National INSIDER THREAT Task Force

Protect Your Organization from the Inside Out: Government Best Practices

2016

Insider incidents account for billions of dollars annually in "actual" and "potential" lost revenue, according to CERT©, a well-recognized source for insider threat data. Losses result from malicious actions such as thefts of trade secrets, deliberate destruction of computer systems, and damage to an organization's reputation once the loss is made public. It is a myth that only large visible global organizations, such as defense contractors, are targeted. The risk is steadily increasing and occurs regardless of size and location. Many organizations simply do not see themselves as vulnerable, but a life's work on a unique design or piece of software can be stolen and transferred out of the country in a few minutes. Disgruntled or former employees can slowly bleed data away for years or simply destroy the organization's systems. The impacts are devastating and spill over into communities in the form of lost jobs and opportunities. In some instances, entire industries and research efforts have been lost to overseas competitors who used those secrets to build rival firms. Sensitive national security programs are put at risk, as well, when components, parts, design plans, and specialized equipment are stolen.

- *An insider left her company with the names of thousands of clients and used them to gain favor with potential new employers.*
- *A disgruntled employee left his company with his employer's trade secrets. The foreign company that paid the perpetrator for the information hired him as a "consultant."*
- *A retired research scientist recruited still-employed former colleagues to steal trade secrets to be marketed overseas.*
- *Foreign nationals, as part of a partnership, stole a critical software program. They set up a competing firm back home. Over 700 of the 900 employees were let go and the company valuation went from $1.4 billion to $87 million (almost a 95 percent loss).*

Under Executive Order 13587, the National Insider Threat Task Force (NITTF) has worked with numerous government departments and agencies to develop their insider threat programs. Drawing from those best practices, this guide provides advice intended for organizations of all sizes to help them take the first steps to protect what matters most to their vital interests. Many institutions have "perimeter defenses" (gates, guards, access controls, computer firewalls) but are nonetheless vulnerable to insider theft or destruction of critical data. These steps can help them start to protect the things that make America cutting-edge and may ultimately affect national security.

The steps to reduce the risk can be low-cost and include practical changes to current management practices that are drawn from industry and U.S. Government best practices. A brief appendix includes a list of the most comprehensive resources available that add more detail on the risks insiders pose to organizations and explain what additional measures can be taken beyond "getting started."

U.S. university campuses share the private sector's increasing vulnerability to the theft of valuable intellectual property and are ill-prepared to fight it. During an interview in 2012, a senior FBI counterintelligence official stated that the "open, collaborative environment of U.S. campuses and growing numbers of foreign graduate students makes universities easy targets for thefts of research and products developed in the schools' labs." Law enforcement officials note universities are also vulnerable to "academic solicitation," which appears as genuine offers of collaboration or requests to study with specific professors. They are often thinly veiled efforts to gain access to expertise and sought-after technologies. University officials are doing little to educate their staff and students on how to protect their research and the schools' future revenues from marketable patents. An informal survey of U.S. engineering students showed that 68 percent did not understand the concepts of "trade secret," and over half could not define "copyright." This is troubling, as knowledge of key definitions is critical to understanding the threat.

An insider is any person with authorized access to an organization's resources to include personnel, facilities, information, equipment, networks, or systems.

The insider threat is the risk an insider will use their authorized access, wittingly or unwittingly, to do harm to their organization. This can include theft of proprietary information and technology; damage to company facilities, systems or equipment; actual or threatened harm to employees; or other actions that would prevent the company from carrying out its normal business practices.

Accurate estimates of annual losses are elusive because of how costs are estimated and what is widely recognized as significant underreporting. CERT© maintains an "incident data base" that captures reported incidents. In 2012, just the top eight incidents totaled close to $2.5 billion in actual (cost of the product) and potential (anticipated) revenues across multiple business areas.

Every Organization Everywhere is Vulnerable

Risks from malicious insiders are real and leave no sector of the economy or part of the country untouched. All organizations, whether in small towns or big cities, are vulnerable to insider attacks. Small firms of less than 500 employees, or medium-sized firms up to 5,000 employees, are not immune to this threat.

What makes your organization special—the "crown jewels"—also makes you a target. The consequences can be life changing for you, your employees, and the public. Malicious insiders can be anyone, acting on their own or conspiring with outsiders.

- *In Indiana in mid-2011, a foreign national with permanent residence status was convicted in the state's first ever case of insider theft. Working for two companies, he stole formulas for pesticides and food additives with the intent to establish a company in his home country with co-conspirators. The technology and the site of the theft were deliberately targeted.*
- *In Louisiana, a naturalized U.S. citizen with 27 years of service working for a U.S. chemical company conspired with former colleagues and overseas partners to steal a specific formula and market that technology to companies in his native country.*
- *In Colorado, insiders stole plans for a chip that controlled sound quality in cell phones. The insiders created a joint venture with a foreign university with the intent to mass produce the technology and market it to commercial entities.*
- *At the University of Wisconsin-Madison, a research assistant was convicted of shipping samples of a cancer treatment to his home country to start his own research center to develop and market the drug.*

A Stolen "Crown Jewel": Insider Theft of Software Devastates American Superconductor

This cautionary tale underscores how the theft of a "crown jewel" can quickly ruin a small/medium-size organization—and a life's work—in a matter of weeks.

In the mid-1980s, four MIT professors set up an energy company, American Superconductor (AMSC), in Devens, Massachusetts. AMSC marketed proprietary software to manage the flow of electric power through the grid. Wind power companies quickly adopted the software to move electricity produced by wind turbines. The company expanded rapidly, building a work force of over 900 with global operations. The stock price fluctuated over the years with the alternative energy market, but at the start of 2011, it was hovering around $300/share and its market valuation was over $1 billion. The main driver was demand from China's Sinovel Wind Group, the U.S. company's single largest customer and sometime collaborator.

Sinovel emerged as a critical player in upgrading China's electrical grid and building wind farms using AMSC's proprietary software to control the wind turbines. Sinovel accounted for over 70 percent of AMSC's revenue. AMSC was confident it had firewalled its software, sharply limiting access to proprietary data and securing the program on a separate server in Europe.

The relationship between AMSC and Sinovel appeared to be on firm ground, so AMSC was slow to expand its customer base. Then, in March 2011, Sinovel suddenly started refusing shipments. Within two weeks, news of Sinovel's decision spread, and AMSC's stock price dropped to $77/share: 40 percent of the company's value evaporated in one day, and the loss rose to 84 percent by September.

The CEO tried to repair the relationship, but Sinovel refused to budge. In June 2011, an AMSC repair crew servicing a windmill in China discovered it was operating on an unreleased version of AMSC's proprietary software. The Chinese had enticed a trusted Austria-based AMSC employee with access to the server to steal the source code and share it with Sinovel employees. Sinovel was now poised to market it to its own—and AMSC's—customers.

As a result of losing just one software program, AMSC's workforce had shrunk to about 250 people by July of 2015. In late 2015 the stock was trading at around $4/share and the company's total valuation hovered around $87 million. AMSC's future remains in doubt. Sinovel prospers and is valued at over $39 billion. After spending four years in litigation, Chinese courts ruled against AMSC's claims of software copyright infringement, and now Sinovel can counter-sue and potentially seize AMSC's assets in China.

The insider was arrested in Austria and received a short prison term. Although Sinovel promised him employment and $1.7 million, his payment for almost ruining AMSC was a mere $20,000. The United States indicted the Chinese perpetrators, but they remain out of reach in China.

Accurate Assessments of Scope are Elusive... but Threats are Growing

Public and private sector organizations which monitor this issue all agree that instances of insider threats are steadily increasing, especially regarding thefts of technology. Analysts estimate that close to 75 percent of insider thefts go unreported or undetected, regardless of an organization's size. This is especially true for small- and medium-sized businesses because they are the least prepared to detect the thefts, according to one assessment, or they opt not to report them. This lack of reporting makes it nearly impossible to define the true scope of the damage.

In a 2013 survey conducted by CERT©, over 200 responding small companies reported experiencing some form of cybercrime.

Insiders perpetrated close to one-third of the crimes. Most of the victims reported damage from insider attacks was more extensive than attacks from outsiders. Over 80 percent of the incidents included the loss or exposure of confidential information, and over 70 percent resulted in the theft of customer data.

In 2013, Spectorsoft, a computer use and monitoring company, reached similar conclusions from a survey of 355 information technology (IT) professionals across companies of all sizes. Over a third experienced insider attacks; close to half resulted in data leaks and 16 percent in IP theft. Forty percent of the attacks were committed by personnel in IT departments.

What are the Warning Signs?

With the heavy emphasis on deterrence in preventing damaging insider attacks, multiple studies in and outside the U.S. Government have developed warning indicators to help identify employees who may pose an insider threat.

Not surprisingly, the warning indicators focus most heavily on spotting disgruntled employees. Studies agree that, in general, disgruntled employees can be hard to stop because many of them are willing to get caught for the chance to "get even."

The FBI has developed what is widely regarded as the most authoritative set of indicators to help employers and staff identify potential risks. The indicators focus on both personal factors and workplace behaviors.

Personal factors may motivate or increase the likelihood an employee will act against their employer. Some potential issues or motivators include the following:

- ◊ Anger/revenge - wanting to retaliate against the organization for actual or perceived slights such as a lack of recognition, missed promotions, conflict with management or co-workers, or pending layoff
- ◊ Compulsive or destructive behaviors - drug or alcohol dependencies
- ◊ Ego/self-image - "above the rules attitude," subject to flattery or promises of a better job elsewhere
- ◊ Family problems - marital difficulties or other stressors at home

Personal behaviors may indicate an employee intends to act, or is acting, against their employer:

- ◊ Removing proprietary information or seeking access to material outside the scope of assigned job duties
- ◊ Working odd hours without approval
- ◊ Taking multiple short unexplained trips, particularly overseas
- ◊ Making unapproved contacts with competitors or business partners
- ◊ Showing interest in projects or work outside the employee's job areas
- ◊ Remotely accessing the computer network from home or vacation outside approved work routines
- ◊ Unnecessarily copying manuals or large volumes of materials

It is important to remember that the presence of some, or even all, of these potential indicators does not mean that an employee is engaged in illegal insider activity. Similarly, an employee's demonstration of none of the indicators does not guarantee he or she will not pose an insider threat.

Getting Started: First Key Steps

What follows is a series of steps based on U.S. government best practices to help get started. People with ill intent tend to go after the easiest target. Even the most basic steps can deter a malicious insider. There are numerous resources available online, as identified below, to assist with getting started or to build upon further.

1 Decide who should be engaged

Start with a single individual within your organization who will be responsible for supervising the effort. The individual should be senior enough within your organization to be able to marshal the necessary people and resources.

Identify individuals from key areas of your enterprise to participate. Depending on the size and scope of your organization, they may include personnel from human resources, security, IT systems, internal policies and procedures, training, and legal, as well as front line managers or supervisors.

It is important to include multiple areas because information indicating an insider threat can come from multiple sources. Sometimes individual indicators are not considered a problem, but, when coupled together and reviewed, may indicate an issue.

These individuals should assist with the following steps, which can be done simultaneously.

2 Determine what matters most to your organization

Identify your "crown jewels," the information that if stolen or destroyed would hurt, cripple, or ruin the enterprise. This could include unique products, formulas, production techniques, software, algorithms, and customer information.

Identify what makes the "crown jewel" vulnerable. Is it available on an IT system? If so, are there any controls on who may access the information? Can any employee copy the information, print it, download it to a removable storage device, or e-mail it outside the organization? If not on an IT system, the same types of questions should be asked to help decide what steps may be taken.

Is the "crown jewel" being shared with outside partners? What controls do they have in place? Protection in one location does not make your critical assets totally secure if they are left unprotected elsewhere.

3 Reassess personnel management practices

This step should include a review of all management practices for individuals who may be provided access to information, IT systems, and facilities, to include outside consultants, contractors, and business partners.

Perform background checks. There are many reputable means available (including online) to conduct at least basic checks at low cost. At a minimum, references, previous employment, place of residence, and education should be checked and verified. Checks should be done on prospective employees and business partners, as well as outside consultants and contractors.

Conduct periodic re-checks on employees. Staff circumstances can change over time, and reviewing areas such as workplace behavior can help spot issues that could raise flags.

Consider non-disclosure agreements (NDA) and non-compete clauses in work agreements. This puts employees and others on notice that information is proprietary and should be protected. Consider those with access to your "crown jewels" or whose work roles could potentially put them at risk. Including non-compete clauses in employment agreements can help protect proprietary information after employment ends. Many employees, feeling entitled to the contact network they built and the projects they did, try to take them when they leave.

4 Develop clear termination procedures

A checklist for termination actions can be extremely useful. When an employee, consultant, contractor, or business partner is let go or resigns, ensure consistent procedures are in place to protect the security of the organization, the "crown jewels," and the workforce. An insider can do just as much damage in the 30 to 90 days after leaving as in the time prior to departure.

These procedures may include, but are not limited to:

- ◊ Close review of the departing employee's network activity within a defined time frame of departure, such as 30 days prior
- ◊ Exit interviews to determine the employee's frame of mind and any potential risk he or she may pose
- ◊ Reminders about disclosure of proprietary/corporate information and the existence of NDAs, if used
- ◊ Termination of access to facilities (change the locks and/or alarm codes)
- ◊ Deletion of network accounts, including remote access ability

Follow up with recently released employees to check on their welfare after a week or two, as a simple indication of concern about their well-being could make all the difference. Remember, even if they didn't take anything with them, they still have a lot of knowledge in their head. Or, perhaps they bear grudges upon which they might be tempted to act in a violent manner.

Engage the workforce 5

Employees should understand the potential damage insiders can inflict on the organization, especially to its reputation and future health. Their jobs are at stake. Preventing this should be a well-publicized effort, and employees at all levels should be part of the process of protecting the company's "crown jewels."

Develop a communications plan to educate the workforce about any changes in policy or procedures instituted to mitigate the risks from insiders. These changes need to be clearly communicated to the entire workforce so they understand this course of action is being done *for* them and not *to* them.

Create a mechanism for employees to provide feedback, to convey any concerns, or provide suggestions. In addition, be sure there is a mechanism for employees to quickly and anonymously engage leadership or security to report a potential insider threat issue.

Identify what is (or should be) normal across the organization so abnormalities can be easily identified and addressed.

Engage with the workforce to create a culture of awareness of everyone's role to protect the "crown jewels," the company, and their jobs.

6 Review IT systems for security and vulnerability

Any system connected to the Internet needs to be protected, not only from external hackers, but also from insiders.

Can employees log in from the Internet? Do they need to and what can they do? Who has e-mail, can they attach files, and is there a limit? Where globally is your information stored?

Depending on the size, scope, and criticality of the IT system, you may wish to log and monitor all user activity on the system, consistent with applicable privacy laws. System monitoring can identify if insiders are accessing information they do not need for their job; if they are copying, printing, or e-mailing excessive amounts of information; or if they are engaging in anomalous activity that goes beyond their work role.

Consider restricting some capabilities to certain trusted individuals.

The entire workforce should be trained on the security requirements for access and use of the system. Enforce security requirements and address violations.

Use a computer "banner" or other electronic notice on your computer network to remind employees of what is and is not an authorized activity on your company's computer networks and that their activity may be monitored.

If you already have an IT backup system, in case of a natural or other disaster, it should be reviewed to ensure it is adequate and secure from tampering. This could serve double duty and also provide protection from a malicious insider.

Engage your privacy experts 7

Ensure policies are consistent with current privacy laws, and protect the rights of your workforce.

Privacy laws differ between countries and even between U.S. states. You may have different authorities or restrictions with respect to your employees' privacy in some places of your organization than in others. Employee buy-in is contingent on their belief that their privacy is being respected.

8 Put information into context

Information that indicates a potential insider threat may come from many sources: tips about unusual behaviors, reports of security violations, or identification of anomalous activity within an IT system. To assess the potential risk, the behavior must be put into context. Is it within the normal bounds for your workforce? Only you know what is normal for your organization and your individual employees. Putting information into context requires a team effort. Engage the team identified in Step 1 to review available information.

- Look for issues across the various disciplines – changes in job performance, use of IT systems, or work habits.
- If an employee is downloading large volumes of information from your network, is that activity within the employee's work role?
- If an employee is entering or exiting organization facilities at odd hours, does he or she have a legitimate work reason?
- If an employee is making changes to the IT system, does he or she have the authority to do so?

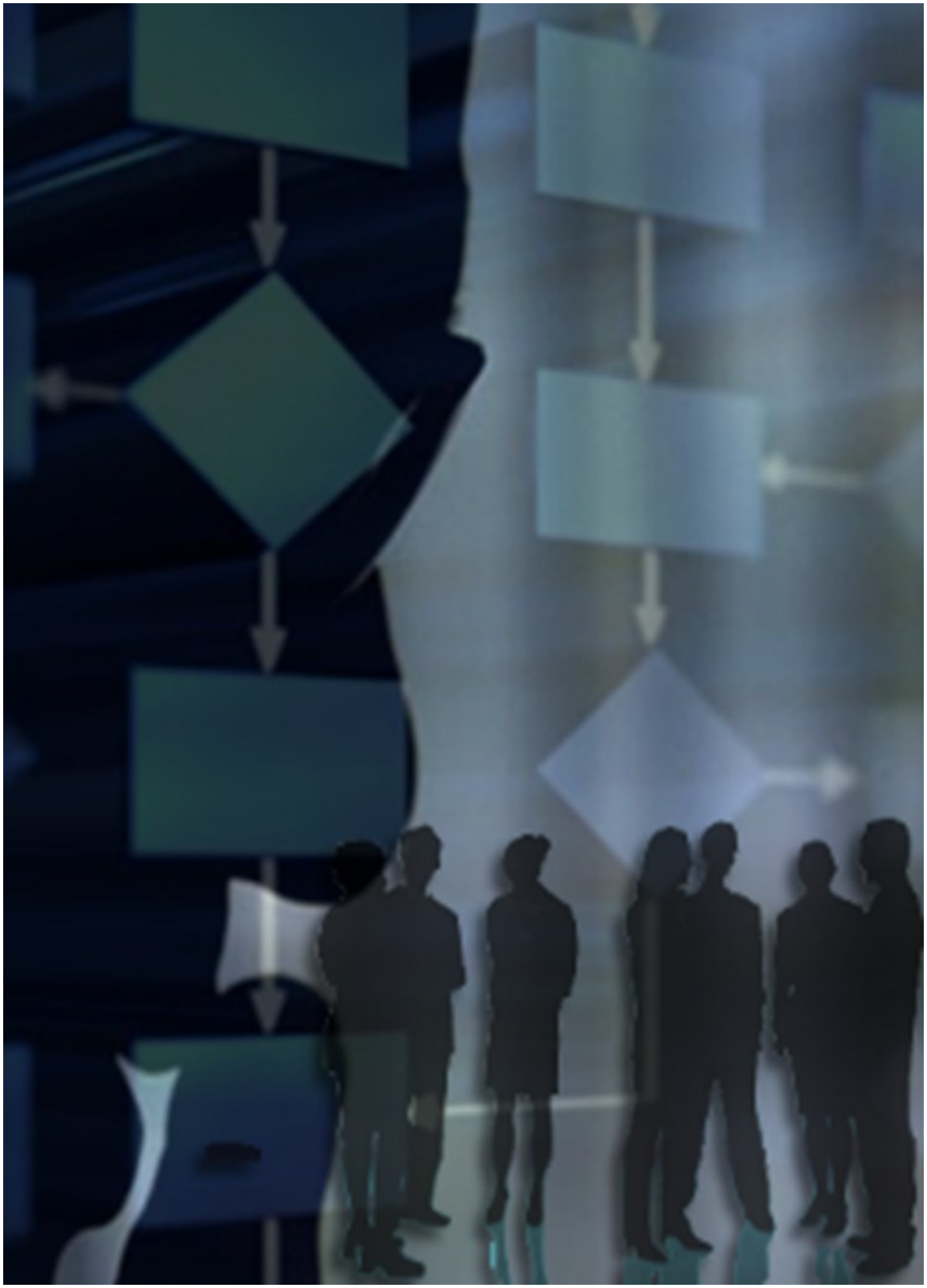
A single point of anomalous behavior may not stand out, but anomalies in several areas may indicate an insider threat issue.

9 Test your security posture

Continuous review of your security posture is key. Consider:

- Red teaming—Send out fake spearphishing emails to your workforce to see who clicks on the links, or put USB drives in a common area in the organization to see who inserts one into a computer. Educate those who don't pass the test.
- Tabletop exercises—Develop an insider-driven worst case scenario and run the organization through it to improve processes before you need them in real life.

Insider threats have the ability to seriously degrade an organization's ability to fulfill its mission. The loss of intellectual property and proprietary information can even impact an organization's ability to survive. Any entity—regardless of how small or large, how simple or complex—can become the victim of an insider. Undertaking the activities described within this guide is a significant step towards protecting your organization, your employees, your communities, and your future.



Appendix

NCSC.gov/nittf

The National Insider Threat Task Force (NITTF) is an entity created by Executive Order 13587. The NITTF mission is to deter, detect and mitigate actions by employees who may represent a threat to national security by developing a national insider threat program.

FBI.gov/About-US/Investigate/Counterintelligence/the-insider-threat

The FBI maintains a robust program to help U.S. organizations, including private sector companies, academic institutions, and non-profits, to deter risks from insiders. It also investigates crimes committed by insiders. Local FBI field offices are key points of contact for assistance in developing a mitigation program.

CERT.org

CERT© is a U.S. Government-funded organization located at Carnegie Mellon University that, among other activities, oversees a comprehensive collection of information and resources related to risks from insiders.

NCSC.gov/issues/ithreat

The National Counterintelligence and Security Center (NCSC) provides leadership and support to the counterintelligence and security activities of the U.S. Intelligence Community, the U.S. Government, and U.S. private sector.