



# COMPONENTS OF EFFECTIVE INSIDER THREAT TRAINING

**INTELLIGENCE AND NATIONAL SECURITY ALLIANCE**

Insider Threat Subcommittee

October 2019



INSIDER THREAT  
SUBCOMMITTEE



## ACKNOWLEDGEMENTS

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

### INSA MEMBERS

Sandy Maclsaac, *Deloitte; Subcommittee Chair*

Vince Corsi, *IBM; Subcommittee Vice Chair*

David Denning, *Northrop Grumman*

Julie Coonce, *TransUnion*

Lee Armstrong, *Harris*

Tom Read

### INSA STAFF

Chuck Alsup, *President*

Larry Hanauer, *Vice President for Policy*

Peggy O'Connor, *Policy & Communications Director*


Caroline Henry, *Marketing & Communications Assistant*

Megan Anderson, *Intern*

Jessica Willmore, *Intern*

## EXECUTIVE SUMMARY

Harmful acts by trusted employees—including both malicious acts involving theft of information, sabotage, or workplace violence and unintentional breaches—can dramatically affect an organization's finances, reputation, and workplace culture. Many large organizations have extensive technical surveillance programs in place to identify malicious insiders by scrutinizing their workplace computer network usage, data downloads, and email habits. But savvy actors can get around such technical hurdles, and many technical monitoring programs are useful principally as forensic tools to investigate a breach that has already occurred. The most effective sentinel to guard against insider threats is an informed and motivated co-worker who is: aware of the damage insiders can cause, trained to recognize the indicators of aberrant behavior, taught to identify characteristics of external social engineering techniques that lead to unintentional breaches, cognizant of how to share concerns with an established reporting chain, and motivated to protect the organization. An established and reinforced education and awareness program that addresses insider threats and encourages the positive benefits of a reporting culture is the most effective defense against insider threats.



The unauthorized release of classified information can cause extensive damage to U.S. national security; the theft of intellectual property can devastate a company that invested years of staff time and resources in its work; and trusted insiders who feel mistreated or wronged can lash out at their co-workers, engaging in threatening or violent behavior at the workplace.

## BACKGROUND

When trusted insiders steal valuable information from their employers, whether classified national security information from a government agency or proprietary R&D from a private company, the impact can be devastating: The unauthorized release of classified information can cause extensive damage to U.S. national security; the theft of intellectual property can devastate a company that invested years of staff time and resources in its work; and trusted insiders who feel mistreated or wronged can lash out at their co-workers, engaging in threatening or violent behavior at the workplace. While many organizations have instituted comprehensive insider threat programs, others – particularly smaller companies with fewer resources – have limited or immature insider threat programs, if any at all.

Technical solutions can be put in place to identify suspicious behavior before a trusted employee can cause harm, as well as to build a prosecutable case after the discovery of a breach. However, an effective insider threat program also depends heavily on informed, alert and observant employees willing to report their suspicions for the good of the company. Employees must be trained to identify concerning behavior, and organizations must establish mechanisms for reporting concerning behavior that work effectively in their organizational structures and cultures. Employees must also be trained to recognize suspicious social media exploits such as phishing emails designed to enable unauthorized individuals to gain access to valuable company resources. Different types of training – in-person, online, and hard copy reading materials – have varying degrees of effectiveness depending on the size, geographic dispersion, and culture of the organization.

This paper examines who needs to be trained on insider threats and why; the elements of effective insider threat training, the advantages of different types of training; and the resources that are available to insider threat program managers. It also examines why technology alone is not the panacea it is made out to be, and why employee buy-in is critical.

## ORGANIZATIONS RELY TOO HEAVILY ON TECHNOLOGY

Since many data thefts now involve terabytes of electronic information rather than photocopies of paper documents, many post-mortem discussions of insider threats conclude that better monitoring of computer network behavior would have prevented a loss. Similarly, since many people who exhibit violence in the workplace express violent thoughts online, it is easy to believe in hindsight that more robust monitoring of social media or email would have enabled an organization to help its troubled employee before he or she harmed anyone.

Technical monitoring solutions can always be improved, and many software tools are available – at significant cost – to monitor user network activity, analyze emails for latent sentiment or aberrant language, and collect open source data of employee behavior outside the workplace. Such tools, it is hoped, will raise “red flags” to help identify the next potential malicious insider. Companies and government agencies – which often rely heavily on technology in their core business lines – are often willing to spend significant sums in search of the magic algorithm, software tool, or compilation of data points that will avert a crisis. Smaller firms, however, may not be able to dedicate resources for such technical solutions.

However, in some of the most high-profile and high-value thefts of information by trusted insiders, technical solutions failed to alert anyone to suspicious patterns of activity or to the theft of data, though they were often utilized to build a prosecutable case after the discovery of the breach. One example is the extremely high profile case involving former NSA contractor Reality Winner, who printed a Top Secret document regarding alleged Russian interference in the U.S. election and provided the document to the *Intercept*, an online news publication. Within hours of the article’s publication, authorities backtracked the information, determined who had access and who had exfiltrated the information from the network, in this case to a copy machine/printer. NSA determined six personnel had printed the document, and a review of internal networks revealed Winner had

exchanged email messages with the *Intercept*. While the FBI and NSA quickly solved the exfiltration and arrested the “insider,” no internal procedure or tool detected the exfiltration at the time of its occurrence and/or alerted internal security procedures. Had Ms. Winner been a spy handing the document to a hostile intelligence service – as opposed to a leaker seeking to get the material openly published – this particular theft of classified information might never have been discovered.

While larger organizations often fund technical solutions, they do not always give sufficient attention or funding to labor- and time-intensive training and awareness programs that would teach employees how to spot suspicious behavior by a co-worker. Such programs often consist of little more than mandatory PowerPoint presentations or webinars designed to comply with a regulatory requirement or government security mandate. To make matters worse, these security presentations are frequently provided to overwhelmed employees during initial onboarding or added to an already voluminous list of required online training.

Training and awareness is even more important for smaller organizations with comparatively fewer resources to devote to expensive technical tools. Many such organizations are deep within the supply chains of military services, major defense contractors, and large manufacturers, making them particularly vulnerable “back doors” into important military platforms and complex commercial products.

While relatively “passive” security awareness training methods are the principal means of preparing the workforce to recognize and counter malicious insider threats, more active methods are available for countering unintentional insider threats, such as simulated phishing email campaigns conducted by the organization to both assess the awareness of its staff and to direct remedial training to those who succumb to these simulated threats.



## POPULATIONS TO BE TRAINED

Different types and levels of training may be required depending upon the various roles of employees within the organization. While all employees would benefit from training, there are three general population levels to consider in developing insider threat training and education: Leadership, Insider Threat working groups and staffs, and the general population.

1. **Leadership training** focuses on ensuring that executives have a full understanding of the issues surrounding the impacts of malicious insiders, their own role in developing and enforcing policies, and the critical role they play by reinforcing the organization's messages. A vigilant staff is the result of a vigilant culture, which needs to be created and supported by its leaders. To some degree, leadership training must first convince senior

leaders that insider threat programs are not just a money-losing cost center, but rather a critical insurance policy against intellectual property theft, reputational damage, workplace violence, and potentially large-scale financial losses.<sup>1</sup>

2. **Insider Threat working group members and staffs** charged with handling and/or investigating reports of malicious insiders require both broad and deep training. To enhance their understanding of insider threats, they should be provided training on the psychology of malicious insiders and the motivations that drive people to violate their employers' trust. Case studies from both government and industry would provide real-world examples of scenarios that could manifest themselves in the trainees' organizations.



<sup>1</sup> For more information on why C-Suite executives should value insider threat programs, see Sandy Maclsaac and Chuck Alsup, "Companies Must Invest in More Robust Insider Threat Programs," *Cipher Brief*, June 26, 2018. At <https://www.thecipherbrief.com/column/strategic-view/companies-must-invest-robust-insider-threat-programs>.

To operate effectively within their organizations, insider threat program managers also require an understanding of their organization's policies and guidelines related to its insider threat programs, which include its approach to employee privacy, electronic monitoring, and both physical and network security. Training should make program managers aware of resources that are available to address concerning behavior, such as human resources counseling programs that can help employees cope with stress, personal problems, and financial difficulties. They must also be taught the importance of taking indicators seriously, as failure to act on red flags, including tips from coworkers, can allow problems to grow and reduce the motivation of coworkers to report concerning behavior in the future. Finally, program managers should be given tools for appropriately engaging co-workers who might see preliminary signs of concerning behavior, from line workers and supervisors to human resources staff and members of the information technology team.

3. **The general workforce** must be made aware of the existence of insider threats and taught that the company's health – the security of its information and the safety of its people – requires their continuous awareness. They become the eyes and ears of the organization and can report indicators of suspicious behaviors beyond what can be monitored by sophisticated network tools. They must be taught how they can prevent and confidentially report concerning behavior. They must also be informed about methods used by external threat actors, such as phishing emails that induce staff to inadvertently provide unauthorized access to company resources, as well as cyber hygiene techniques to protect their networks from attacks.

## THE IMPORTANCE OF A COMMUNICATIONS PLAN

Because insider threat awareness is just one of many topics on which employees receive training, the company must develop a communications plan to promote to all employees the importance of the training and to highlight the organization's commitment and expectations. Leadership must clearly express their commitment to countering insider threats and – to encourage employees to report concerning information – to helping employees who need assistance. The more visible leadership support is to the program, the more impact it will have; indeed, research has shown that clear management support for training improves its effectiveness.<sup>2</sup>

The communications plan (and training units) should also clearly convey to employees why insider threats matter to them. Such efforts should explain the threat and the negative impact that malicious and unintentional insiders could have on both the organization and on individual employees (on personal safety, for instance). The impact of insider threats should be made "personal" to promote employee buy-in and engagement. Insider case studies that show real people making real harmful decisions can make insider threat scenarios tangible and relatable.

## TYPES OF TRAINING

Organizations must determine the best approach for initial training and for follow-up refreshers. Seeing insider threats (and sometimes also training and corporate security) as cost centers rather than investments, companies often choose to provide limited security training at the minimum cost required, especially if a principal goal is to comply with an oversight entity's requirement. However, to ensure that insider threat training reaches a diverse workforce that inevitably has a wide range of learning styles, the organization must develop a comprehensive package of initial and ongoing training that combines classroom-style teaching, interactive online training for remote employees and annual or semi-annual refreshers, and reading materials disseminated on a regular basis.<sup>3</sup>

<sup>2</sup> See, for example, Tung-Chun Huang, "The relation of training practices and organizational performance in small and medium size enterprises", *Education + Training*, Vol. 43, No. 8/9 (2001), pp. 437-444. At <https://doi.org/10.1108/00400910110411620>.

<sup>3</sup> For an overview of the effectiveness of different types of training, see Kristen Rich, "State of Employee Training," West UC, blog post, October 14, 2015. At <https://www.westuc.com/en-us/blog/webinars-enterprise-streaming/state-employee-training-infographic>.

Three general types of media are traditionally available to organizations: Instructor-led, computer-based and hard copy. Each has advantages and disadvantages.

1. **Instructor-led training** has the most impact on the population. It allows for rapid adaptation and focused instruction. The cost for development is modest, but audience size is limited, and organizations incur delivery costs over time. In-person instruction is the best forum for complex issues that require long-term retention. Given that many employees may not have given any previous thought to insider threats, in-person instruction is likely to be the best way of delivering initial training and making employees aware of both the threat and the impact of malicious activity.
2. **Computer-based instruction** ranges widely in the levels of development and presentation complexity. A basic briefing presentation is inexpensive but provides the least knowledge retention. More complex designs can approach the effectiveness of instructor presentations, but most training is usually a video of a short skit, a variant of a webinar, or a narrated slide deck. Adding quizzes and feedback loops increase the value of the presentation by forcing employees to focus and retain information; low quiz scores can be used to calculate employee risk ratings, which can, in turn, influence the frequency and content of periodic training. Increasing complexity results in increased cost of development but also increases learning. Expenses can be amortized by increasing audience size – for example, deploying the training module across the entire organization – thus reducing cost per individual. Periodic simulated phishing exercises provide opportunities for highly interactive experiences that facilitate transfer of training/ learning to the operational environment, as well as identifying individuals who require additional training and awareness that may be administered via computer-based instruction.

3. **Hard copy training** is comprised of training aids that can be printed and handed out individually or distributed as part of an awareness program. Alone, such materials are of minimal value, as they may be overlooked by employees unaware of their importance or relevance. As a supplement to in-person or online training, however, they can enable the provision of more in-depth training content to all or select employees.

The most effective training utilizes “active learning” approaches that fully engages employees. After completing initial training, employees should receive periodic refresher or awareness training to maintain vigilance and state of knowledge about insider threats. Training must be considered an ongoing process, not a one-time event.

## ESTABLISHING AND COMMUNICATING REPORTING PROCESSES

Establishing mechanisms through which employees can report insider threat concerns to management is critical to the success of the program. All organizations should establish multiple mechanisms for handling reports of concerning behavior in ways that protect the privacy of both the reporter and the employee of concern; confidential reporting that eliminates the fear of repercussions, according to Carnegie Mellon University's CERT Division, helps overcome “the cultural barrier of whistleblowing.”<sup>4</sup> Many organizations identify an initial point of contact in human resources or security, while others establish anonymous reporting hotlines. Given that some employees may not feel comfortable reporting to a centralized support office with which they have little interaction, alternate processes should be established to enable employees to report concerns to a supervisor. Supervisors should then be taught how to handle such requests in a formalized manner that is consistent across the organization.

<sup>4</sup> Dawn M. Cappelli, Andrew P. Moore, Randall F. Trzeciak, *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)*, (Pittsburgh: Carnegie Mellon University Software Engineering Institute, 2012), p. 161.



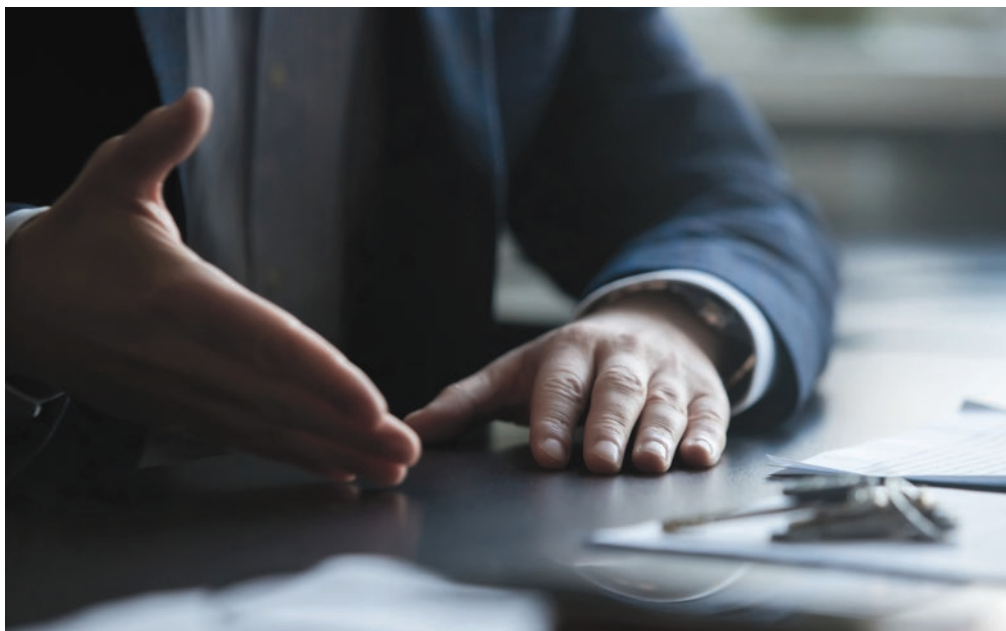
Reporting avenues must be addressed in core training and reinforced in every awareness initiative, including signage throughout the organization. Reporting processes should be periodically tested to ensure the officials at different stages of the reporting chain are aware of their responsibility to share information up and/or across the organization.

### OVERCOMING BARRIERS TO REPORTING CONCERNING BEHAVIORS

Even if training emphasizes how to recognize behavioral indicators and report concerns, employees may still have reservations about reporting a co-worker. The best training and the most efficient reporting process will accomplish little if the organization cannot establish a culture of reporting – yet without creating what could be perceived as a “big brother” environment. One successful strategy to overcome this obstacle is to embed and reinforce the focus on the welfare of the individuals involved across all training and awareness events. Odd or suspicious behaviors are often associated with life crises, such as work stress, financial pressure, and personal life stressors like divorce or illness. By calling attention to a co-worker’s aberrant behavior, an employee may help a troubled person to get assistance and resolve a life crisis before harming him/herself or others.

Similarly, if employees understand that the actions of malicious or unintentional insiders have the potential to negatively impact the company’s reputation, its financial strength, and even its ability to keep or gain business, they may be more likely to report a colleague whose behavior is concerning. Employees who can tie the threat to a personal risk of harm to themselves or others, to include unemployment, may be more likely to come forward regarding suspicious activities of a co-worker.

Finally, though confidential information gleaned through an investigation of an employee considered a potential insider threat should not be widely shared, employees who submit a report about a co-worker should be given some feedback to demonstrate that their report was taken seriously. If employees believe their reports are not investigated, they will not be motivated to report in the future.



## TRAINING RESOURCES

The good news for government agencies and companies of all sizes and complexities is that they can take advantage of free and high quality resources to support education and awareness programs. The Defense Counterintelligence and Security Agency (DCSA), which is responsible for industrial security in the defense sector, maintains extensive libraries on the web site of its Center for Development of Security Excellence (CDSE).<sup>5</sup> Its offerings include basic and interactive awareness programs for initial training, as well as case studies and videos for on-going awareness campaigns; CDSE developed a wide range of new training and awareness materials for Insider Threat Awareness Month, a new initiative launched in September 2019 with the support of the Office of the Director of National Intelligence.<sup>6</sup> CDSE has also made available training programs<sup>7</sup> to help establish an insider threat program; its resources focus on the reporting architecture, roles and responsibilities, and training for different levels of an organization.

While every organization under the purview of DCSA must establish education/awareness programs that meet minimum standards, the resources made available through its site provide enough material, at no cost, to build a comprehensive education and awareness program. Using the resources already created by DCSA, organizations of virtually any size have the capability to build a program as robust as they like. Other government agencies, such as the National Counterintelligence and Security Center (NCSC), also make a wide range of educational materials and case studies available to both government and private organizations. NCSC's materials include flyers, signage, and videos in which counterintelligence officers describe actual insider cases.<sup>8</sup>

“Using the resources already created by DCSA, organizations of virtually any size have the capability to build a program as robust as they like. Other government agencies, such as the National Counterintelligence and Security Center, also make a wide range of educational materials and case studies available to both government and private organizations.”

<sup>5</sup> Materials are available at <https://www.cdse.edu/index.html>.

<sup>6</sup> Links to 2019 Insider Threat Awareness Month resources are provided in the information packet at <https://www.cdse.edu/documents/toolkits-insider/2019-it-awareness-month-package.pdf>.

<sup>7</sup> See <https://www.cdse.edu/toolkits/insider/awareness.html#training>.

<sup>8</sup> See <https://www.dni.gov/index.php/ncsc-home>.

# CONCLUSIONS

Organizations of all sizes must develop an appropriately scaled and resourced structure that can implement education, awareness, and reporting programs across the organization. A truly ingrained education and awareness program that addresses insider threats and encourages the positive benefits of being a part of a reporting culture is the greatest defense against malicious insiders. Even at large organizations where network security is tight and computer monitoring is common place, a savvy malicious insider can get around electronic surveillance. The one sensor that cannot be circumvented is the educated and observant co-worker who is willing to report suspicious activity.

Government oversight agencies tasked to assess organizational efforts to mitigate insider threats should consider the size and resources of the organization. A small company or agency that has instituted few technical countermeasures but has established a comprehensive education and awareness program and a culture in which reporting is encouraged should be considered as meeting many of the requirements to establish an effective insider threat program. Further, an organization with vast resources implementing a wide array of technical solutions but a weak employee training program and a culture of organizational mistrust may very well have an inadequate insider threat program. Employee insider threat education and awareness training is the keystone of protecting any organization's interests, property, and people.

## ABOUT INSA

The Intelligence and National Security Alliance (INSA) is a nonpartisan, nonprofit forum for advancing intelligence and national security priorities through public-private partnerships. INSA's government and private sector members collaborate to make government more effective and efficient through the application of industry expertise and commercial best practices. INSA's 160+ member organizations are leaders in intelligence collection and analysis, data analytics, management consulting, technology development, cybersecurity, homeland security, and national security law, and its 4,000 individual and associate members include leaders, senior executives, and intelligence experts in government, industry, and academia.

## 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 (particularly, but not only, those working on intelligence and national security issues), cleared contractors, and other public and private sector organizations. The objective of the Subcommittee's work is to enhance the effectiveness, efficiency, and security of both government agencies and their industry partners, as well as to foster more effective and secure partnerships between the public, private and academic sectors.



INTELLIGENCE AND  
NATIONAL SECURITY  
ALLIANCE

*Building a Stronger Intelligence Community*

(703) 224-4672 | [www.INSAonline.org](http://www.INSAonline.org)