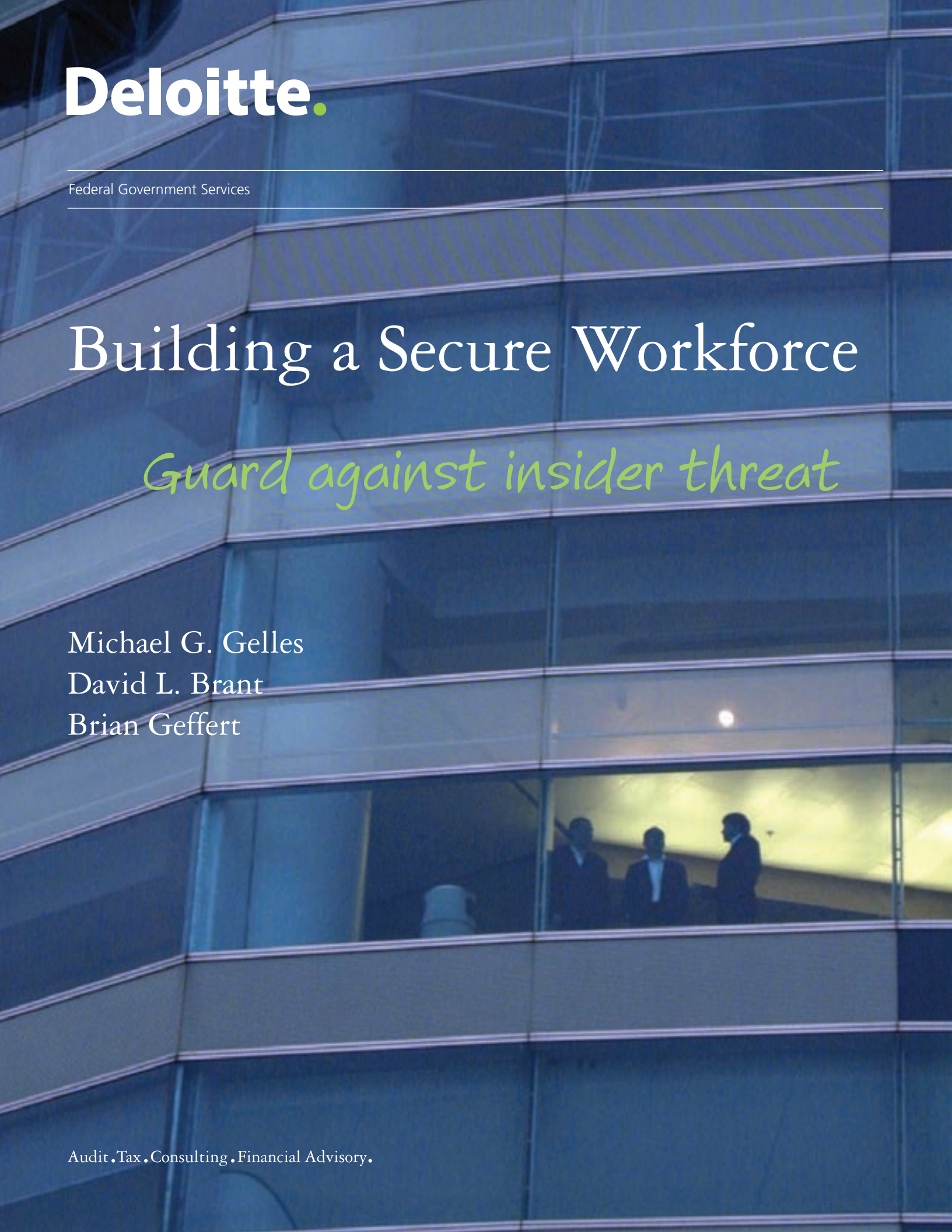


Deloitte.

Federal Government Services

Building a Secure Workforce

Guard against insider threat

Michael G. Gelles
David L. Brant
Brian Geffert

Audit . Tax . Consulting . Financial Advisory .

Table of Contents

Introduction

In today's evolving and changing global environment, business in the public sector is increasingly more challenging. There is an ongoing need to adapt a more balanced and integrated approach to protecting information and other assets. As the world becomes a virtual community of competitors and predators, an organization's assets are at greater risk than in the past, when the world was more localized, compartmentalized, and siloed. The dilemma that leaders face today is managing an evolving networked organization that is virtually connected, but secure.

As the continued growth of technology forces the world into a more networked work environment, it is important to sustain an integrated risk managed posture that assures that a compromise of critical assets does not result in a breach of national security, the loss of lives, or lapse of public confidence.[i] Developing strategies to mitigate the risk of asset loss may very well be the critical success factor that defines and prioritizes an organization's goals for success, whether the mission is national security, public safety, supply chain integrity, or just sustaining market share.

The purpose of this paper is to define the risks associated with asset loss and an approach to mitigate an "insider" threat through the development and management of a secure workforce. It is our opinion that a secure workforce should be a key strategy and primary objective of any organization. People are an organization's greatest asset and most critical vulnerability. Addressing physical and information security are only two-thirds of the necessary equation for protecting against asset loss. Managing a secure workforce and mitigating the threat posed by the vetted employee or the "insider" is in many cases the most critical variable in the equation. Our point of view incorporates an understanding and a set of solutions for consideration to help mitigate the insider threat and minimize asset loss through an integrated approach with physical and information security.

Asset Loss and Insider Threat Defined

Asset loss has several different agents: espionage (to include economic), sabotage, fraud, and terrorism. In all cases, the activity that is linked to asset loss is specific to the environment 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 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 or in some cases unwittingly by an "insider," an employee. While there are many definitions associated with asset loss and insider threat, the following definitions are offered for the purposes of this paper.

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 insider threat that lead to asset loss:

- **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.[ii]

- **Embezzlement** is "the fraudulent conversion of property of another by a person in lawful possession of that property."[iii] 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, 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.[iv]

- **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.[v]

- **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.[vi]

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
- 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 impacts national security and 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

The environment in which an organization operates defines its threats and vulnerabilities and will dictate its risk management strategy to protect its assets. We believe that all organization leaders will agree that asset loss will occur to some degree – 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 – and will likely directly impact the overall performance of the organization and in most instances, if it became public knowledge, the organization's reputation and public confidence. The goal of any organization is to mitigate that risk as much as possible.

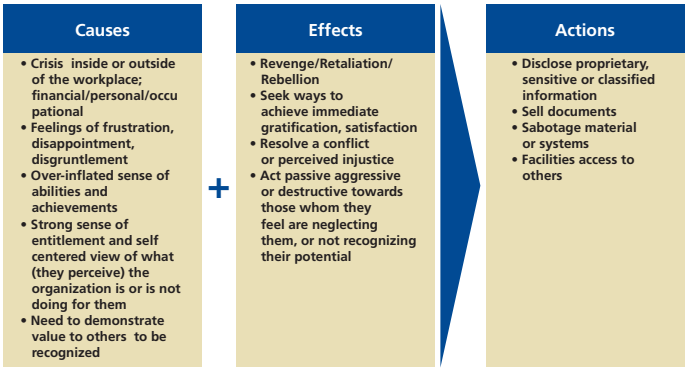
Understanding the Insider Threat

During past decades, there has been a significant investment by the United States Government in the study of behavioral risk indicators associated with espionage, sabotage, and threats to information systems associated with an employee. 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."[viii] 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 Department of Defense (DOD) Personnel Security Research Center (PERSEREC) in 1992 and then most recently in 2008[viii, ix] as well as studies completed by Carnegie Mellon and the United States Secret Service (2005.[x] Project Slammer (1990), a less published study conducted by DOD and the Federal Bureau of Investigation closely examined the motives and patterns of behavior of convicted spies.[xi] Additionally, there have been studies in police corruption and fraud, and most recently a study of sabotage and the exploitation of information systems.[xii]

Summary of Findings: Insider Threat

The findings from all of the studies noted above are consistent when it comes to the behavior and actions of the "insider." The actions that are taken are not impulsive, but intentionally pursued over an extended period of time. 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

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 on open information systems. In almost every case, these activities – if recognized by a vigilant workforce and reported to management – could have been easily interrupted.[xiii]

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 would be a step towards a secure workforce. Organizations need to look closely at refining their hiring, vetting, and monitoring processes to anticipate who may be at risk, and potentially require counseling should a crisis arise.

Risk Indicators and Characteristics

There are a number of characteristics that have been identified and associated with an employee at risk who engaged in corruption, disclosures, or sabotage. Just as there are many negative factors identified with potential security risks and possible espionage, there are mediating factors that balance some risk indicators.[xiv]

Risk Indicators
Behavior that is consciously pursued over an extended period of time
End results of a complex set of problems, conflicts, and disputes, generally reflected in the individual's personal life
Individuals feeling the organization was unresponsive to their needs
Individuals seeking validation of their self-aggrandized view of their abilities and achievements
Self-centered, entitled, and undervalued persons
Individuals seeking immediate gratification and satisfaction
Individuals that, if their needs are not met, act in ways that are rebellious, passive aggressive, or destructive
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
Intolerance of criticism, inability to assume responsibility for their actions, blaming others and minimizing their mistakes or faults

The table below outlines several characteristics that employers should seek in potential employees to mitigate the risk of inside threat.[xv]

Risk Mitigators
An individual who works well with others
An individual who displays genuine warmth and compassion toward others, lacking a sense of entitlement
A person who responds well to criticism without becoming defensive
Characterized as good-natured
Someone who can clearly and appropriately express anger and frustration

Competing Loyalties

There were an estimated 1.1 million immigrants who entered the United States this year, and while there is no definitive statistic, there are many more naturalized citizens who hold dual citizenship in the United States with their country of origin. Employees who are naturalized citizens may have an additional set of risks. 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:

- Other countries looking to compromise national resources and impact national security
- Drug cartels, smugglers, and other criminals who seek personal gain
- Terrorists who seek to destroy the economy and infrastructure

This is a risk that needs to be carefully managed, exercising great sensitivity when vetting foreign born employees.

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 companies.[xvii]

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 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.[xviii]

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 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
- 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

Additionally, a change in the United States workplace 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 My Space and Facebook. 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
- Millenials 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 lifecycle 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. 16 percent of companies surveyed stated they intend to implement both outbound and inbound e-mail control systems within the next year.

Risk of Public Information in Private Hands

The continued movement towards a more networked global economy and a more networked workplace across the Federal sector includes commercial entities that provide mission-critical services on behalf of the Intelligence Community, the Department of Defense, and civilian agencies. Public-private "partnerships" result in some instances where organizations have become interconnected, unknowingly due to the size, complexity, and siloed nature of the organization. Therefore, whether by insider threat or more conventional physical and cyber penetrations, private sector asset loss poses a real and present danger to national security.

Mitigating Asset Loss: A Series of Interventions and Action Plans

Develop an Integrated Approach to a Secure Workforce to Mitigate Asset Loss

A key to prevention and early detection 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, for example, refining the vetting and hiring process; establishing a system to report suspicious behavior and activity; providing resources to assist employees who may experience a crisis that leads them to exploit assets as a solution; and augmenting the workforce to function as a security sensor and therefore an early warning system.

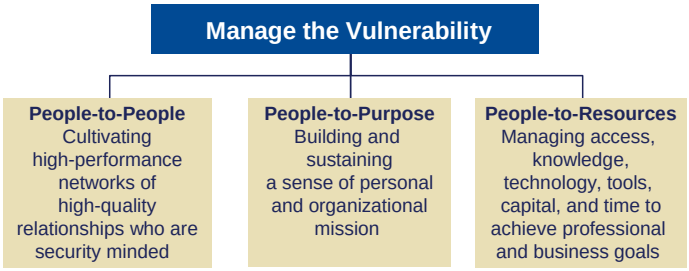
Establishing a Workforce Culture to Mitigate Risk

There are competencies that identify people who are less likely to pose security risks. As the culture and demography of the workforce transforms, individuals who are selected for positions in sensitive and secure jobs will need to possess core competencies that reflect integrity, self-restraint and a dedication to the "collaborative cause." Generation Y has been noted to be a generation that "could" bring a new type of risk in a secure work environment – based on their need for rapid fire communication, constant connectivity, and a natural propensity to share information.[xix] However, with sensitivity to the right competencies, the individuals sought should be team-oriented, responsive to constructive criticism, and more likely to express, rather than withhold, frustration – characteristics of employees who are less likely to disclose classified information.[xx] Companies should vet and hire employees with these competencies.

Competencies for a Secure Workforce

Because asset loss is often perpetrated by employees with inside access, securing the workforce by implementing awareness and antirisk 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 enable 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.



The Employee Assistance Program (EAP) a Tactical Mitigation Strategy

We have learned that almost every case involving an insider threat was due to an individual crisis. Therefore, the return on investment of an EAP cannot be underestimated as it relates to asset loss. The EAP generally offers guidance and support to employees dealing with personal problems that may affect their state of mind, which in turn can impact workplace behavior, performance, and well-being. It can make a critical difference in interrupting forward motion of a potential insider who is in crisis and whose solution is the intent to compromise information. While an EAP may be standard in most organizations, it is not yet ubiquitous.

Perhaps more critical than just making an EAP available to employees is the attention those employees require from a manager or supervisor. Organizations will need to evaluate their managerial development programs and ensure that supervisors are engaged with and tuned into their subordinates, and able to discern when a problem exists that needs attention, long before it develops into a crisis.

The Workforce as a Monitor: "Operationalizing" Security Awareness Training

It is our opinion that despite resources being heavily invested in cyber security in a growing world of virtual business, we must not neglect the day-to-day activities at facilities, plants, and agencies where physical security is one of the first lines of defense. One way to do this is with workforce monitors.

Historically, the use of the workforce as a monitor has been very successful in attempts to thwart assassinations, espionage, fraud, and workplace and school violence. Communities have developed neighborhood watches, and federal task forces who have looked to disrupt terrorist attacks have relied on the local police and patrol officers to recognize and collect information regarding subtle changes in neighborhoods where a preattack plan may be under development. There are many instances in similar contexts that reflect the efforts employers have made to develop the workforce's awareness. The practice of security awareness training has purposely been designed to keep the workforce informed and to mobilize greater awareness in the workplace or community. However, to date the idea of moving a workforce from informed and aware to trained observers and collectors has not yet been accomplished in most organizations.

The different vantage points in any setting that make up the workforce provide an opportunity to enhance the level of security surveillance by implementing a program that uses the workforce as a monitor of potential adversary intention. The organized use of the workforce as the eyes and ears of its security is an innovative idea that can be augmented with the right technology and social networking tools. Capturing and collecting that information through internal blogs, wikis or hotlines can provide a multidimensional view of the workplace and allow security a more comprehensive view of what is occurring in the workplace. For example, if an insider is seeking material and information from multiple sites within a facility, there is greater likelihood that their actions will be observed by different people in different locations, intensifying a footprint of potential hostile intent.

Develop the Workforce as a Security Sensor and Collector

Steps to consider:

- Assess the degree of vulnerability to exploitation across the employee network, including those vulnerable to exploitation and unwitting disclosures in support of their work because of a need for validation or support of a dual loyalty
- 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 on-boarding 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

Leveraging Human Resources as a Risk Mitigator

An organization's Human Resources (HR) function possesses a unique opportunity to assist in managing a secure workforce. 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 be the first line of defense for supervisor seeking assistance in managing an employee problem or a resource for an employee crisis. 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.

Risk Management Through Information Access Management

Regardless of the change driver, private companies and governments alike have had to adopt and use technology to address and meet mission requirements. The continuing proliferation of information systems and information technology has resulted in increased collaboration tools and Web enablement. The progressive developments in cyberspace have resulted in an increase in the risk associated with providing access to information to employees who have been cleared or vetted within organizations.[xxi] Subsequently, as organizations become more networked they must also become more sensitive to information access management. Organizations must adopt an information access management approach which includes automating processes that are currently done manually. For example, a user account provisioning and deprovisioning, proactively looking for access violations through logging, and alerting, enforcing, and monitoring for separation of duty controls.

Case Reviews

There are some well established procedures that an organization should consider to better understand the risks that may reside within their organization, as well as a methodology to help develop or refine existing programs geared toward creating a secure work environment and promoting a secure and managed workforce.

A typical threat-risk review can be oriented towards a short-term (8 to12 weeks) assessment of the relationship between the baseline workforce; the reported range of insider threat cases with a specific emphasis on parameters associated with behavior, circumstance, crisis, and opportunity; and a gap analysis of the current process associated with recruiting, hiring, vetting, training, and managing the organization's workforce. The following is an overview of a suggested approach to the review.

Project Initiation

- Identify and organize a multidisciplinary team to guide the review and provide subject matter experience and knowledge related to the role, function, and challenges of the organization, its mission and workforce
- Define the specific scope of the study: identify specific data sets and cases available for review
- Identify necessary subject matter specialists to comprise the study team, e.g., infrastructure, technology, scientist, and security specialists

Establish a Baseline: The "As-Is State"

- Examine and document the demographic of the organization workforce: age, demographics, locations
- Examine the employee lifecycle: recruitment, hiring, resignation, transfer, and retirement
- Evaluate current policy and programs associated with recruiting, vetting, hiring, training, security policy and reporting, investigative thresholds, and approaches
- Assess oversight of employees, knowledge of employees, awareness of and response to problem employees or employees in crisis, and management
- Assess the user administration process related to system or data access including provisioning, deprovisioning, segregation of duties in processes, change in position, or change in role within the organization and its level of automated versus manual controls
- Evaluate key data access control policies, procedures, and enforcement mechanisms (e.g., use of USB drives, removable hard drives)
- Evaluate security awareness training policies and procedures for employees

Case Sampling and Methodology for Review

- Develop criteria for case sampling: range of cases from minor violations to major criminal acts
- Analyze data
- Identify specific cases for follow-up reviews
- Develop Structured Interview Guide for case study interviews
- Organize multidisciplinary interview team security specialist, behavioral specialist, etc.
- Obtain appropriate releases to conduct interviews
- Conduct detailed review of specific cases for lessons learned

Conduct a Gap Analysis and Profile the "To-Be State"

- Compare and contrast findings from case reviews, case study interviews with policies reviewed in baseline phase, identify gaps, and develop a "to-be state"
- Using identified gaps and the "to-be state," develop suggested changes for refinement of policy and programs

Recommendations for Future Study and Change

- Provide recommendations for an early warning system of potential insider threat
- Provide recommendations of using the workforce as a security monitor
- Provide recommendations for policy and program refinement in the areas of hiring, vetting, training, security, policy and implementation, investigations
- Provide recommendations for how to mitigate risk with a managed workforce model that ensures early intervention for employees in crisis
- Provide recommendations regarding an information management framework for reporting and decision making in allocating resources against identified threats
- Provide recommendations to support the hiring of new employees based on anticipated growth with a process that is expeditious but ensures the due diligence necessary for a secure workforce
- Provide recommendations to leadership regarding the changing demographic of the workforce over the next five years
- Develop a results-management approach to managing and monitoring the effects of program changes on the success of sustaining a secure workforce; developing and maintaining performance metrics
- Augment the recruiting process with key indicators associated with the insider threat

Appendix A

Enterprise Risk Framework and the Insider Threat

The underlying premise of risk management is that every organization exists to provide value for its stakeholders. All organizations face uncertainty and the challenge for management is to determine how much uncertainty to accept as it strives to grow stakeholder value. Uncertainty presents both risk and opportunity, with the potential to erode or enhance value. In regard to protecting against asset loss, an organization needs to decide what and how much of their assets they are willing to lose. They must decide based on mission essential demands what risks they will take and develop strategies to mitigate as much of the risk as possible.

Developing a risk management framework can enable management to effectively deal with uncertainty and associated risk and opportunity, enhancing their capacity to build value.

Value can be maximized when management sets strategy and objectives to strike an optimal balance between growth and return goals and related risks, and efficiently and effectively deploys resources in pursuit of the entity's objectives.

A Risk Management Framework should encompass the following concepts as it relates to the Insider Threat:

- **Aligning risk appetite and strategy** – Management considers the organization's risk appetite in evaluating strategic alternatives, setting related objectives, and developing mechanisms to manage related risks associated with people and their access to information
- **Enhancing risk response decisions** – Risk management provides the rigor to identify and select among alternative risk responses – risk avoidance, reduction, sharing, and acceptance in areas that present with the most vulnerability or are a target of high threat
- **Reducing operational surprises and losses** – Organizations gain enhanced capability to identify and anticipate potential events and establish responses, reducing surprises and associated asset losses
- **Identifying and managing multiple and cross-organizational risks** – Every organization faces different risks affecting different parts of the organization, and a risk management framework facilitates effective response to the interrelated impacts of multiple risks. For example, developing a comprehensive awareness and reporting mechanism that captures information about potential risks across the organization providing a fuller picture of a potential threat by an insider than if just focused on one area of the organization
- **Seizing opportunities** – By considering a full range of potential events, management is positioned to anticipate and identify potential areas of risk and proactively realize opportunities to mitigate
- **Improving deployment of resources** – Obtaining robust risk information allows management to effectively assess overall resource needs and optimize resource allocation

These capabilities inherent in a risk management framework can help management achieve the organization's mission objectives and prevent asset loss. An effective risk management framework can help ensure effective reporting and compliance with security procedure and help avoid asset loss and the subsequent damage to the organization's reputation and associated consequences. In sum, an effective risk management framework can help an organization meet objectives and avoid potential losses and surprises.

Key Components of Any Risk Management Framework Include:

- Internal Environment
- Objective Setting
- Event Identification
- Risk Assessment
- Risk Response
- Control Activities
- Information and Communication
- Monitoring

Risk Equation

Within the security community, risk is converted into a useful equation that can help identify discernible patterns of behavior that could lead to possible harm in any organization. The equation multiplies the following factors:

- An individual's personal vulnerability
- The external threat posed by outside adversaries
- The context or mission-essential features of the work the individual will be conducting
- The assets that would be lost if information or material were compromised

Risk Equation

Risk = Vulnerability x Threat x Context x Asset Loss x Consequence

In this equation, risk is a dynamic phenomenon interacting with potentially changing variables.

The first variable, **Vulnerability**, speaks to certain characteristics of the individual based on patterned behavior that suggests poor judgment and reliability, ranging from behavior consistent with criminal and subversive activities, to episodes of indiscretion. The requirement is to identify characteristics, behaviors, and activities that make an individual vulnerable to situations that might lead to the witting or unwitting compromise of sensitive information. Additionally, the individual can be a threat to somehow destroy operating systems, production lines or supply chains. Using the criteria developed in a defined set of eligibility guidelines, vulnerability can begin to be operationalized by noting and managing discernible patterns of behavior that can negatively impact an individual's judgment and reliability, and provide insight into their intentions. Specific attention is focused on the criteria that describe behavior and activities associated with use of information systems and foreign influence and preference, mental and emotional functioning, personal conduct, criminal conduct, substance abuse, affiliation with known terrorist cells and financial issues.

In the equation, **Threat** is defined as some action or issue which originates from a source external to the person and impacts the person's ideas, actions, and intentions. This may include assessments or definitions of threat by police, counterterrorism or counterintelligence professionals, or by other intelligence services to include themes associated with specific intelligence collection, technology, information systems, and terrorist recruitment methods. Additionally, it can include domestic situations, such as divorce, bankruptcy, or foreclosure, that directly impact a person's life or their view of themselves as competent.

Context is defined as the mission, facility, activity, materials, and/or function that involves the individual. Although a threat may be present in the activity in which the person is engaged, it may be sufficiently insulated as to mitigate any risk to insider exploitation, loss of pubic confidence or worse, damage to national security or safety. On the other hand, an individual may be vulnerable just by affiliation, past behavior, or current crisis.

In regard to **Assets**, here defined as information, material, facility or activity, the risk is evaluated according to what assets could be compromised if an individual wittingly or unwittingly disclosed information or took some action. From a security perspective, it is an "anticipatory" damage assessment.

Consequence is the actual result of the impact to, or loss of, assets. In some cases, the consequence resulting from the impact or loss may be acceptable. In other cases, it may be catastrophic.

Finally, it is important to note that a risk may be present and assessed and not manageable based solely on the individual's behavior and activities.

In summary, examining the individual's vulnerabilities interacting with the outside threat, and within the context in which activities are conducted, establishes the risk. While the assessment of risk provides a valuable insight, it offers very little in terms of developing a plan by which to address and mitigate issues of concern.

Appendix B

Information Management Framework and the Insider Threat

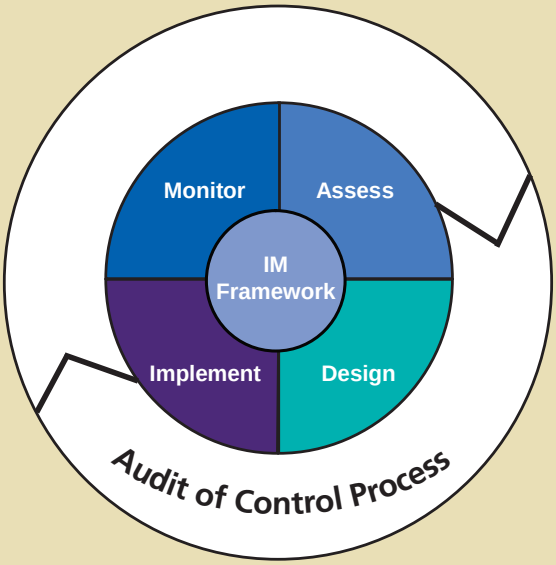
Organizations need to move from a risk avoidant to a risk management decision making style by recognizing that some risk exists, and it is necessary to take steps to discern and manage threats in accordance with the potential risk. This can be accomplished by transitioning from basic information sharing to robust knowledge management. The fundamentals of business and financial management audits and internal controls should be applied to the management of insider threats. Leaders should utilize regulatory controls and governance to manage, discern, and share information and intelligence in order to optimize the resources allocated to insider threats in accordance with the organization's mission.

An information management framework can allow organizations to metabolize a massive amount of data into meaningful information to be used in making critical, timely decisions to effectively manage insider threats. The framework permits the organization to develop its capabilities alongside the evolving insider threat by being able to expeditiously analyze new and emerging information, implement a response, and audit that response for purposes of measuring performance and modifying future approaches to ensure a response that is adequate, cost-effective, and minimally taxing on the resiliency of the workforce. The diagram (right) outlines rule sets regarding the implementation of an information management framework that can help enhance such governance and regulatory control.

Information Management Framework: Rule Sets

Monitor
- Assess outcomes based on threat categories and deployment of resources
- Evaluate new sources of data
- Monitor data quality
- Evaluate threat categories
- Report on outcomes

Implement
- Assess & establish controls for information collection, data integrity and response criteria
- Build centralized database and
- Set information criteria standards
- Develop a category system for managing assessed threats, e.g. high, medium, minor, hoax
- Develop response & implementation plan for the categories
- Audit implementation plan and outcome



Assess
- Monitor local & regional environment
- Examine most recent insider threats
- Examine insider threat response policies & controls
- Identify insider threats resources
- Assess past response in regards to resources and costs to past insider threats and incidents
- Assess technology solutions

Design
- Governance, policies, & standards
- Conduct threat analysis
- Assess current level of capability of resources to current threat state
- Allocate appropriate funding
- Assess status of current resource response pool
- Develop multidisciplinary risk management team as executive advisors to strategic decision maker
- Build technology requirements

References

i Gelles, M.G., Link, C., and Brant, D. (2008) Creating a Networked Workforce in Government. Deloitte Consulting. Washington, D.C.

ii topics.nytimes.com/top/reference/timestopics/people/r/brian_patrick_regan/index.html - 49k

iii wordnet.princeton.edu/perl/webwn

iv www.nbc4.com/news/14784701/detail.html

v Mohr, B. (1994) findarticles.com/p/articles/mi_m3289/is_n3_v163/ai_15312359

vi Sullivan, R. (2004) www.msnbc.msn.com/id/6001526/

vii Gelles, M (1999) rf-web.tamu.edu/security/secguide/Treason/Mind.htm

viii Wood, S. and Wiskoff, M. (1992) TR 92-005 Americans Who Spied Against Their Country Since World War II. Defense Personnel Security Research Center.Monterrey, California

ix Herbig, K.L (2008) TR 08-05 Changes in Espionage by Americans 1947 to 2007. Defense Personnel Securty Research Center. Monterrey, CA

x Capelli , D. et.al.(2005) Insider Threat and Computer Sytem Sabatage in Critical Infrastrucutre Sectors. CERT Prorgram Carengie Mellon University, Pittsburgh, PA

xi 1992. Project Slammer Interim Report. antipolygraph.org/documents/slammer-12-04-1990.shtml

xii 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.

xiii Shaw E. (2006) www.infolocktech.com/download/ITM_Whitepaper.pdf

xiv Turner, J and Gelles, M (2004) Threat Assessment a Risk Management Approach, Insider Threat Chapter, Haworth Press, New York

xv Krofcheck, Joseph, (2003) The Study of the Unspy, unpublished manuscript and personal communications. Yarrow Associates, Virginia.

xvi DHS Immigration Statistics (2006) www.dhs.gov/ximgtn/statistics/

xvii Claburn, T 2008) InfomrationWeek www.informationweek.com/news/security/government/showArticle.jhtml?articleID=206905727

xviii Kazalia, J. (2005) Al Qaeda leader in Columbus. columbusoh.about.com/cs/media/a/terror.htm

xix Cara Garretson, "Balancing Generation Y preferences with security" (NetworkWorld, 2007). URL: www.networkworld.com/news/2007/082907

xx Krofcheck, J (2001). "the Un-Spy Study" (unpublished government report).

xxi http://www.privacyrights.org/ar/ChronDataBreaches

Contacts

Greg Pellegrino
Principal
Deloitte Consulting LLP
gpellegrino@deloitte.com

David L. Brant
Director
Deloitte Consulting LLP
dbrant@deloitte.com

Brian Geffert
Principal
Deloitte & Touche LLP
bgeffert@deloitte.com

Michael G. Gelles, Psy.D
Senior Manager
Deloitte Consulting LLP
mgelles@deloitte.com