

Security along the Border:
The Insider Threat
Building a secure workforce



Table of contents

1	Introduction
2	Attempting to understand the insider threat
2	Summary findings: Insider threat
4	Asset loss and insider threat defined
6	Risk indicators and characteristics
6	Risk of increased computing and networking
6	Risk from changing workforce demographics
7	Risk of competing loyalties
8	Mitigating asset loss: a series of interventions and action plans
8	Develop an integrated approach to a secure workforce to mitigate assets loss
8	Develop the workforce as a security sensor and collector
9	Leverage human resources as a risk mitigaor
9	Use predictive analytics to assess workforce
11	Manage risk through cyber security and information access management
13	Why now?

Introduction

People are an organization's greatest resource, yet, at times, they pose a significant threat to its mission and operations. For an organization executing a complex and politically visible mission, the potential loss of confidence in public support at the hands of an employee undermines the agency's ability to execute the mission, recruit staff, and develop sustainable partnerships with other U.S. and international agencies. The 58,000 employees of the Customs and Border Protection Agency (CBP), along with their international, federal, state, tribal and local partners, play a vital role in determining the security of our nation at America's borders and ports of entry. A security breach at the U.S. border could potentially facilitate some of the most egregious crimes, such as human and drug trafficking, smuggling of weapons of mass destruction and firearms, and illegal entry for terrorists. To effectively patrol a border spanning over 7,000 miles, including over 300 air, sea, and land ports, the U.S. federal government must prioritize the need to understand who poses an 'insider' threat to the mission and operations of its agencies entrusted to protect the border.

With over 45,000 CBP law enforcement officers and agents assigned to protect the United States border and ports of entry, there is a need to adopt an integrated approach to reduce the threat posed by 'insiders.' An initial challenge for most organizations is to understand and define the risks associated with potential breaches of security, including agents assisting in illegal border crossings or allowing other illegal activities, either through willingness or complacency. A secure workforce is the most viable solution to mitigating and managing compromises at any level by employees of the organization, who, both intentionally and unintentionally, exploit assets and mission objectives. Addressing physical and information security through technology comprises only two-thirds of the necessary equation for protecting against asset loss. The third part of the equation, managing a secure workforce and mitigating the threat posed by the vetted employee or the 'insider' is often the most critical variable.

The 'insider threat' for border security is real and well documented. In a March 2010 Senate briefing, officials from the U.S. Department of Homeland Security (DHS) stated that Mexican drug cartels are aggressively attempting to recruit border agents to facilitate narcotics and human smuggling through ports of entry¹. These cartels, through financial resources and developed networks, have the ability to facilitate the smuggling of drugs, weapons, and illegal aliens, as well as the ability to recruit and 'turn' agents. Since 2007, there have been 80 corruption-related convictions among enforcement officials along the U.S.-Mexico border and 129 agents were arrested since 2003 on corruption-related charges along all U.S. borders. Unfortunately, these types of cases are increasing, with CBP corruption investigations opened by the Inspector General of the United States of America climbing from 245 in 2006 to more than 770 in 2010.^{viii} Recent cases, such as those involving CBP agents, Martha Garnica and Eric Macias, are a stark reminder that the threats of corruption and espionage exist within DHS, much as they have in the intelligence community for decades. The cartels are attempting to infiltrate every level of border security, including agents away from the border, but with access to sensitive information.²

In addition to the physical threat and attempts to infiltrate the border, new technologies that surpass existing mitigation strategies require agencies to adopt an integrated risk posture to confirm that a compromise of technical barriers does not result in a breach of national security. Competitors and predators, often now literally and virtually inside the organization, pose a greater risk to assets now than when the organization was compartmentalized and siloed. Developing strategies to mitigate the risk of asset loss, while developing a new level of awareness of the threats, must be centered on building a secure workforce. Building this secure workforce requires agencies to fully utilize their hiring and vetting process, to empower supervisors, through training and leadership, to create an employee culture that serves as the first line of defense against the insider threat.

Attempting to understand the insider threat

In the early 1980s, we learned that the most significant risk to national security was associated with the employee who was on the inside, and not the result of actions conducted by “secret agents from foreign governments.”³ Subsequently, the United States government conducted research to enhance law enforcement investigative and operational capabilities. Some of the best examples are studies conducted by the U.S. Department of Defense (DOD) Personnel Security Research Center (PERSEREC) in 1992 and then most recently in 2008⁴ as well as studies completed by Carnegie Mellon (University) and the United States Secret Service (Agency) (2005).⁵ Project Slammer (1990), a less published study conducted by the DOD and the Federal Bureau of Investigation (FBI) closely examined the motives and patterns of behavior of convicted spies.⁶ Additionally, there have been studies in police corruption and fraud, and most recently a study of sabotage and the exploitation of information systems.⁷

Summary of findings: insider threat

The findings from all of the studies noted are consistent when referring to the behavior and actions of the ‘insider.’ The actions that are taken are not impulsive, but intentionally pursued over an extended period. They are often the end result of a complex set of problems, conflicts, and disputes, or a crisis in the individual’s personal life. In many cases that means obtaining money, validation, or empowerment. Few entered their organization with the specific intent to violate a trust or facilitate the loss of the organization’s assets. Therefore, the motivation to violate trust occurred after they were vetted and hired and while they were already employed and had authorized access to information.

Asset loss process: evolution from idea to action

Causes

- Crisis inside or outside of the workplace; financial/personal/occupational
- Feelings of frustration, disappointment, disgruntlement
- Over-inflated sense of abilities and achievements
- Strong sense of entitlement and self-centered view of what (they perceive) the organization is or is not doing for them
- Need to demonstrate value for others to others to recognized



Effects

- Revenge/retaliation/rebellion
- Seek ways to achieve immediate gratification, satisfaction
- Resolve a conflict or perceived injustice
- Act passive aggressive or destructive towards those whom they feel are neglecting them, or not recognizing their potential

Actions

- Disclose proprietary, sensitive, or classified information
- Sell documents
- Sabotage material or systems
- Facilities access to others

In all cases, insiders engaged in a pattern of behavior that reflected a movement from having an idea to taking an action, all in the service of some solution to a problem. The patterns include: irresponsible handling of classified or proprietary information; irresponsible use of information systems; disclosure or dissemination of information determined to be proprietary or classified to persons without clearance or purpose to have the information; removal of proprietary or classified information or material from secure areas, often taking it home or inappropriately placing it in an open information system; and providing information to others for purposes of facilitating their actions for personal gain or vengeance against perceived wrongdoings by an agency. In almost every case, these activities, if recognized by a vigilant workforce and reported to management, could have been easily interrupted. Additionally, one of the most frequently offered rationalizations by violators is that no one notices, and that physical and information security was lax; if tighter, it would have been more of a deterrent. The lesson learned is that identifying indicators and patterns of at-risk behavior prior to hiring someone and watching for them while an individual works for the organization is a step towards a secure workforce.



Asset loss and insider threat defined

Asset loss has several different agents: corruption, espionage (to include economic), sabotage, fraud, and terrorism. In all cases, the activity that is linked to asset loss is specific to the organizational context and agency mission in which an organization (public or private sector) operates: government, critical infrastructure, manufacturing, finance, or technology. In many cases, the greatest vulnerability to asset loss may not just be from an outsider, someone who physically or virtually penetrates the organization, but the end result of a pattern of behaviors and actions taken wittingly by an 'insider,' an employee, and in some cases unwittingly, influenced by outsiders to include family, friends, and associates, who manipulate insiders to provide sensitive information and material that can lead to considerable exploitation of an organization's assets. While there are many definitions associated with asset loss and insider threat, the most common include:

- **Asset loss** is when sensitive, classified, or proprietary information, material, or systems are disclosed, compromised, or disrupted, causing damage to an organization's interests, productivity, and/or public confidence.
- **Insider threat** exists within every organization where employees (**insiders**) comprise the core of an organization's operational plan and are the key drivers of its mission execution. As a result (**threat**) of some perceived injustice, retaliation, sense of entitlement, or unwitting need for attention and/or validation, the employee takes some action as part of a contrived solution that results in negative consequences for the organization.

Some examples of an insider threat that lead to asset loss:

- **Corruption** is securing an advantage through means, which are inconsistent with one's duty or the rights of others.

Martha Garnica, a former CBP officer, devised secret codes, passed stacks of cash through car windows, and sketched out a map for smugglers to safely haul drugs and undocumented workers across the border.⁸ Eric R. Macias, a Border Patrol agent helped drug traffickers smuggle cocaine and marijuana into the country for about two years before being arrested in January 2009 when he told a confidential informant how to avoid getting caught smuggling marijuana and provided cover by escorting two shipments of cocaine.⁹ Former CBP officer Margarita Crispin was arrested in El Paso in 2007 and sentenced to 20 years in prison after pleading guilty to a charge of conspiracy to import more than 1,000 kilograms of marijuana. Prosecutors alleged she accepted more than \$5 million in bribes over several years in exchange for letting smugglers' vehicles pass through her checkpoint without inspection.

- **Espionage** is the practice of spying or using spies to obtain secret information about another government or business competitor.

Brian Patrick Regan was arrested for committing espionage in 2002, while he was a government contractor. He buried 20,000+ pages of Top Secret — Sensitive Compartmented Information (TS/SCI) materials and then sent a letter to Saddam Hussein offering locations and orbits of spy satellites and reports on Iran for \$13 million. He drafted a similar letter to Libya. When he attempted to board a flight to Switzerland, he had the addresses for the European diplomatic offices of Iraq, Iran, and Libya in his shoe. His motivation was to gain some relief for over \$100,000 of debt and to sustain an image of being responsible and competent.¹⁰

- **Embezzlement** is "the fraudulent conversion of property of another by a person in lawful possession of that property."¹¹ Crimes of this nature generally involve a relationship of trust and confidence, such as an agent, fiduciary, trustee, treasurer, or attorney.

Harriette Walters, a city tax office employee in the District of Columbia, was charged with leading a group of colleagues that allegedly wrote and cashed fake property tax refunds for companies that did not exist or were not owed a refund. In all, prosecutors have estimated at least \$20 million was stolen from the city (District of Columbia).¹²

- **Sabotage** is to hinder normal operations, or the deliberate act of destruction or disruption in which equipment or a product is damaged.

Earl and Mary Triplett were at their home near Tacoma, Washington, drank a can of soft drink, and then went to sleep. The next morning Earl picked up the container, which had been left overnight on a table, heard a rattle and found a syringe inside. The couple called their lawyer, who called the press and local health officials, who alerted the police. Within days, there were 50 similar reports in 23 states. In New York City, a man claimed that he accidentally swallowed two pins that were in a soft drink bottle. In Beach City, Ohio, a woman said she found a sewing needle in a can of the soft drink, and in Jacksonville, Florida, a man discovered a screw in his beverage container.¹³

- **Disclosure of Personally Identifiable Information** occurs when someone gains access to personal information (e.g., social security number) of employees or company records, resulting in the exploitation of assets and potentially much more.

Philip Cummings was an employee at Teledata Communications Incorporated, a company that provides information technology support for a credit bureau information network. He provided credit reports, passwords, and codes to a co-conspirator, who sold them for up to \$60 a report. This resulted in depleted bank accounts; unauthorized charges to credit cards; and ordered checks, debit cards, ATM cards, and credit cards. The identities of 30,000 victims have been assumed by others for over three years, resulting in a combined loss of \$2.7 million.¹⁴

Other potential results of asset loss caused by insider threats include:

- Loss of scientific and technological ideas and solutions (e.g., intellectual property) that contribute to the ongoing evolution of products, services, revenue, and safety
- Impact on supply-chain integrity that interferes with the import and export of crucial resources critical to the economy and/or national security apparatus
- Potential sabotage and contamination of product or materials executed by employees or people given access to secure areas that could result in hostile actions or loss of public confidence
- Loss of proprietary to classified information that effects national security and the competitive edge by individuals who have been granted access
- Use of violence as a solution to a problem within an organization to destroy people, property, and reputation
- Nontraditional terrorist attacks on the public, such as sabotaging a regional or national power grid or the Internet
- Compromise of critical infrastructure, including electrical power grids, nuclear power generation, communication systems, and transportation networks
- Cyber attacks on critical information technology systems and/or the use of cyber attacks to secure information that is critical to mission operations
- Information leaks that threaten the safety and security of personnel and external assets, as well as undermine ongoing operations

The environment in which an organization operates defines its threats and vulnerabilities and will dictate its risk management strategy to protect its assets. Any attack on an organization, whether the result of an employee selling sensitive and proprietary information, a rogue financial manager absconding with funds, or a saboteur who seeks to disrupt a supply chain, will directly effect the overall performance of the organization and in most instances, if it becomes public knowledge, the organization's reputation and public confidence. The goal of any organization is to mitigate that risk as much as possible.

Risk indicators and characteristics

It is possible to identify the insider threat prior to an insider taking action. A number of characteristics have been identified and associated with an employee who engaged in corruption, disclosures, or sabotage. Conversely, there are mediating factors that balance some risk indicators.¹⁵ Examples of these indicators and mitigators are identified below:

Risk indicators	Contra-behaviors
Individuals feeling the organization was unresponsive to their needs	An individual who works well with others
Individuals seeking validation of their self-aggrandized view of their abilities and achievements	An individual who displays genuine warmth and compassion towards others, lacking a sense of entitlement
Self-centered, entitled, and undervalued persons	A person who is characterized as good-natured
Individuals that, if their needs are not met, act in ways that are rebellious, passive-aggressive, or destructive	Someone who can clearly and appropriately express anger and frustration
Intolerance of criticism, inability to assume responsibility for their actions, blaming others, and minimizing their mistakes or faults	A person who responds well to criticism without becoming defensive
Individuals who seek out others who will meet their needs or undermine the efforts of those they feel have neglected them, or who did not recognize their potential	A person who is fulfilled by their current responsibilities and develops relationships with subordinates, peers, and superiors
Individuals who are burdened by financial debt or under pressure to increase their financial standing	A person who is financially solvent and does not need additional income sources to maintain their current standard of living

In addition to the indicators and characteristics of employees, there are three additional risks that warrant further in-depth discussion. Outlined further below, these include the increased risk due to the increased use of computers and networks to share information, changing workforce demographics, and competing loyalties of employees.

Risk of increased computing and networking

Changes in the way business is conducted in the world today shape the vulnerability to insider exploitation. The shift from a world of bricks and mortar to computer bits and bytes brings along a number of new challenges to managing a secure workforce and protecting the organization's assets:

- E-mail based text searches do not account for other media (e.g., instant messaging, mail attachments, web postings)
- Making physical copies is no longer required
- Manipulating records can be done from almost anywhere on the globe
- Data is more mobile through e-mail and on USB drives, iPods, smart phones, etc.
- Telecommuting gives employees access to network and systems with fewer restrictions
- Web-based applications/multiple systems used in the same process are proliferating and provide global accessibility
- Organizations still rely on policies and manual controls to review user administration, provision, segregation of duties, etc., for a multitude of systems and databases across their enterprise

Risk from changing workforce demographics

The shift to a virtual and globally connected world is more relevant today considering the change in the United States workplace that is underway. The incoming Generation Y is filling the gaps left by retiring Baby Boomers. This is a generation raised on the Internet and socially networked, for example, via Facebook and Twitter. They have developed an expectation for constant and immediate access to information, and they readily share information as part of a daily pursuit of knowledge. This new workforce will present many new security issues as the workplace becomes more networked with increased access to information. This new workforce will challenge some of the security procedures in place from the Cold War era. These new challenges include:

- Change in information medium and mobility, both which promote fewer restrictions on sharing
- Millennials who tend to be opportunistic

- Limited controls with the increased degrees of freedom in cyberspace to include anonymity
- New medium to personal 'connectedness' and validation
- Increased levels of technical expertise across the workforce
- Lack of understanding by organizations or approaches to manage information through its life cycle, including information access management

A recent study by the Aberdeen Group found that 80 percent of 116 companies surveyed view loss of confidential information, either by intercept or sent by an insider, as a significant threat. Yet only 43 percent of companies have a system in place to monitor and control the flow of outbound e-mail, compared with the 79 percent of companies who control the flow of inbound e-mail. A small percentage (16 percent) of companies surveyed stated they intend to implement both outbound and inbound e-mail control systems within the next year.

Risk of competing loyalties

There were an estimated 1.1 million immigrants who entered the United States this year, with many more naturalized citizens holding dual citizenship in the United States and their country of origin. Employees who are naturalized citizens may have an additional set of risks that must be considered when completing a workforce assessment. Whether witting or unwitting, the emotional connect to one's country of origin and culture can leave someone vulnerable to being exploited and to provide information without any malevolent intent. Some examples include:

- Individuals seeking to provide entry for family members and friends who are restricted from entering the country legally
- Other countries looking to compromise national resources and impact national security
- Drug cartels, smugglers, and other criminals seeking personal gain
- Terrorists seeking to destroy the economy and infrastructure by gaining access to information or infrastructure

This is a risk that needs to be carefully managed, exercising great sensitivity when vetting foreign-born employees, while avoiding profiling and stereotyping. The reality is that within the federal government, certain skill sets require a broader search for qualified candidates, many that are difficult to vet and clear. The balance must be struck by performing the appropriate level of due diligence without paralyzing the operations of the organization. Even with this screening, 'insiders' will continue to pose a threat.

In an April 3, 2008 story, the Washington Post highlighted the case of Chi Mak, a Chinese national who resided in the United States for 20 years before he was arrested for attempting to courier sensitive plans for United States naval weapons systems to China. Mak worked for a defense contractor, and used the access afforded to him by his job to exploit data loss prevention weaknesses not uncommon among private sector companies¹⁶.

Since 9/11, there has been a significant increase in concern regarding a potential attack on an organization that will destroy its productivity, personnel, and public confidence. While there is an understandable focus on the threat from an external terrorist cell, the threat from the inside should be viewed with near-equal concern. The concern rests with an employee who may become radicalized during the course of employment and might share critical information that is used by others to organize an attack.

Lyman Farris was a 34-year-old of Kashmiri descent when he came to the United States in 1994. He gained citizenship in 1999, and lived in Columbus, Ohio. In 2000, he made a pilgrimage to Mecca, then traveled to Afghanistan and trained in Al Qaeda camps. He returned to the U.S. and was tasked by Khalid Sheik Mohammed to target the U.S. infrastructure. He was specifically asked to assess the feasibility of bringing down the Brooklyn Bridge by slashing its suspension cables. Mr. Farris drove fuel trucks to airports and retained access to very sensitive areas after becoming radicalized. He pled guilty to two counts of providing material support to terrorists.¹⁷

Mitigating asset loss: a series of interventions and action plans

Develop an integrated approach to a secure workforce to mitigate asset loss

Organizations, and leaders within the organization, need not feel helpless to the threats outlined above. A key to prevention and early detection to combat insider threat is the development of a secure, managed workforce as a risk mitigation practice. Such an approach takes into account what is known about insider threat, the risk indicators, and the associated triggers that result in asset loss, and aligns them to a series of solutions. These solutions include:

- 1) develop the workforce as a security sensor and collector;
- 2) leverage human resources (HR) as a risk mitigator;
- 3) use predictive analytics to assess workforce; and
- 4) manage risk through cyber security and information access management.

Develop the workforce as a security sensor and collector

Because asset loss is often perpetrated by employees with inside access, securing the workforce by implementing awareness and anti-risk activities is often an organization's best opportunity to thwart insider threats. Ongoing educational campaigns directed at the workforce about the threats posed by insiders can heighten sensitivity to insider threat challenges, and provide concrete, practical steps employees can take to minimize asset loss. Additionally, strong disincentives to violate clear-cut policies around unauthorized dissemination can help the private sector to deal with asset loss swiftly and decisively.

Organizations should also structure their people and processes carefully. A networked work environment defies the well-ingrained models of compartmentalization and creates risk. The diagram below depicts a model for a highly secure networked workforce connecting people to purpose and resources.



Actions to consider:

- Develop and articulate values that clearly state the organization's beliefs in protecting critical information that is foundational to mission operations and information security
- Develop workforce standards to mitigate risk, including hiring practices, security requirements, management practices for problem employees, disciplinary procedures, resources provided to employees in crisis, and crisis management practices
- Develop a curriculum that includes observation skills, targeted behaviors, reporting protocols, and quality assurance mechanisms (e.g., techniques to minimize false positives)
- Develop a set of specific targeted behaviors that are consistent with current preoperational tactics (e.g., patterns discerned from the case studies database, individuals who demonstrate undue interest in specific areas and functions, unusual patterns of activity, such as employees being in places that are not relevant to their tasks)
- Develop training for reporting suspicious and aberrant behavior consistent with a process designed to capture data collected and reported by the workforce
- Develop baseline awareness training as part of the onboarding process for all employees working in the transportation system
- Develop a generalized training for employees in noncritical vantage points, and targeted and specific training for employees in critical vantage points
- Develop a continuing education program for all employees to update their initial training and reinforce awareness and vigilance practices as the adversary evolves
- Develop a security plan that includes roaming interviews of the workforce in real time
- Develop a test mechanism to ensure quality assurance and determine where additional training should be conducted

Leverage human resources as a risk mitigator

An organization's HR function possesses a unique opportunity to assist in managing a secure workforce; providing critical oversight; and coordination for vetting, hiring, monitoring, and debriefing employees throughout their time at the organization. The HR staff is generally the first and the last to interact with an employee, based on their opportunity to conduct exit interviews, access employee files, and serve as the first line of defense for a supervisor seeking assistance in managing an employee problem or a resource for an employee crisis. An example of this opportunity includes being able to understand the cultural and social expectations of workforce demographics. As highlighted above, the changing workforce demographics consistent with the millennial generation will provide HR managers and organizational leadership with unforeseen challenges. Many of the millennial's characteristics, such as tendency to overshare information, increases the likelihood that information will be provided to those who should not have access. HR can provide a critical role in employee relations and a perspective and view of employees that is invaluable in assessing the potential insider threat. Lastly, HR will usually be the last organizational resource to interact with a departing employee and in some cases may gain insight into what risks an employee may suggest if departing under negative circumstances.

Use predictive analytics to assess workforce

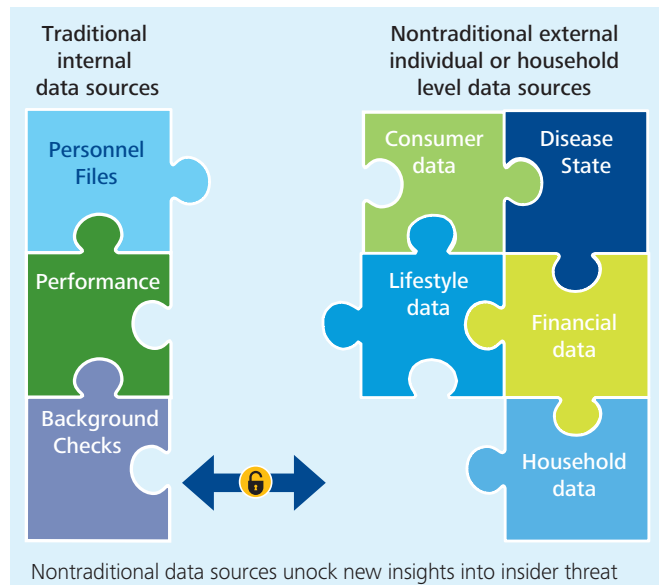
Traditionally, available organizational data could make it difficult to differentiate individuals, especially in terms of who might be most likely to pose an insider threat. Data compiled from human resource files, resumes, and observation may not be able to answer critical questions, such as:

- Who is most likely to consider some form of exploitation to the organization?
- What external events are influencing an employee's decision-making ability?
- Who may be more likely to harm themselves or others in a violent attack?
- Who may be more likely to commit fraud, due to financial burdens?

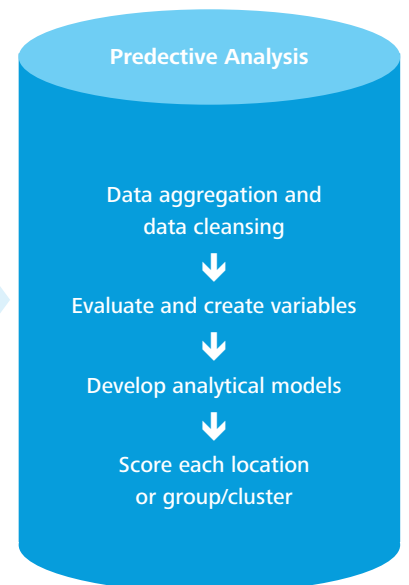
By applying advanced analytics, an organization can effectively use available internal and external data to better understand individuals recognize indicators that more accurately predict future events involving insider threat. If agency leadership cannot answer these critical questions, they are effectively operating with blinders on when it comes to this crucial area of security. The challenge is deciding which potential threats need to be measured and then bridging the gap between the vast stores of enterprise data that may be available, especially that which relates to your 'insiders,' and the strategic risk issues that the executive team needs to address.

By taking a more strategic approach to decision making and using advanced analytics to turn employee data into actionable business intelligence, agencies can leverage internal and external data, including the following examples: existing Enterprise resource planning (ERP) systems; security clearance data; personnel files; data warehouses; publicly available purchase, credit, and survey data; contractor invoices; and disbursement histories. These insights can help guide decisions that are critical as the agency confronts a range of threats. This capability is not a "nice to have," but a "must have" going forward. Such an approach requires:

Innovative data sources



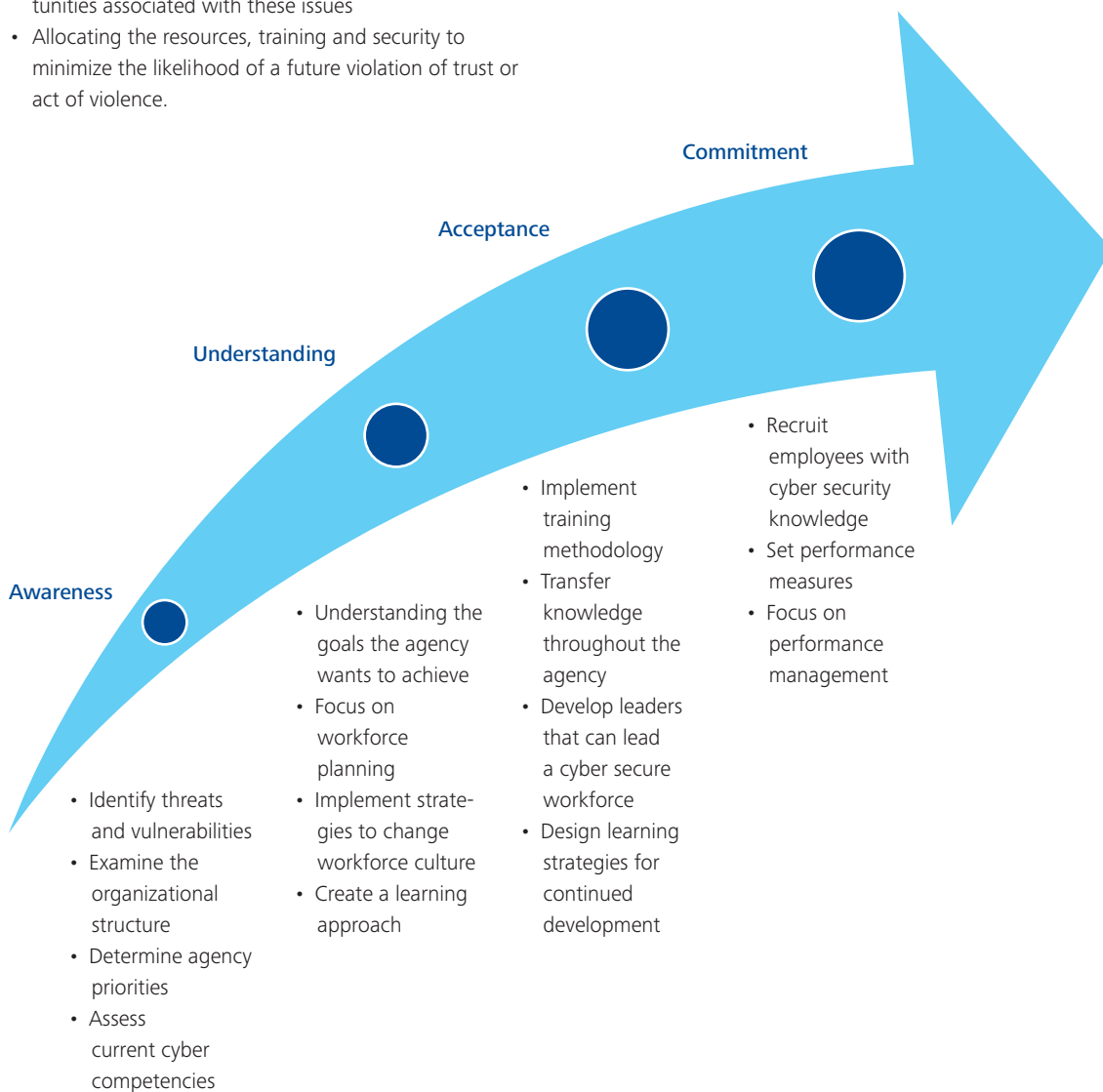
Customized segmentation analysis



- Understanding and quantifying the components of the agency's most pressing insider threats
- Formulating the key strategic inside threat questions related to these issues
- Mapping these questions to the agency's enterprise data sources, as well as external third-party data, to determine whether the organization has the information needed to find answers
- Using advanced analytics to explore scenarios that answer the questions and address the risks and opportunities associated with these issues
- Allocating the resources, training and security to minimize the likelihood of a future violation of trust or act of violence.

Manage Risk through Cyber Security and Information Access Management

An integrated risk management approach to mitigate the insider threat must also consider the implications of technology and information sharing. In the context of the insider threat, technology is a force multiplier, allowing employees access to information that is easily sold, shared, or stolen. Organizations must focus on both developing a cyber secure workforce, in addition to developing an information access management system that addresses



the threats posed by insiders. A cyber secure workforce is a collection of employees across all facets of government that understands the importance of protecting governmental information and is equipped to effectively keep this information secure. These individuals are the key resource in establishing and managing cyber security. Proactively establishing a cyber secure workforce that recognizes the threats, vulnerabilities, and risks associated with handling and managing mission critical information must be a primary goal across all federal agencies. Fostering a cyber security culture will help to mitigate both threats from intentional or unintentional insider actions and the predatory behavior of an outsider seeking to cause a cyber security breach. Agencies must develop the incentives and leadership practices to move their workforce from awareness to understanding and acceptance, with the end goal of having a workforce committed to sound cyber security practices.

The continuing proliferation of information systems and information technology has resulted in increased collaboration tools, Web enablement, and social networking. These same progressive developments have resulted in an increased risk associated with providing access to information to employees who have been cleared or vetted within organizations.¹⁸ Subsequently, as organizations become more networked, they must also become more sensitive to information access management and the potential vulnerabilities to be exploited by the insider. This means not merely the creation of barriers to sharing information, but rather a thorough understanding of who has access to critical assets, how this access aligns with responsibility, and if partnerships between several individuals could result in too much information exchange.

Why now?

The success of DHS' collective border security efforts is closely connected with its ability to recruit, train, and monitor over 45,000 agents that actively protect the U.S. border and ports of entry. Being successful in maturing these organizations' workforces is not simply a question of aptitude, training, or resources, but also understanding an employee's motivators and intentions. Understanding the 'insider threat' allows agencies to understand and mitigate the threat that puts their mission at risk and the threats that undermine their undercover operations. For agencies operating in an environment that is based on trust between individual employees and between national and international organizations, the high-risk threat of an insider compromising the organization's mission requires immediate action. Working in harmony with high levels of physical and information security, a secure workforce provides organizations with the tools it needs to deter or mitigate the next Martha Garnica or Eric Macias, employees who were once trusted agents of the U.S. government, but turned into substantial threats to our nation and its border security.



Contacts

Michael G. Gelles, Psy.D

Director

Deloitte Consulting LLP

mgelles@deloitte.com

John K. Cassidy, M.P.P

Manager

Deloitte Consulting LLP

jocassidy@deloitte.com

Contributing Authors

Andrew Petzold

Alex Daubert

References

- 1 latimesblogs.latimes.com/laplaza/2010/09/corruption-customs-agents-border.html
- 2 www.boston.com/news/nation/articles/2010/03/11/us_customs_mexican_cartels_corrupt_border_agents/
- 3 Wood, S. and Wiskoff, M. (1992) TR 92-005 Americans Who Spied Against Their Country Since World War II. Defense Personnel Security Research Center. Monterey, California
- 4 Herbig, K.L (2008) TR 08-05 Changes in Espionage by Americans 1947 to 2007. Defense Personnel Security Research Center. Monterey, CA
- 5 Capelli, D. et.al.(2005) Insider Threat and Computer System Sabotage in Critical Infrastructure Sectors. CERT Program Carnegie Mellon University, Pittsburgh, PA
- 6 1992. Project Slammer Interim Report. antipolygraph.org/documents/slammer-12-04-1990.shtml
- 7 Band, Steven et.al. "Comparing Insider IT Sabotage and Espionage: A Model Based Analysis."Carnegie Mellon, CERT Program. Technical Report CMU/SEI-2006-TR-026. December 2006.
- 8 www.washingtonpost.com/wp-dyn/content/article/2010/09/11/AR2010091105687.html
- 9 www.centerforinvestigativereporting.org/blogpost/20100614borderpatrolagentsentencedtosixyearsforcorruptionconviction
- 10 topics.nytimes.com/top/reference/timestopics/people/r/brian_patrick_regan/index.html
- 11 wordnet.princeton.edu/perl/webwn
- 12 www.nbc4.com/news/14784701/detail.html
- 13 Mohr, B. (1994) findarticles.com/p/articles/mi_m3289/is_n3_v163/ai_15312359
- 14 Sullivan, R. (2004) www.msnbc.msn.com/id/6001526/
- 15 Turner, J and Gelles, M (2004) Threat Assessment a Risk Management Approach, Insider Threat Chapter, Haworth Press, New York
- 16 Claburn, T (2008) Information Week www.informationweek.com/news/security/government/showArticle.jhtml?articleID=2_06905727
- 17 Kazalia, J. (2005) Al Qaeda leader in Columbus. columbusoh.about.com/cs/media/a/terror.htm
- 18 <http://www.privacyrights.org/ar/ChronDataBreaches>

As used in the document, "Deloitte" means Deloitte Consulting LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.

This white paper includes data and information that shall not be disclosed outside of government and shall not be duplicated, used, or disclosed – in whole or in part – for any purpose other than consideration of this white paper. In no event shall any part of this white paper be used in connection with the development of specifications or work statement with respect to any solicitation subject to full and open competition requirements. This restriction does not limit the government's right to use information contained in these data if they are obtained from another source without restriction.

This publication contains general information only and is based on the experiences and research of Deloitte practitioners. Deloitte is not, by means of this publication, rendering business, financial, investment, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this publication.