A PRELIMINARY EXAMINATION OF INSIDER THREAT PROGRAMS IN THE U.S. PRIVATE SECTOR

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

CYBER COUNCIL: INSIDER THREAT TASK FORCE

SEPTEMBER 2013

INSA

ACKNOWLEDGEMENTS

INSA CHAIRMAN
Ambassador John Negroponte

INSA ADVISORS
The Honorable Charles E. Allen, *Senior Intelligence Advisor*

Ambassador Robert Joseph, *Senior National Security Advisor*

INSA STAFF
Ambassador Joseph DeTrani, *INSA President*

Chuck Alsup, *INSA Vice President for Policy*

Kate Swofford, *INSA Research Intern*

CYBER COUNCIL
Terry Roberts, *TASC, INSA Cyber Council Co-Chair*

Ned Deets, *SEI at Carnegie Mellon University, INSA Cyber Council Co-Chair*

EDITORIAL REVIEW
Joseph M. Mazzafro, *CSC*

EDITING & SUPPORT
Sandra Shrum, *SEI at Carnegie Mellon University*

Tara Sparacino, *CERT Division of the SEI at Carnegie Mellon University*

Pennie Walters, *SEI at Carnegie Mellon University*

COPY EDITOR
Elizabeth Finan

INSIDER THREAT TASK FORCE
Dawn Cappelli, *CERT Insider Threat Center of the SEI at Carnegie Mellon University (Lead)*

Zalmai Azmi, *CACI International, Inc.*

Steve Coppinger, *CACI International, Inc.*

Christopher King, *CERT Division of the SEI at Carnegie Mellon University*

Kevin Lawrence, *Accenture*

Terry Monahan, *Lockheed Martin Corporation*

Shannon Peterson, *Accenture*

James Robinson, *Websense, Inc.*

Robin Ruefle, *CERT Division of the SEI at Carnegie Mellon University*

Jim Simon, *Intelligence Enterprises LLC*

Roccie Soscia, *Lockheed Martin Corporation*

Douglas Thomas, *Lockheed Martin Corporation*

Randall Trzeciak, *CERT Insider Threat Center of the SEI at Carnegie Mellon University*

ABOUT THE INSA CYBER COUNCIL:
The INSA Cyber Council is a group of current and former executives from the public, private and academic sectors with expertise in cyber security. The Council engages government and industry communities in pursuit of innovative solutions and thought leadership that will improve existing cyber security policies, practices and organization for both sectors.

INSA INSIDER THREAT TASK FORCE:
This Task Force was formed to engage with Intelligence Community and DOD thought leaders, CIOs, and representatives from private sector companies to examine best practices regarding internal cyber security measures, particularly as these measures relate to insider threats.

Join the discussion for this white paper online using #INSAWhitePaper

INSA SUPPORTS A HEALTHY PLANET
INSA White Papers are printed on recycled paper that is 50% recycled content including 25% post consumer waste.

EXECUTIVE SUMMARY

Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information,* signed in October 2011, and the *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs,* signed in November 2012, mandate and provide guidance for insider threat programs in federal agencies that handle classified information. Since the release of this guidance, the federal government has paid significant attention to its insider threat mitigation programs.

However, no mandates, standards, or benchmarks exist for insider threat programs in the private sector. Therefore, it is difficult for companies to assess where they stand relative to their peers and to make decisions about their insider threat mitigation strategies. The purpose of this report is to address this issue by providing a preliminary examination of insider threat programs in the U.S. private sector. Much of the critical infrastructure of the nation is owned by private corporations, including much of the communications and information technology infrastructure over which important and sensitive government work is conducted. Additionally, the economic health of private industries is a factor in the overall security and well-being of the nation. Insider threats in the private sector can be very damaging, including: undermining the economic viability of a company, causing a loss in confidence in the company's brand and reputation, and compromising important government work—ultimately having a negative impact on national security.

For the purposes of this report, insider threat is defined to include fraud, theft of intellectual property (e.g., trade secrets, strategic plans, and other confidential information), information technology (IT) sabotage, and espionage. In-depth interviews were conducted with 13 organizations; most were large national or global organizations.

The first three sections of this report explore the program structure, incident management, and technologies associated with insider threat programs. For each topic, we provide the results of the interviews and recommend practices for mitigating insider threats in organizations. Some practices are based on the interview results; all are based on the subject matter expertise of task force members.

We list the interview questions in Appendix A and the financial-sector online survey questions in Appendix B. The results of the online survey in Appendix B can be found on the INSA website.

This report does not represent the state of the practice or best practices in the private sector. Because of the limited number of participants, this report is instead an initial examination of how some organizations in the private sector approach insider threat mitigation. We believe this report can help others consider what private sector organizations should and should not do to mitigate insider threat. This report is intended to encourage others to provide similar information in the future so that this work can grow to provide a true benchmark of the current state of the practice.

MAJOR FINDINGS

- Many insider threat programs are technology-focused, centered on tools that monitor network traffic and online activity, and that monitor only specific people that display concerning or suspicious online behavior. However, insider threat experts agree that an insider is a person. Therefore, organizations must identify psychosocial events—anomalous, suspicious, or concerning nontechnical behaviors. A robust insider threat program integrates and analyzes technical and nontechnical indicators to provide a holistic view of an organization's insider threat risk from individuals identified as potential threats.
- Executives in companies with mature programs support aggressive efforts to stem insider threats and are fully engaged in the program. An insider threat mitigation program cannot succeed without senior leadership support and involvement.
- An effective program requires a governance structure and solid partnerships with corporate Information Security, IT, Human Resources (HR), Public Relations, General Counsel, Ethics, Counterintelligence,[1] Physical Security, and Executive Management involvement and engagement.

Just over half of the companies interviewed have an insider threat mitigation program, although they vary widely in maturity and scope. Only five of the thirteen organizations have a formal incident management plan for insider threat. Many use detection technologies, but only a few mentioned having preventive controls. Most tools focus on network or host activity, with little inclusion of human behavioral issues. Eight companies have an awareness initiative related to insider threat. Companies reported that having a *confidentiality* program that employees can use to report suspicious behavior increased reporting of suspicious incidents.

Some companies implemented programs that closely monitor employees who display suspicious online behavior or act out in the workplace. The mature programs

A robust insider threat program integrates and analyzes technical and nontechnical indicators to provide a holistic view of an organization's insider threat risk from individuals identified as potential threats.

document and track employee online activity, such as websites visited, and files downloaded. These programs also document and track nontechnical information, such as badging records and phone records. This holistic type of program should be the goal of most companies, particularly those in critical infrastructure sectors. Decisions about the scope of a company's insider threat mitigation program should vary and depend on the criticality of its systems and information, as well as the potential impact if its confidentiality, integrity, or availability is compromised.

In summary, company executives should focus on the three major findings described above and support the formation of a formal insider threat mitigation program that:

- Spans the entire organization
- Includes employee monitoring (technical and nontechnical)
- Implements an effective training and awareness program focused on both external and internal threats
- Has the authority to conduct counterintelligence inquiries and investigations

The remainder of this report provides information for evaluating programs, designing a new program, and enhancing the strategy of an existing program.

INTRODUCTION

The damages caused by malicious insiders each year are not only substantial, but also on the rise. According to a recent RSA presentation that cited open-source, data-breach reports, and data-loss surveys gathered over a recent ten-year period, "The average cost per incident is $412,000, and the average loss per industry is $15 million over ten years. In several instances, damages reached more than $1 billion."[2]

These financial losses strongly suggest that organizations need to address insider attacks. President Barack Obama recognized that need in October 2011 when he signed Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*.[3] This order mandates "responsible sharing and safeguarding of classified information on computer networks" and tasks agencies with meeting both of those goals.

In November 2012, the White House issued the Presidential Memorandum, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, which directs U.S. departments and agencies to establish effective insider threat programs that "deter, detect, and mitigate actions by employees who may represent a threat to national security."[4]

These political actions focus attention on the insider threat[5] issue in federal agencies, but what about the private sector? Although the private sector "owns and operates approximately 85 percent of the nation's critical infrastructure,"[6] it does not have a similar mandate. Without such a mandate, U.S. companies are unprepared to tackle the pressing risk of insider threat. To address this issue, the Intelligence and National Security Alliance (INSA) formed an Insider Threat Task Force to examine insider threat programs in private sector organizations. This report describes the results of that effort.

In this report, insider threat is defined to include

- Fraud
- Theft of intellectual property (e.g., trade secrets, strategic plans, and other confidential information)
- IT sabotage
- Espionage

The following are examples of each type of case that illustrate how a malicious insider can deny, degrade, disrupt, destroy, deceive, corrupt, usurp, etc.

Fraud: A lead software developer at a prominent credit card company devised a scheme by which he could earn fraudulent rewards points by linking his personal accounts to corporate business credit card accounts of third-party companies. He cashed in the rewards points for gift cards and sold them in online auctions for cash. In all, he was able to accumulate approximately 46 million rewards points, $300,000 of which he converted into cash before being caught by internal fraud investigators.[7]

Theft of Intellectual Property: China sought to develop a manufacturing process for developing a pigment used in paint, plastics, and paper. China's state-owned Pangang conspired to steal the technology developed by a U.S. company. A naturalized U.S. citizen who had spent 35 years with that U.S. company said he used his former employer's trade secrets to help Pangang, which was building a 100,000 metric-ton-per-year plant to produce the pigment. The financial impact of this incident is estimated to be in the billions of dollars, and that does not factor in the consequent loss of jobs in the United States.[8]

IT Sabotage: A hospital employed a contractor as a nighttime security guard who was extensively involved with the cyber underground and the leader of a hacking group. He used his security key to obtain physical access to the computer that controlled the heating, ventilation, and air conditioning (HVAC) for the hospital. Using various methods, including password-cracking programs and a botnet, he rendered the HVAC system unstable, eventually leading to a one-hour outage. The insider and his cyber conspirators were planning to use the hospital's systems to conduct a distributed-denial-of-service (DDoS) attack against an unknown target. Fortunately, a security researcher discovered the insider's online activities. The insider was arrested, convicted, ordered to pay $31,000 in restitution, and sentenced to nine years and two months of imprisonment followed by three years of supervised release.[9]

Espionage: A former Air Force intelligence analyst was arrested as he was boarding a flight for Switzerland carrying missile site information on Iraq. Computers searched in his home led to the discovery of letters offering to sell secrets to Libya, Iraq, and China. In the Iraq case, he asked the Saddam Hussein regime for $13 million. He is thought to have been motivated not only by money (he had very heavy personal debts), but also by a sense of disgruntlement, as he complained frequently to former coworkers and neighbors about his job and station in life. He was convicted and sentenced to life imprisonment without parole. Information he provided after sentencing led investigators to 19 sites in rural Virginia and Maryland where he had buried over 20,000 pages of classified documents, five CDs, and five videotapes, presumably stashed for future sales.[10]

These examples demonstrate the complexity and diversity of the insider threat problem.

Although the theft of intellectual property is just one type of insider threat included in this report, it is a significant one, as addressed in the *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets,* released in February 2013, which addresses both internal and external threats.[11]

Thirteen organizations participated in interviews for this report. Most of these organizations were large national or global organizations, including IT services and consulting firms, financial institutions, technology vendors, aerospace and defense organizations, research institutions, and data analytics providers. All interviews, except two, included members of management or senior management. In over half of the interviews, participants included members of the "C-suite," directors, or vice presidents. Acting as part of the INSA Insider Threat Task Force, staff from the CERT® Insider Threat Center of the Software Engineering Institute (SEI) at Carnegie Mellon University conducted the interviews, as the CERT Division of the SEI has traditionally served as a trusted broker in handling confidential information.[12]

The original intent of this project was to collect information to write a state of the practice report for insider threat programs in the private sector. INSA put out broad calls for participants to various private sector groups, but found that despite procedures put in place by the task force to ensure confidentiality of participant information, organizations are hesitant to discuss the details of their insider threat programs because of the following fears:

- Their employees might feel mistrusted.
- Gaps in their programs could make them vulnerable to regulatory scrutiny.

- Competitors could use the information to their advantage.

As a result, this report does not represent the state of the practice, but instead provides a current snapshot examination of insider threat programs in the private sector as well as recommendations for organizations that are establishing or improving their existing programs. We are grateful to the 13 organizations that were willing to share their information with us in an attempt to improve the state of the practice in the private sector.

To gather additional information, we conducted an online survey of 71 organizations from the financial sector. See Appendix B for the questions and the INSA website for results.

INSIDER THREAT PROGRAM STRUCTURE

This section describes how the organizations that were interviewed structure their insider threat mitigation programs, recommend best practices, and identify areas for consideration in developing and managing an insider threat program.

> These programs are quite diverse, illustrating the need for a more widely accepted definition of what a formal insider threat mitigation program is, so that best practices and results can be shared.

INSIDER THREAT PROGRAM STRUCTURE: FINDINGS

Formal Insider Threat Program

Just over half of the organizations interviewed have a formal insider threat mitigation program. These programs are quite diverse, illustrating the need for a more widely accepted definition of what a formal insider threat mitigation program is, so that best practices and results can be shared.

Of the organizations with a formal program, five integrate insider threat into their incident response teams rather than establishing a separate team focused solely on insider threats; one focuses on counterintelligence, and another has a program that involves several departments. The Security department operates the formal program for over half of the companies that have a program. The technologies used in these formal programs include web and email filtering, data leakage protection, data discovery and searches, forensics tools, threat intelligence, active blocking and passive monitoring, and malware analysis. There was little evidence that these programs use detection strategies that focus on suspicious nontechnical behaviors, such as alarming psychosocial events in the workplace.

In the survey of financial sector organizations, only one-quarter of the respondents have a formal insider threat mitigation program. In those organizations, authority for the program usually rests with the chief information security officer (CISO), the office of IT, or Security. Most of these programs include employee monitoring, awareness training, and identification and monitoring of critical assets and intellectual property. Technologies used in most of the programs include access controls, logging, data loss prevention, and host-based monitoring.

Insider Threat Awareness

Eight of the companies interviewed have some type of awareness initiative related to insider threat. They educate staff using a variety of channels. Some focus specifically on insider threat, and others address insider threat in the context of more general security awareness: web-based training courses, printed or electronic newsletters, a component of their standard orientation for new employees and contractors, company-wide emails, and company web pages. Those interviewed reported that they accomplished the following specific activities as part of their awareness training programs:

- Presentations by outside speakers from the FBI and U.S. Secret Service
- Mandatory annual training on how to use information and information systems properly and how to report incidents
- Training focused on social engineering, unintentional leaks, and social media that show staff how to protect information both at the office and at home
- Informal helpdesk team training that covers account privileges and the importance of noticing who requests access to the "crown jewels" (i.e., a company's most protected information/resources)
- Training modules targeting the company's business unit
- Annual training in security, privacy, and intellectual property (IP) protection
- Training for all users and maintainers of classified systems about their responsibilities before they are given access
- Training on how to handle potential foreign intelligence or competitor elicitations, such as being approached at conferences, being asked to write white papers, or being offered employment or off-the-books work for foreign entities

One organization goes so far as to offer financial rewards for reporting suspicious incidents and holding contests for spam catchers. Another company conducts awareness training exercises periodically: Employees can earn free coffee by identifying and challenging people who are walking around the office without an ID badge.

To address the struggles that one company had with promoting insider threat awareness, the staff rewrote company procedures to include how to handle sensitive information. The company went a step further and developed four training sessions, planned a tabletop exercise, and asked its Communication department to stage a security awareness road show every two years. All employees at this company are now required to take online security training and 98 percent of them participate.

The interview responses varied about whether systems are in place to ensure that employees sign IP agreements, policies, or standards-of-conduct forms. Specific documents that are signed by employees in one or more of the organizations include the agreement that the company can wipe the sandbox portion of the employee's cellphone, IT acceptable-use policies, code of conduct agreements, non-disclosure agreements (NDA), ethics handbooks, intellectual property agreements, standards-of-conduct agreements, information security policy acknowledgements, privileged user agreements, and user responsibility agreements.

Three participants indicated that they routinely debrief staff following foreign travel to detect potential threats that employees may or may not have been aware of while traveling.

Most organizations in the financial sector include the following training and awareness content: malicious or illegal behavior by employees; responsibilities of employees to report threats and crimes; handling of sensitive information and intellectual property; consequences, sanctions, and process for reporting malicious or illegal behavior; and the proper use of separation of duties.

Over half of the surveyed financial organizations also provide training on unintentional actions that may cause an employee to unknowingly leak information as well as the proper use of configuration and change management.

Mergers and Acquisitions

We asked respondents about the precautions they take during mergers and acquisitions. Three interviewees' organizations scan the networks of the affected organizations before they are merged. Six perform a review, but did not provide details. Two do nothing. One organization conducts risk assessments on all the companies with which it works.

When new employees join the company due to a merger or acquisition, one or more of the participating companies screens them like new employees: They perform a robust background check and require all new employees and subcontractors to sign an NDA. One respondent said that the HR department reviews the new employee's previous background check, but did not know if a new check is conducted. Two respondents noted that the vetting process is not as thorough as it should be.

Policies for Contractors

When working with contractors, close to half of the interviewed organizations follow the same account management process they use for their own employees. The rest restrict contractors' access in some way, such as not allowing them to VPN into the company network or allowing access for a specific timeframe with an automatic cutoff date.

Close to one-quarter of the surveyed organizations restrict contractors' access to only the data they need. One organization uses different naming conventions for contractor usernames to facilitate their identification in user monitoring. One respondent said that the process followed for contractors is different but flawed; sometimes managers forget to notify HR when a contractor leaves, so the contractor's access is not terminated when it should be.

One participant noted that most of his company's subcontractors work on DoD contracts; therefore, these subcontractors must be a member of the National Industrial Security Program (NISP) and adhere to the same policies and procedures as their employees.

INSIDER THREAT PROGRAM STRUCTURE: RECOMMENDATIONS

- Establish an insider threat oversight body that includes senior executives from the company's HR, Security, Legal, Privacy, Ethics, Incident Response Team, IT, and Public Relations departments.
- Implement a formal insider threat incident response plan. This plan should include current and former employees, contractors, and business partners.
- Assign an attorney from the Legal department to be the point of contact who handles all legal issues related to the Insider Threat Program.
- Whenever possible, include staff members on the insider threat team who already have experience in dealing with insider threats and foreign intelligence threats, such as experienced counterintelligence staff. This selection of experienced staff is especially important for companies in which mishandling of classified, proprietary, trade secret, and intellectual property material could culminate in law enforcement action.
- Include the following components in an insider threat program: employee monitoring, awareness training, and identification and monitoring of critical assets and intellectual property. Technologies should include access controls, logging, data loss prevention, and host-based monitoring.
- Implement a formal training and awareness program for all employees to ensure that they are trained annually on topics such as IP, ethics, standards of conduct, and that they acknowledge their receipt of the training by signing IP agreements, NDAs, and so forth.
- Provide training to raise awareness about issues of heightened risk, such as joint ventures, mergers, acquisitions, and the company's supply chain. More detailed training should exist for critical personnel (e.g., system administrators). Defensive counterintelligence briefings should be provided for personnel involved in overseas travel and domestic and international conferences and trade shows.
- Use specialized technologies to detect and prevent insider threats that mine diverse datasets for anomalies, such as employees' computer login or physical access times that are outside normal work hours. Monitor employees for other potential

indicators, such as financial problems, unexplained increases in wealth, declines in job performance, and signs of disgruntlement.

- Involve the Counterintelligence Office in all mergers and acquisitions to ensure that a domestic or foreign company is not controlled by or tied to a foreign intelligence service or foreign government. This involvement can help protect proprietary, trade secret, and/or U.S. classified material.
- Implement a program that tracks metrics to compare them to industry benchmarks (which do not yet exist) and assess the effectiveness of the program over time.

INSIDER THREAT INCIDENT MANAGEMENT

This section describes the process that the organizations interviewed use to manage insider threat incidents. The responses cover two areas: incident management trends and proactive response preparation. The following sections describe the findings and recommended practices for each area.

> Only five of the thirteen organizations interviewed have formal incident management plans for insider threat.

INCIDENT MANAGEMENT: FINDINGS

Management of Insider Incidents

Only five of the thirteen organizations interviewed have formal incident management plans for insider threat. Three have an informal plan, two handle insider threat incidents using the same process for handling external incidents, and three have no insider threat incident management plan. Just under half of organizations surveyed in the financial sector have a formal plan for responding to insider security events; nearly all of them include that process as part of their normal incident response process.

One organization reported that as a member of the NISP they are mandated by law to report any insider incidents to Defense Security Service (DSS), even if they do not involve national security. Therefore, they implement the same policies and procedures for both classified and unclassified information and systems.

Some companies implement a weighted response program in which an employee who starts to display suspicious online behavior or acts out in the workplace is monitored more closely. The more mature insider threat programs document and track each insider event to provide a record of incidents to help strengthen their insider threat defense. Insider events include online activity, such as websites visited, files downloaded, and so on, as well as nontechnical events, such as badging records or phone records.

At least one company handles employees who inadvertently introduce malware onto the network by training and counseling them on "safe" online behaviors. While some companies terminate employees who are involved in malicious insider activities, most prefer not to pursue criminal action due to cost, negative publicity, and possible counter lawsuits. These organizations realize that unprosecuted malicious insiders may "move on" and cause damage to other organizations but, to them, the risks of criminal prosecution outweigh the benefits.

Online Social Media and Insider Threat Implications

Several companies block all online social media and do not allow file-sharing software on their network. They educate their entire workforce about this policy and respond to violations swiftly.

INCIDENT MANAGEMENT: RECOMMENDATIONS

- Consider the full range of disciplinary actions, including legal action, if warranted, against malicious insiders. Simply firing an employee pushes a potentially serious problem to another unsuspecting organization.
- Block social media and prohibit file-sharing software on company networks. Educate staff about this policy and respond to violations quickly.
- Institute a weighted response program to closely monitor staff who exhibit suspicious technical or nontechnical behavior. Monitor their outgoing email and use of removable media to ensure they are not exfiltrating proprietary or other sensitive information. Using data loss prevention (DLP) software is one way to do such monitoring. In addition, audit application use and critical file access for illicit activity.
- Document and track each insider event to provide a record of incidents and help strengthen insider threat defenses.

PROACTIVE RESPONSE PREPARATION: FINDINGS

Monitoring Employees

In some of the more mature insider threat programs, security and information assurance personnel are notified about employees who are deemed to be "at risk"—that is, those who exhibit suspicious online activity or who are reported to HR for performance or behavioral issues. When employees display suspicious behavior, these companies monitor them closely through badging records, observation, and other tactics, and always involve the company's general counsel. In some cases, the employee's behavior requires intervention or termination.

> In some of the more mature insider threat programs, security and information assurance personnel are notified about employees who are deemed to be "at risk."

Involving Top Management

Executives in some programs support aggressive insider threat efforts and are fully engaged in the program. Most schedule time on their calendars to be briefed on the cause and results of every significant insider threat event. This practice helps in two ways: (1) company executives understand the negative effects of malicious insiders and support corrective actions, and (2) the staff knows that senior leadership fully supports defensive insider threat efforts and a prompt response to illegal activities.

Educating Employees

According to some interviewees, an important practice with regard to employee awareness and reporting of potential insider threats is the establishment of a "confidentiality" program for employees who report suspicious behavior. Companies reported that having this program in place increased the reporting of suspicious incidents. Following the reporting of a number of home computer incidents, one company implemented a training and awareness program for employees on how to protect both their work and home computer networks. This program was well received by many employees and resulted in the early identification of threats to company networks. Another method that some companies us to educate employees is requiring that they read and sign a local IT user agreement (coordinated through the company's general counsel) in which they pledge not to violate the company's "safe" online behaviors.

PROACTIVE RESPONSE PREPARATION: RECOMMENDATIONS

- Executive leaders in the company should actively support and be engaged in insider threat efforts. When a significant insider threat event occurs, brief these leaders on its cause, all actions taken by the company, and the end result.
- Train HR to recognize and respond to malicious insider threat situations, especially those in which the employee is purposely harming IT systems or illegally removing propriety information. In addition, train employees to recognize the indicators to look for when hiring and recruiting staff.
- Develop and institute a focused training program to help employees identify suspicious employee or contractor activities, such as attempts at escalating privileges or access rights, creation of backdoor accounts, installation of unauthorized software, unusual physical access, violations of separation of duties, attempted social engineering, and so on. This program should teach employees how to report these activities immediately, so they can be triaged for proper response and defensive action.[13]
- Establish a confidentiality program for employees who report suspicious behavior to encourage staff to report suspicious incidents.
- Implement IT user agreements (coordinated through the company's general counsel) that employees must sign. These agreements can provide a clear legal basis for termination if they engage in unsafe actions that introduce malware, viruses, and other unapproved software to the network.

TECHNOLOGY

This section describes how the organizations interviewed use technology in their insider threat programs. The findings and recommendations are broken down into the three areas of insider threat technologies: prevention, detection, and response. Most of these tools focus on network or host activity, with very little inclusion of human behavioral issues. One organization is building its own tool because no tool on the market currently fits its needs.

PREVENTION TECHNOLOGIES: FINDINGS

Many of the organizations interviewed use detection technologies, but few mentioned preventive controls or methods. This deficiency is not surprising because preventing insider threat is similar to preventing crime. For the most part, people still act in certain ways despite the risk and potential consequences. In this study, prevention refers to technologies or techniques that reduce the means, motive, or opportunity to commit a crime.

Many of the organizations interviewed use detection technologies, but few mentioned preventive controls or methods. This deficiency is not surprising because preventing insider threat is similar to preventing crime.

Only one organization interviewed described a formal strategy for technically preventing insider threats. It uses these technologies: smart cards with two-factor authentication, strong passwords, user profiles, biometrics, laptop theft-tracking software, prohibiting employees from printing or downloading email, and disallowing

a "bring your own device" or BYOD environment where employees can bring their own smart phones or other technology for integration with the companies network. Most other organizations are investigating preventive controls or have no prevention strategy at all. Other organizations mentioned physical methods, such as role-based access controls for individual buildings and floors or video surveillance.

DETECTION TECHNOLOGIES: FINDINGS

Almost every organization interviewed uses some form of detection technology, including content monitoring; custom site blocking; a DLP tool with checks for "dirty words;" commercial DLP tools; custom technology; web-monitoring tools; a specialized insider threat tool to capture keystrokes and voice; foreign travel tracking; monitoring of daily time reporting; employee reporting sites; email monitoring; and log aggregation. Some of these tools were built solely for detecting insider threats, while others were repurposed from existing network or security-monitoring tools. Several organizations are in the process of testing different types of DLP or web-monitoring tools. Two organizations have custom-built tools they use for improving their detection capabilities. The prevailing technology across all organizations interviewed is web-content monitoring that uses existing proxy servers or a network-based, web-monitoring tool.

In the financial sector, many of the same technologies are also in use. In addition, most companies surveyed use host-based monitoring, monitor employees with privileged access, and monitor access to and movement of critical assets and intellectual property. Many also monitor off-hours activity and use configuration management tools; slightly more than half perform targeted auditing of employees with access to critical information when they resign. More than one-third monitor employees "on the HR radar" and use automated scripts to detect potential fraud activity. A few companies indicate they monitor employee mobile devices.

RESPONSE TECHNOLOGIES: FINDINGS

Insider threat response is closely related to traditional incident response. After detecting malicious insider activity, an organization must decide what actions to take. Whether it is gathering data for law enforcement or legal action, the response activities must be thorough, but conducted expeditiously and judiciously. Two organizations said they use commercial forensic tools for their response activities. These tools enable their incident response team to acquire employees' hard disks in a forensically sound manner for analysis and use in criminal prosecution.

TECHNOLOGY: RECOMMENDATIONS

Designing and Instrumenting Networks

- When designing networks, focus on data flow outside the organization as well as inside. Because insiders already have access to an organization's systems, data, and secrets, building an insider-resilient network takes some preparation. Building a network that uses preventative controls, enables detection, and informs response activities, begins with understanding what an organization wants to achieve with regard to security.
- To determine the most efficient technology to use, find out what tools are available and what data the organization wants to monitor and how. Many vendors call their product a DLP tool; it is important to make vendors clarify how their product will work for an organization's needs.
- Choose the right sensor types for what is to be monitored:
  - To develop long-term baselines of network activity, use a net flow sensor such as Yet Another Flowmeter (YAF) or System for Internet-level Knowledge (SiLK).
  - To better inform response activities or to further investigate them, use a full packet sensor.
  - To track employees' website visits or to focus on potential risky employees (e.g., those who with heavy personal email use), use a web content sensor.
- Choose the right log types for what is to be monitored:
  - To monitor logins, log outs, or USB device connects/disconnects, use Active Directory (Windows) or syslog (Unix).
  - To monitor websites visited (if not web content sensors), use proxy logs.

  - To monitor potential email-based exfiltration, use email logs.
  - To monitor employees deemed to be high risk, use HR logs (if none exist, build a database to contain HR information).
  - To monitor building-access logs, use physical security logs.
- Design networks with sensors in each organizational unit (OU). Often, members of particular groups or teams have similar access and browsing patterns. Rather than normalize the data across the organization, collocate sensors within the OUs to help identify discrepancies.
- Collect web content data at the enterprise level and collect net flow and full packet data at the OU level.
- Centralize collected data into a single server or into a log-aggregation tool for better analysis.
- Because federal and state laws may alter or prevent the use of certain monitoring tools, always consult with the Legal department before purchasing a monitoring system. Doing so may help avoid violation of privacy policies.

Taking Preventive Measures

- Make all employees in an organization aware of the insider threat mitigation program. Let them know that the latest technology is being used to protect them and to deter possible criminals from stealing sensitive information.
- Consider including human behavioral issues as part of the insider threat mitigation program. For example, combine the sensor logs of those with access to critical data, building-access logs, records of hours worked, and individuals that the HR department says are having problems. This combined view of data provides a much more complete picture of risk than simply relying on one or two tools.
- Gather data about how people interact with the system and try to build baselines over a period of at least six months. These baselines can later be used to identify anomalies that could point to insider incidents.
- Focus on deterrence rather than detection. One way to do that is to crowdsource security by allowing users to encrypt and classify their own data and to think of better ways to protect it. One can also let employees know that the company is tracking how they are using that data.
- Implement DLP tools properly to increase protection and prevent data loss.
- Implement strong password initiatives and force password changes regularly. Also, promote the dangers of password sharing and unlocked computers.
- Implement a biometrics platform to help create identifications for individuals. The criteria to create an identification can be used as a red flag for incoming or outgoing traffic. Monitoring individuals by level of security clearance and access to critical data can help better protect intellectual property.
- Maintain vigilance with social media. Educate all employees about the latest threats in social media networks and the dangers of revealing too much information in user profiles.
- Identify an organization's sensitive data and monitor who is accessing it.
- To better monitor and identify potential insiders, combine technical data (e.g., system logs, net flow, proxy logs) with nontechnical data on individuals (e.g., HR notes, sanctions, building logs).
- Consider requiring positions in critical business processes, like accounting, finance, benefits, inventory, and HR, to have back-up positions with overlapping responsibilities and shared access.

This security control is implemented by some organizations to deter individuals from participating in fraudulent activity, since someone else doing their job could potentially identify suspicious or fraudulent activity.

- Implement separation of duties so that more than one person is required to perform a business process to prevent employees from committing fraudulent activity against the organization.
- Consider implementing separation of duties for critical functions in the IT department, such as creating or destroying credentials; provisioning or modifying authorization to IT assets; creating and deleting transaction logs; and creating and destroying backups. This separation may reduce the likelihood that a privileged IT employee could singlehandedly affect the confidentiality, availability, or integrity of critical information or systems.
- Apply the concept of least privilege to all employees, contractors, sub-contractors, and trusted business partners to ensure they have only the minimum privileges needed to perform their job. All too often, individuals accumulate access as they migrate between departments or jobs, giving them access to resources they no longer need and possibility providing them with the ability to bypass the separation of duties implemented to prevent fraudulent activity.

Detecting Malicious Insiders

- Implement a behavioral monitoring program on an organization's network.
- Use log aggregation or security information management tools to decrease the time it takes to detect incidents.
- Run tests on the network by sending "false" requests for information to employees to see if they respond.
- Use network-based computer forensic tools that contain signature and hash analysis.
- Acquire forensic analysis capabilities.

Responding to Incidents

- Ensure that all responses requiring legal action are backed with accurate intelligence and presentable evidence.
- Implement a Security Operations Center for reporting and responding to incidents.
- For all cases that involve investigations, collaborate with the HR and Legal departments.
- Incorporate a triage system with incident response.

CONCLUSION

> Insider threat experts agree that an insider is a person—a human being—a heartbeat.

Many organizations think that insider threat programs are technology-focused and centered on the digital cyber world and its networks. However, insider threat experts agree that an insider is a person—a human being—a heartbeat. To protect an organization, one must use tools to monitor the traffic in and out of the networks and be able to focus that monitoring on specific people who do something concerning or suspicious. It is equally important to have a manual or automated process for identifying psychosocial events—anomalous, suspicious, or concerning nontechnical behaviors. A robust insider threat program integrates and analyzes technical and nontechnical indicators to provide a holistic insider threat risk score on an individual basis.

Whether an organization has just ten employees or hundreds of thousands, insider threat is always a security risk. Information is valuable—whether it is a trade secret, important research data, or bank account information. However, all too often insider threat is equated with theft of information, or in the financial sector, fraud. Consider the risk of insider IT sabotage. What if an employee, contractor, or business partner sabotages a critical system or tampers with the integrity of a company's information?

Systems and data can be heavily guarded by personnel or require many different physical and/or virtual keys for access. Unfortunately, attackers motivated by greed, revenge, ego, and ideology can come from both sides of the front door. The tools available to use against potential attacks are very real and will work—but at what cost? As malicious insiders become more innovative, the cost associated with defending against them will grow. Every organization needs to consider its risk tolerance to insider threat and assign the appropriate mitigations within its budgetary framework.

In fact, insider threat risk mitigation should be integrated into an enterprise risk management process. This process should identify critical assets, including systems, services, programs, and information that, if compromised, would cause harm to the organization, people, national security, or others. A threat assessment should identify both internal and external threats to those assets. Finally, a mitigation strategy should be designed and implemented accordingly.

INSA hopes this report sheds light on what some organizations are doing and what can be done to mitigate the threat posed by insiders. We hope, in a future report, to provide a more comprehensive benchmark and elaborate on the practices we've provided here by gathering additional input from those gaining practical experience confronting insider threats in the private sector.

APPENDIX A: Interview Questions

1. Do you have a formal insider threat incident handling process?
    a. Is it part of your normal incident response process or different?
    b. Is your computer security incident response team involved in the handling of insider threats?
    c. Describe the process or how the insider threat would be handled.
    d. How would this process change if contractors, subcontractors, suppliers, trusted business partners, or unions were involved?
    e. Are your account management processes the same or different for contractors and subcontractors?
    f. What is your process for mergers and acquisitions?
    g. How would this process change depending on the type of incident (i.e., fraud, sabotage, IP theft)?
    h. What types of organizational policies or procedures are in place that enable or constrain your handling of such incidents?
    i. Are there thresholds that must be met before a specific type of enforcement action is taken? What are they?
    j. How effective is this process?
2. Do you have a formal insider threat mitigation program to help prevent such incidents?
    a. Who has authority for this program?
    b. What does the program include (i.e., the components)?
    c. What types of technologies are used to detect and prevent insider incidents as part of this program?
    d. What type of training and awareness is done for your organization's employees?
    e. What type of training is done for the personnel that handle such insider threat incidents?
    f. Do employees sign IP agreements, acceptable use policies, and/or standards-of-conduct forms?
    g. How effective do you think this program is?
3. Have you had an incident at your organization that was perpetrated by an insider?
    a. If yes,
        i. How was it detected (e.g., by accident, by monitoring, by reporting, through incident or forensic analysis)?
        ii. Where was it reported? What part of the organization?
        iii. Who handled the incident through resolution? What part of the organization? What type of staff (e.g., HR, Legal, IT, Security, specialized team)?
        iv. How many such incidents would you say you have had in the last ten years? How many, on average, in a year? Last year?
    b. If no,
        i. Where would you want the incident to be reported?
        ii. Who would handle the incident through resolution?

APPENDIX B: Survey of Financial Sector Organizations

1. How many full-time employees are in your financial institution?
2. Which one of the titles most closely describes you?
3. What does your definition of "insider threats" include?
4. Does your organization have a formalized plan for responding to insider security events committed against your organization?
5. Is the plan part of your normal incident response process?
6. Who has the authority for handling events perpetrated by an insider?
7. How is your computer security incident response team involved in the handling of the event?
8. How effectively does your organization report, manage, and intervene in cyber threats with internal employees?
9. Do you have a formal Insider Threat Mitigation Program to help prevent such incidents?
10. Who has (or will have) authority for this program?
11. What does the program include (i.e., the components)?
12. What type of technologies are used (will be used) to detect and prevent insider incidents as part of this program?
13. What type of training and awareness is provided to your organization's employees?
14. What type of training is provided to the personnel that handle insider threat incidents?
15. How effective do you think your Insider Threat Mitigation Program is?
16. Provide the percentage of cyber crimes committed by insiders at your organization in the following categories?
17. How are most insider incidents or events at your organization detected?
18. How many insider incidents does your organization experience per year?
19. What percentage of insider incidents in your organization caused significant damage?
20. Provide the percentage of insider incidents in your organization that belong to the following categories.
21. How has the number of incidents changed in the last year?
22. What actions has your organization taken in the last year with respect to insider threat?

The results of this online survey can be found on the INSA website at www.insaonline.org.

ENDNOTES

[1] *A common ontology does not exist across government and industry for cybersecurity and the threats posed by insiders. The following five definitions are from government sources:*

***Counterintelligence**—Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or international terrorist activities, but not including personnel, physical, document or communications security programs.* Executive Order 12333 (4 Dec 1981)

***Counterintelligence**—Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or their agents, or international terrorist organizations or activities.* Executive Order 12333 (as amended 30 July 2008 and JP 2-01.2, CI & HUMINT in Joint Operations, 11 Mar 2011)

***Counterintelligence**—Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. Department of Defense Directive 5240.2 (22 May 1997)*

***Counterintelligence**—Information gathered and activities conducted to detect, identify, exploit, and neutralize the intelligence capabilities and activities of terrorists, foreign powers, and other entities directed against U.S. national security.* Department of Defense Instruction 5240.17 (26 Oct 2005)

***Counterintelligence insider threat**— A person, known or suspected, who uses their authorized access to DoD facilities, personnel, systems, equipment, information, or infrastructure to damage and disrupt operations, compromise DoD information, or commit espionage on behalf of an Foreign Intelligence Entity (FIE).* Department of Defense Instruction 5240.26 (4 May 2012)

[2] *Richards, Kathleen. "RSA 2013: FBI Offers Lessons Learned on Insider Threat Detection."* TechTarget SearchSecurity.com. *http://searchsecurity.techtarget.com/news/2240179082/RSA-2013-FBI-offers-lessons-learned-on-insider-threat-detection (2013).*

[3] *The White House. Executive Order 13587*–Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information. *http://www.whitehouse.gov/the-press-office/2011/10/07/executive-order-structural-reforms-improve-security-classified-networks- (2011).*

[4] *The White House.* Presidential Memorandum–National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs. *http://www.whitehouse.gov/the-press-office/2012/11/21/presidential-memorandum-national-insider-threat-policy-and-minimum-stand (2012).*

[5] *In this report, we define* insider threat *as malicious activities by a current or former employee, contractor, or trusted business partner, including fraud, IT sabotage, theft of intellectual property, and espionage.*

[6] *Department of Homeland Security.* Critical Infrastructure Sector Partnerships. *http://www.dhs.gov/critical-infrastructure-sector-partnerships (2013).*

[7] *Software Engineering Institute.* Insider Fraud in Financial Services. *http://www.sei.cmu.edu/library/abstracts/brochures/12sr004-brochure.cfm (2012).*

[8] *The Commission on the Theft of American Intellectual Property.* The Report of The Commission on the Theft of American Intellectual Property (2013) *http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf*

[9] *Silowash, George; Cappelli, Dawn; Moore, Andrew P; Trzeciak, Randall F.; Shimeall, Timothy J.; & Flynn, Lori.* Common Sense Guide to Mitigating Insider Threats, 4th Edition. *http://www.sei.cmu.edu/library/abstracts/reports/12tr012.cfm (2012).*

[10] *Band, Stephen R.; Cappelli, Dawn N.; Fischer, Lynn F.; Moore, Andrew P.; Shaw, Eric D.; & Trzeciak, Randall F.* Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis. *http://www.sei.cmu.edu/library/abstracts/reports/06tr026.cfm (2006).*

[11] *Office of the President.* Administration Strategy on Mitigating the Theft of U.S. Trade Secrets. *http://www.whitehouse.gov//sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf (2013).*

® CERT and CERT Coordination Center are registered marks of Carnegie Mellon University.

[12] *See http://www.cert.org/insider_threat/ for more information on the CERT Insider Threat Center.*

[13] *"Separation of duties" is the concept of more than one individual required to complete a task.*

ABOUT INSA

INSA is the premier intelligence and national security organization that brings together the public, private and academic sectors to collaborate on the most challenging policy issues and solutions.

As a non-profit, non-partisan, public-private organization, INSA's ultimate goal is to promote and recognize the highest standards within the national security and intelligence communities.

INSA has over 150 corporate members and several hundred individual members who are leaders and senior executives throughout government, the private sector and academia.

To learn more about INSA visit www.insaonline.org.

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE
BUILDING A STRONGER INTELLIGENCE COMMUNITY

901 North Stuart Street, Suite 205, Arlington, VA 22203
(703) 224-4672 | www.insaonline.org