, a decrease in overall engagement, and a limited ability to establish the trust and relationships typically fostered by in-person interactions.



Information Technology (IT) and Information Security (IS) departments bore a heavy burden to add capabilities and controls to support secure remote work. The new environment created vulnerabilities and concerns for InTPs that ranged from new logs and alerts that needed to be analyzed to new behavior patterns for individual employees.

CHALLENGE 3

Psychological Impacts

Long-term psychological impacts are much harder to address because there is not a common approach for InTPs to gauge these stressors. As it became increasingly clear that WFH would continue, feelings of isolation, psychological angst, and uncertainty about the future impacted personnel performance. Personal stressors including health, job security, finances, and challenges with childcare and eldercare became magnified. InTP monitoring led many organizations to observe a spike in their threat assessment activity from keyword searches or posts to internal, organization-wide social media platforms.

At the same time as the nation was weathering the unprecedented COVID-19 pandemic, heightened racial tensions and a contentious presidential election contributed to social unrest across the country. One USG program manager highlighted these non-health dynamics as sources of psychological stress for employees:

“Generally, yes, (we are at a greater risk) but that is due not just to COVID, but to the myriad of other activities which have taken place over the past year, including increased periods of unrest and various socio-political challenges. These extended periods of difficulty can cause great stress and uncertainty and the result can lead some to a sense of feeling overwhelmed, out of control or defeated. When individuals reach this point, if left unaddressed, it could weaken resilience and then translate to increased risk across our organization from insiders.”

Many organizations increased mental health and physical wellness measures in order to reduce stress and undue burdens on WFH employees. For instance, one company stopped doing meetings on Fridays, while other companies invested more in Employee Assistance Programs (EAPs). Some programs have embraced a “whole person” approach and have implemented increased mental health and well-being services to reduce stressors that may lead to insider threats. One company interviewed has integrated its EAP with its InTP, leveraging risk indicators to offer specific and relevant assistance to employees. The result is transparent InTP and EAP programs that can proactively inform and assist.

The risk of missing indicators increases any time a company loses capacity to observe its employees directly and engage its workers personally. In such circumstances, data that can be observed becomes even more important. While the pandemic certainly created greater physical, psychological, emotional, and financial stress on employees, there is no data to indicate that these stressors created risks that would be displayed. While some individuals and families were visibly affected – for example, public health data shows an increase in domestic violence reports in 2020 and early 2021 – others may have kept their stress under wraps.

Emotional, financial, interpersonal, and even socio-political stressors can amplify behaviors that indicate a potential insider threat. But with limited physical interaction to monitor behavior and identify anomalies, InTPs must rely on different methods to identify potential red flags.



The inability to interact in-person led employees to communicate electronically, which increased the amount of data being stored, used, maintained, and disseminated.

CHALLENGE 4***Changing Threats***

Early in the pandemic, some organizations noted an increase in data hoarding due to job security concerns. Employees fearing that they may be furloughed or laid off tried to exfiltrate useful data, “just in case” they might need it for a job search or to assist in subsequent employment. As staff remained in their positions – and were reminded to maintain best information management practices – data hoarding decreased.

The inability to interact in-person led employees to communicate electronically, which increased the amount of data being stored, used, maintained, and disseminated. This includes increased email traffic, instant messages (via Teams, Jabber, Slack, etc.), text messages, phone calls and video conferences. The increased use of these methods of communication resulted in more tangible, and potentially sensitive, data being shared or stored electronically. In addition, WFH – in an environment that is not configured ideally for sound data security practices, and in which professional and personal papers and data are easily mixed – raised the risk of inadvertent mishandling of sensitive information.

Companies found it more difficult to secure data when remote employees left the organization. Indeed, more laid-off or furloughed individuals were observed attempting to indiscriminately capture data, regardless of whether it was of high value. Further, when offboarding employees working remotely, employers found it challenging to collect company-owned and government-issued electronic devices.

CHALLENGE 5***Adjusting Tools and Analytical Capabilities***

New or continued COVID-19 budget constraints eliminated or postponed many organizations’ plans to acquire new analytic tools and capabilities. Analytical tools in place needed to be adjusted, either updating rules or behavioral baselines for the new WFH environment and practices. While no single improvement was identified as a focus area for risk mitigation, many InTPs indicated that a shift to more predictive data and models provided awareness of situational stressors, which become issues when compounded by prolonged WFH.

There is no one-size-fits-all approach to a predictive InTP model, and it is unlikely that large organizations can adapt a uniform strategy when addressing the entire workforce. While programs need to find the best fit for their unique needs, managers and peers have become increasingly important in mitigating insider threat issues as WFH continues.

Both corporate and government officials indicated they adjusted the use of analytical tools required to effectively evaluate the new operating environment. Before such adjustments, one interviewee stated, an increase in false-positive alerts consumed a disproportionate amount of security resources.

OBSERVATIONS AND RECOMMENDATIONS

OBSERVATION 1 // Both corporate and government InT programs are challenged by devising and implementing solutions designed for long-term remote work.

RECOMMENDATION 1

Update security standards to address remote work risks and provide training and equipment needed for compliance.

Agencies and companies must address the reality that some degree of WFH will become a permanent practice and equip the workforce for full- or part-time remote work. Well-defined and clearly communicated standards, accompanied by resources and equipment needed to comply with them, can ensure security and productivity while taking advantage of the greater flexibility that employees have come to expect.

Leadership should develop standard operating procedures for working securely at remote locations, train all employees in best practices, and reinforce these practices through regular communication. Factors to consider must include secure printing and data storage, secure destruction of data and hard copy documents, updating and maintaining internet security for home-based devices, and defining conditions for working outside of one's home network, like in a coffee shop or a publicly accessible co-working space. Organizations should be prepared to provide employees with equipment or subsidies needed to implement these standards, such as Wi-Fi routers that meet an organization's security requirements and high-quality cross-cut or micro-cut document shredders. Since remote employees may work offline more frequently than office-based employees, laptops and other devices may need to be configured to monitor access to locally stored data to detect if employees print documents or download data to a portable storage device while disconnected from the network.

RECOMMENDATION 2

Update insider threat training programs to address risks from employees working remotely on a regular basis.

Long-term or frequent remote work creates unique psychological stressors on employees and hinders the ability of managers and co-workers to notice signs of stress. Organizations should revise InT training programs to teach all employees about potential stressors and their indicators; promote employee assistance programs (EAPs) that staff members can access confidentially to deal with stressors as they arise; and ensure that all employees know how to seek help from, and report concerns to, managers and human resources executives.

RECOMMENDATION 3

Collaborate with communications teams to develop creative or innovative insider threat messaging and awareness campaigns specifically for remote personnel.

Insider threat programs should draw on communications and marketing teams to improve information dissemination and workforce engagement. Each agency or company should customize messaging to reiterate organizational standards and best practices, like encrypting sensitive information, urging personnel to report phishing, and providing regular updates on department-wide initiatives. When many employees work remotely, organizations should make security and InT messaging routine elements of their employee outreach.

RECOMMENDATION 4***Ensure privacy and security programs utilize the latest security technologies.***

Remote work has increased the amount of data that is created and stored within each device. Government agencies and contractors should prioritize system compliance by conducting a current state assessment of their programs and systems, identifying gaps in their procedures, and taking measures to remediate these risks. Developing a strong privacy and security program with actionable best practices is vital to securing data and sensitive information.

**RECOMMENDATION 5*****Ensure WFH environments are updated to protect company devices and data while operating on private and public networks.***

Remote work has increased the amount of data that is transmitted across organizations' networks as employees are changing where and how they connect to the network and access data. Government agencies and contractors should continue to prioritize cybersecurity by conducting a current state assessment of their programs and systems, projecting near and far-term needs, identifying gaps in their procedures, and implementing measures to remediate these risks. Continually improving IT cybersecurity programs with actionable best practices is vital to securing data and sensitive information.

RECOMMENDATION 6***Provide managers and project leaders with tools, techniques, and training to engage their team.***

Nothing replaces human interaction. With continued WFH, managers and project leaders have the added responsibility of engaging their teams in a mostly online environment. Leaders should prioritize knowing their employees and building teams by incorporating teambuilding exercises, like virtual lunches or coffee hours, and encouraging personnel to turn their cameras on during weekly or monthly staff meetings. Managers should reinforce security and InT messages at staff meetings and other gatherings, to include references to EAPs and other resources. At the same time, firms and the USG should equip managers, project leaders, and human resource executives with training on how to recognize concerning behavioral patterns among remote workers and how to intervene with employees demonstrating concerning behavior.

OBSERVATION 2 // Long-term negative psychological impacts of remote work are still emerging but can and should be addressed proactively.

RECOMMENDATION 7

Periodically push communications to remote employees on possible scenarios that increase InT risks and suggest solutions that help employees mitigate these risks.

Employees working remotely have many different reactions to being physically and socially distanced from their office and their co-workers. Some thrive on the independence and absence of distractions, while others – even if they like the flexibility of remote work – miss the teamwork and camaraderie of being in a shared workspace. Organizations can provide resources to the latter group – tip sheets, morale-focused memos, or even short videos – to help them cope with the added stress of working remotely. The key is to give employees actionable suggestions for reducing stress and maintaining connections to their team members, while letting them know that the organization is looking out for their well-being.

- Managers can encourage employees who feel isolated to meet a colleague for coffee or lunch (while following COVID-related mitigation strategies) to share information, brainstorm, or share struggles in adjusting to the new work environment. An employee who doesn't feel comfortable meeting in-person could schedule a "Zoom coffee" with one or more co-workers to catch up and re-establish a rapport. Managers should affirm that the organization sees such engagements as productive and may want to allow staff to bill such lunches or coffees to the organization if accounting rules allow.
- Similarly, organizations can encourage employees who have difficulty keeping a work routine to reimplement their pre-COVID workday schedule. Set an alarm, dress as though you're going to the office, and call or video-conference a co-worker just as one might "pop into" his or her office for an impromptu discussion. Set schedules for the start of the workday, lunch, breaks, and the end of the workday, as such boundaries can help avoid burnout and Zoom fatigue.

RECOMMENDATION 8

Encourage or require manager-employee 1:1 wellness check-ins.

Senior leadership should mandate periodic one-on-one meetings between managers or project leaders and their team members to ensure that someone in a supervisory role has "eyes on" every employee at regular intervals. (Such interactions are sound management practices, as well as opportunities to assess InT risks.) It is particularly important to engage employees with extensive information access – such as network "superusers" – to provide regular oversight of staff members who could use their access to sensitive data to cause significant damage to the organization. Human resources and internal communications teams, working together, should equip managers with necessary training to detect signs of COVID-19 or WFH burnout and determine options for mitigating stress, dissatisfaction, and potential security risks.

RECOMMENDATION 9

Consider establishing a "COVID-19 Burnout" hotline or online equivalent that employees can use for generating ideas, resources and offering or receiving solutions, and ensure that managers assess employee concerns.

Human resources divisions should ensure all employees are aware of resources to seek help or advice. EAPs should be prepared to address feelings of isolation, overwork, and other symptoms of "COVID burnout". IT teams can create internal message board channels on which employees can share tips for dealing with WFH challenges and let each other know that others share their experiences. Intranet home pages can link to resources such as tips to avoid burnout, Q&A regarding leave and time off, mental health resources, and WFH best practices. Executive leadership and management discussions should review employee observations and feedback and assess whether existing programs should be modified or improved.

RECOMMENDATION 10


Consider “paid time off” during the workday for employees to engage in physical and mental health or wellness programs.

Work with communications teams to ensure that employees know what resources are available to them. In addition, if employees can be flexible in their exact work hours, they can be encouraged to take a break during the day for personal wellness and make up the time later.

CONCLUSION

Many organizations figured out how to continue operations – and even to thrive – by shifting to remote work during the pandemic. The adjustment included changes to work flow – for example, separating out unclassified tasks that could be done remotely so only a more limited number of classified tasks required in-office work – as well as new technologies, such as secure remote software that allowed classified work from outside a secure facility. As necessity is the mother of invention, many organizations innovated to meet unforeseen requirements.

Remote work is here to stay, as large numbers of government and private sector employees have come to value the flexibility it offers. Most organizations will have to create policies and procedures for incorporating some degree of remote work while maintaining performance standards. Such changes also require new approaches to insider threat programs. Agency leaders, corporate executives, and project managers have creative possibilities to consider as they and their teams adjust to new workplace norms. A hybrid workplace that incorporates WFH will require updated security and insider threat measures to ensure the most safe and secure work environment possible.

The most encouraging observation from the COVID-19 pandemic is that resilient organizations find ways to maintain core functions like InTPs even in the face of unforeseen disruptive events. Adjustments are always necessary, and organizations must be adaptable. However, a well-rounded Insider threat program will provide a foundation that can adjust to changes in the work environment. 



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

Sue Steinke, *Peraton*;
Insider Threat Subcommittee Vice Chair

Julie Coonce, *TransUnion*

David Sanders, *Haystack*

Lina Abisoghomyan, *Deloitte*

Megan Anderson, *Deloitte*

Jacqueline Schultz, *Deloitte*

INSA STAFF

Suzanne Wilson Heckenberg, *President*

John Doyon, *Executive Vice President*

Larry Hanauer, *Vice President for Policy*

Peggy O'Connor,
Director of Communications and Policy

Britany Dowd,
Marketing and Communications Assistant

Rachel Greenspan, *Intern*

Cassie Crotty, *Intern*

Ali Berman, *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.