Insider Threat Workshop Proceedings
Papers and Presentations from the CSIAC Insider Threat Workshop
July 2013
TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>BACKGROUND</td>
<td>1</td>
</tr>
<tr>
<td>1.0 INSIDER THREAT: POLICY IMPACT AND OVERVIEW</td>
<td>3</td>
</tr>
<tr>
<td>2.0 PERSONNEL BEHAVIOR PHYSICAL AND VIRTUAL: THE WHOLE PERSON</td>
<td>26</td>
</tr>
<tr>
<td>INSIDER THREAT ANALYSIS PARADIGM</td>
<td></td>
</tr>
<tr>
<td>3.0 PANEL QUESTIONS &amp; ANSWERS TRANSCRIPT</td>
<td>40</td>
</tr>
<tr>
<td>4.0 ANNOTATED BIBLIOGRAPHY</td>
<td>56</td>
</tr>
<tr>
<td>5.0 ABSTRACTS</td>
<td>58</td>
</tr>
<tr>
<td>5.1 Personnel Behavior Physical and Virtual: The Whole Person Insider</td>
<td>58</td>
</tr>
<tr>
<td>Threat Program</td>
<td></td>
</tr>
<tr>
<td>5.2 Insider Threat Workshop Keynote</td>
<td>59</td>
</tr>
<tr>
<td>5.3 Security Attacks and Cyber Crime: Computing through Failures and</td>
<td>61</td>
</tr>
<tr>
<td>Cyber Attacks (Insider Threat Workshop Presentation Summary)</td>
<td></td>
</tr>
<tr>
<td>5.4 Localized Encryption Groups</td>
<td>64</td>
</tr>
<tr>
<td>5.5 Insider Threats Current Events: The Critical Infrastructure</td>
<td>66</td>
</tr>
<tr>
<td>Security Perspective: Cutting Costs or Cutting Our Throats?</td>
<td></td>
</tr>
<tr>
<td>5.6 Generation Y Insider Threat</td>
<td>67</td>
</tr>
<tr>
<td>APPENDIX A – PRESENTATIONS</td>
<td>A-0</td>
</tr>
<tr>
<td>Personnel Behavior Physical and Virtual: The Whole Person Insider</td>
<td>A-1</td>
</tr>
<tr>
<td>Threat Program Presentation</td>
<td></td>
</tr>
<tr>
<td>Insider Threat Workshop Presentation</td>
<td>A-15</td>
</tr>
<tr>
<td>Security Attacks and Cyber Crime: Computing through Failures and</td>
<td>A-21</td>
</tr>
<tr>
<td>Cyber Attacks (Insider Threat Workshop Presentation Summary)</td>
<td></td>
</tr>
<tr>
<td>Localized Encryption Groups Presentation</td>
<td>A-40</td>
</tr>
<tr>
<td>Insider Threats Current Events: The Critical Infrastructure Security</td>
<td>A-45</td>
</tr>
<tr>
<td>Perspective: Cutting Costs or Cutting Our Throats? Presentation</td>
<td></td>
</tr>
<tr>
<td>Generation Y Insider Threat Presentation</td>
<td>A-49</td>
</tr>
<tr>
<td>Insider Threat Research and Development Presentation</td>
<td>A-65</td>
</tr>
<tr>
<td>Best Practices in Insider Threat Mitigation Presentation</td>
<td>A-68</td>
</tr>
</tbody>
</table>
LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1. Research Methodology Overview</td>
<td>32</td>
</tr>
<tr>
<td>Figure 2. Percentage of AOB cases proportional to overall case load</td>
<td>33</td>
</tr>
<tr>
<td>Figure 3. Detailed look at percentage of AOB cases proportional to overall case load for the top 3 criteria</td>
<td>34</td>
</tr>
<tr>
<td>Figure 4. Detailed look at percentage of AOB cases proportional to overall case load for lower prevalence concerns</td>
<td>34</td>
</tr>
<tr>
<td>Figure 5. Common Link</td>
<td>37</td>
</tr>
</tbody>
</table>

LIST OF TABLES

<table>
<thead>
<tr>
<th>Table</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 1. Interesting Higher Risk Offline / AOB Pairs</td>
<td>35</td>
</tr>
</tbody>
</table>
BACKGROUND

This update to the “Insider Threat to Information Systems” State of the Art Report (SOAR) was requested in the fall of 2012 by Dr. Steven E. King, Deputy Director for Cyber Security in the Information Systems and Cyber Security Directorate of the Assistant Secretary of Defense for Research and Engineering, ASD (R&E). The 2008 “The Insider Threat to Information Systems” SOAR was published by the Defense Technical Information Center (DTIC) under the Information Assurance Technology Analysis Center (IATAC). As heir to the IATAC, the Cyber Security and Information Systems Information Analysis Center (CSIAC) was asked to take on the task. Quite a lot had happened in the interim, notably the WikiLeaks exploits of Pfc. Bradley Manning and Publisher Julian Assange. The former was to be sentenced to 35 years in prison the following year, two weeks after the CSIAC held the workshop whose proceedings you are about to read. Little did we know when we started preparations for this update that the Department of Defense (DoD) and the American public would also be heading for a much more serious confrontation with former Central Intelligence Agency (CIA) employee Edward Snowden.

The approach in producing this update was to host an Insider Threat Workshop on 15 August 2013 at the Griffiss Institute in Rome, N.Y., and to provide the findings of this open forum. The Insider Threat Workshop was a one-day review of current trends in Insider Threat tactics and remediation steps of interest to cybersecurity professionals. The workshop provided an overview of the current state of understanding of who the “insiders” are, how they operate, and what threats they pose to information systems and what motivates them. The workshop addressed newer material based on current technology, such as Cloud Computing and Bring Your Own Device (BYOD), and the threats they impose. Participants included members of DoD, academia, state and federal agencies, homeland security, and supporting contractors. We were able to provide significant coverage of the impact of insider’s activities in the course of the workshop and the subsequent publication of this update.

This report, considered to be an addendum to the original SOAR publication, includes research papers provided by attending participants, the slides from all PowerPoint presentations, and transcriptions of our panel discussions. It opens with an original paper by the Center for Infrastructure Protection and Homeland Security, George Mason University School of Law, which CSIAC commissioned for this anthology.
The challenge to National Security from Insider Threats through commission and omission has grown, as has the cybersecurity challenge in general. New DoD policies and practices on continuous evaluation, monitoring, and access control are being put into place now, and the situation will continue to evolve. We will endeavor to do so as well.
1.0 INSIDER THREAT: POLICY IMPACT AND OVERVIEW

Authored By: Christopher Woolley, JD and Mark D. Troutman, PhD

I. Executive Summary

“Insider threat” has become a common concept in the aftermath of the Edward Snowden scandal. This White Paper provides a summary and analysis of the current state of policy and law, the relationship of these elements to the problem of insider threat, and suggests measures to address observed and potential future threats. A single measure is insufficient for protection. Rather, organizations must put in place an integrated system of reinforcing measures and update them as conditions change.

While Snowden has become the current paradigm of insider threat, his profile does not represent all cases for consideration. The information age makes it possible for even low level employees to gain access to unprecedented volumes of data and pose a significant security risk. Insider threats from individuals operating for monetary motives or non-malicious security slips can be as great or greater threats than those from an ideologically driven actor such as Snowden. While no easy or universal solution to address insider threat behaviors exists, it is possible to reduce the risk of occurrence and mitigate the effects of undesirable behavior.

Policy provides broad guidelines for executive action. Legal recourse is a valuable instrument, offering post hoc disincentives of criminal and civil penalties that can impose costs to deter insiders who wish to disclose unauthorized information. However, law cannot reclaim leaked information, and the efficacy of legal or civil penalties is questionable as a deterrent for other insiders. Our research reveals that effective statutes exist, but are in some cases infrequently applied given the vast nature of insider threat.

Outside of the legal world, there are three basic strategies to mitigate insider threat: restrict access to secure information, structure incentives and disincentives to prevent unauthorized disclosure of information, and make the information itself smarter, to facilitate traceability and accountability for sensitive information. A loose analogy for the first approach is to build a stronger wall around a city. The “city” is secure information and the systems which enable its use, and the wall surrounding it the measures taken to restrict access. Structuring incentives to prevent leaks assumes the wall will be broken. Therefore the “city” should be laid out to incentivize loyalty and provide disincentives for leaking sensitive information. Smarter data implies using data structures which make movement more traceable and its ownership, possession, and use more accountable.
II. Key Findings.

1) The motivation for Insider threat falls into three broad classifications, each of which requires specific measures to mitigate the threat.

   a) The threat can come from idealists like Snowden.

   b) The threat can also come from employees motivated by monetary benefit.

   c) A broad threat exists from non-malicious behavior that results from carelessness or lack of competence.

2) Organizations have legal tools available, but these may be under applied. Because legal measures are only applied after the disclosure, they are reactive and cannot offer a perfect remedy to a breach. Therefore, the true efficacy of legal measures as a remedy for the insider threat problem is difficult to measure.

3) Organizations can mitigate insider threats by restricting access to sensitive data. Some broad approaches which incentivize loyalty or provide a disincentive to leaks include:

   a) Hiring practices such as vetting, screening, and employment contract provisions that shape behavior to achieve desired organizational outcomes.

   b) Use of recurring processes such as promotion practices and reviews that reveal new information about employee behavior and allow for the adjustment of access.

   c) The use of structured screening and frequent review for those with greater access as a result of position, seniority, or function to provide a more frequent check on activity.

4) Organizations can reduce the impact of threats by structuring incentives to shape use of access for functions in line with organization norms and to contain the impact of unauthorized release. Some broad incentive-based approaches include:

   a) Use of a value-based approach that aligns individual and organization-based ethics and allows for adjustment when disagreements occur.

   b) Thorough observation of employee behavior that is identified in employment contracts and periodically updated. Technology can assist, but will not completely solve this problem.
c) Linkage of compensation and bonuses to favorable compliance with security practices. Compensation can be intrinsic, such as the prestige or status afforded to a role. Compensation can be extrinsic and linked to desired results. Examples of this linkage are accelerated promotion or deferred compensation that flows after favorable review and demonstrated accountability.

d) Review processes that involve more than one person in the organization and that tie results to corrective action with rewards (for compliance) and penalties (for non-compliance)

5) Organizations should consider using “smarter” data for high value categories of information to provide a trace which establishes accountability for those granted access to these categories.

a) Data structures which track usage and access can create accurate records of use.

b) Depending on the type of system employed, such data structures might also be able to raise alarms if unauthorized users access special category data.

c) The existence of this special tracking capability should be known and disclosed in employment contracts. However, the specific application to categories of data need not be disclosed.

6) Organizations require an integrated framework of measures that include those outlined above. Screening and frequent reaffirmation of expected organizational behavior create cultures of accountability and trust. These measures can be combined with reviews that give employers and employees the opportunity to renew commitments and resolve differences between organizational and individual goals. These procedures provide a framework to align organization and individual goals in voluntary employment relationships.

Introduction

The case of Edward Snowden brought insider threat to the forefront of the public and corporate mind. Snowden provides a case study for the intelligent insider threat, the employee who acts in violation of organization policy, often without warning, and discloses restricted information to the public or a competitor. Snowden’s tale serves as a warning call to government and industry Leaders.

Snowden also serves as a reminder that threats can come from the most unexpected places. His is not the only insider threat story, nor is it the only damage that requires prevention or mitigation.
Individuals seeking personal gain or complacent employees can do as much or more damage. In some ways, they are more threatening than the Snowdens of the world because they have incentive to keep their job, either as a source of information or income. Snowden knew he would not be coming back. His breach was massive but limited in time.

This paper serves as an overview of the incentives involved in mitigation and prevention strategies. It is important to note that there is no conclusive technique to identify insider threats before they occur, nor is there any way to completely prevent the damage they can inflict. However, this study will provide insight into policy which shapes measures and legal tools available to deter unauthorized release. The study will also suggest practical incentive structures, procedures, and use of technology to incentivize compliance and provide a disincentive against unauthorized use. However, leaders must always bear in mind that the decision to provide access to sensitive information bears a risk that the granted party will misuse that access. Therefore, the decision to grant access remains a risk based judgment that the granted party will use the access for purposes that are in line with the organizations’ purposes and ethical framework.

What Does an Insider Threat Look Like?

SEI-CERT defines a malicious insider threat as “a current or former employee, contractor, or other business partner who has or had authorized access to an organization’s network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization’s information or information systems.”

SEI-CERT also acknowledges the existence of unintentional or non-malicious insider threat, which it defines in its blog as “a current or former employee, contractor, or business partner who has or had authorized access to an organization’s network, system, or data and who, through their action/inaction without malicious intent, negatively affects the confidentiality, integrity, or availability of the organization’s information or information systems.”

The SEI-CERT definitions and criteria will define what constitutes threat for this work.

Idealists. Snowden is an example of the idealistic insider. Despite the difficulty of identification, Snowden’s case revealed some indicators that after the fact, paint the picture of an employee with motivations that became different over time from the priorities of the organization. Snowden was

---

1 CERT Insider Threat, https://www.cert.org/insider-threat/
intelligent and convinced that he acted from principled motives. He did not follow the usual course of high school, college, and work pursued by others who held similar functions. He identified strongly as a libertarian in principle. Discussions on internet forums prior to his information release show limited knowledge of broad policy issues, combined with strongly held beliefs. In many ways he is analogous to a “hacktivist,” intelligent and technologically savvy with a strong ideological motivation.

Briefly stated, Snowden held personal motivations that over time diverged from his organization’s priorities. After initial agreement with the intelligence missions of the organizations he joined, Snowden’s views changed as he gained more knowledge of his organization’s operating practices. He felt over time that practices he observed were at odds with democratic norms and impinged on basic freedoms. Snowden claims that he expressed concerns to ten different superiors over the period of his employment. He felt his leaders ignored or dismissed his observations, and perceived that further observations could bring punishment. Snowden concluded that, as a contractor, he “was not protected by US whistleblower laws, and [he] would not have been protected from retaliation and legal sanction.” Whether or not he would have been protected at the time is still somewhat unclear, a fact which in itself is an issue. When he believed the avenues of recourse were insufficient to provide redress, Snowden chose to provoke change by making restricted information public.

Snowden’s position involved broad and trusted access to information. He held access to data beyond levels granted to many members of his organization in order to resolve technical issues, ensure security, and promote efficiency. The decision to grant more access to information in order to promote information sharing within the intelligence community was a deliberate one. Likewise deliberate was the decision to employ contracted specialists such as Snowden to quickly expand the organization’s capabilities. Government leaders employed such measures to address issues of compartmentalization and capability that post 9/11 assessments identified as factors that limited the ability of intelligence analysts to discern patterns and make assessments.

Snowden’s extensive technical skills enabled him to exploit his broadly granted access in unique ways. Intelligence organizations trusted Snowden to work with computers, which formed the

4 Ibid., at 6. Had he been a government employee working in the intelligence sector, the Whistleblower Protection Act would have unambiguously extended to cover him, under Presidential Policy Directive 19.
access points of domestic and international intelligence networks through NSA systems. His status and skills as a network administrator allowed him to move relatively unfettered and without trace of his activity. Ultimately, his leaks caused damage to his employer and the NSA. Snowden became a household name, but apparently has gained little monetary advantage from his disclosures.

Monetary Motivations. Sometimes an outside party approaches a trusted worker in the United States government or the private sector with an offer of monetary gain in exchange for insider information. The employee sees an incentive, often but not necessarily financial, for the installation of access to an information source or in exchange for a storage device full of information. The insider thinks his actions are justified based on need or entitlement. In the process, the organization suffers damage and loses integrity through the compromise of information.

Foreign governments and companies alike have long enticed insiders to leak information. As recently as 2013, a US soldier, Colton Millay, received a prison sentence for trying to sell secrets to Russia. In the corporate world, the danger is no less present. A recent case found two individuals guilty of conspiracy to sell trade secrets to the Chinese government. Insiders willing to sell secure information operate from monetary motives, seeking to sell the trust placed in them to the highest bidder or in exchange for items of value.

Non-Malicious Insiders. Another category of insider threat is not malicious in motive. A poorly trained or inattentive employee can spill secrets over time as precipitously as one who intentionally discloses them. Recently, an IRS employee accidentally exposed thousands of government employees to identity theft. Carelessly, he took a thumb drive home which contained sensitive information, including social security numbers of thousands of coworkers, and connected it to his relatively unsecured home computer. So far the information has not been used by nefarious actors, but the incident would not have occurred if the IRS employee maintained proper security procedures.

---


Another common vulnerability involves employees who fall prey to a “spear phishing campaign,” exposing the entire network to unauthorized access and malware. Such campaigns, which prey on the less technologically literate or able in an organization, are an easy access point for malicious actors to gain access to sensitive information.

**DOD Policy Changes in Response to Insider Threat Vulnerabilities**

**Physical Vulnerabilities.** The physical security aspects of the recent incidents at the Washington Navy Yard have been broadly addressed in the Internal Review of the Washington Navy Yard Shooting of 20 November 2013. The reader is directed to the original document for a full treatment of the necessary and recommended future policies and procedures identified by the Internal Review Board. We provide below the most salient points given in the Executive Summary:\(^8\):

- A centralized insider threat management capability that leverages multidisciplinary subject matter experts and links to functional and organizational areas of responsibility.

- A continuous evaluation program that provides actionable information in real time on the entire cleared DoD population, is serviced by the DoD Consolidated Adjudications Facility (CAF), folds in DoD Intelligence Community personnel as appropriate, and is scalable to include all DoD personnel subject to suitability or fitness adjudications.

- A physical security approach that employs defense in depth using technology and manpower to reduce risk and mitigate potential threats.

The Internal Review Team recommended the following actions:\(^9\):

- Establish a DoD Insider Threat Management and Analysis Center (DITMAC) to provide a centralized capability that can quickly analyze the results of automated records checks and reports of behavior of concern and recommend action as appropriate.

---

\(^8\) Internal Review of the Washington Navy Yard Shooting, Under Secretary of Defense for Intelligence, Nov 20 2013, p.4.

\(^9\) Ibid. p.5
• Leverage existing continuous evaluation capability while continuing to develop and implement a DoD Continuous Evaluation Program.

• Accelerate the Defense Manpower Data Center’s development of the Identity Management Enterprise Services Architecture (IMESA) to enable DoD Components to share access control information and continuously vet individuals against U.S. Government authoritative databases.

We will provide further policy amplification on the impact of the above findings in the following discussion.


“all personnel in national security positions will be required to have a PR every 5 years (regardless of the level of clearance), and a portion of personnel with Top Secret clearances will be subject to a continuous evaluation process as prescribed by the Director of National Intelligence as the Security Executive Agent.”

The Continuous Evaluation Program (CEP). The Army completed a pilot study recently as part of the next generation Automated Continuing Evaluation System (ACES). The current ACES program does not appear scalable to the entire DoD. While results of the small (3,700) Army pilot study were positive, it remains to be seen how the Director of National Intelligence will implement a DoD wide program. The current Identification and Access Management program (IDAM) for DoD is slated to be operated by DISA under the ongoing Joint Information Environment Migration. DoD-wide coordination of this high visibility program under JIE migration will require significant fine tuning.

10 Ibid. p.13
Although physical security is a concern for any insider threat discussion, we focus on those common elements shared across multiple security domains here. Of initial interest will be that element in the trust-chain that centers on Personnel Security Clearance processes and Access Control. We will discuss recent developments in Policy in that will be implemented by DoD and the U.S. Government.

**Cyber Risk Management and the Continuous Monitoring Program.** Although physical security is a concern for insider threat analysis the asymmetric nature of the cybersecurity threat as well as the rapidly changing technical landscape increases our concern for this threat vector. The true cost of the loss of classified or Controlled Unclassified Information (CUI) is difficult to assess, given that victims do not always have an accurate estimate of the extent of the compromise, the extent of the subsequent dissemination of the lost information, or the resultant use that will be made of the compromised information by whatever parties obtain it. We do not address the compounding problem of the introduction of maliciously modified data or malicious executable code. The repercussions from the information systems control breaches exemplified in the Snowden and Manning compromises are huge, and will initiate major changes in clearance management, personnel evaluation, and access control. Digital systems offer the opportunity to transfer data in great volumes, in a manner that may be difficult to detect, and with recurring effects. As noted above, a personnel continuing evaluation program (CEP) is being advocated for DoD. In addition, DoD is promoting a continuous monitoring posture for the information systems to which DoD personnel have access. Information systems capabilities for supporting continuous monitoring are to be implemented to the greatest extent possible according to the latest Risk Management Framework (RMF) for DoD Information Technology (IT) DoDI 8510.01.\(^\text{11}\) Information System Security Managers are required to continuously monitor and assess their information systems and “recommend changes or improvement[s] to the implementation of assigned security controls, the assignment of additional security controls, or changes or improvements to the design of the system…”\(^\text{12}\)

National Institute of Standards and Technology Special Publication 800-53, Revision 4 issued in April 2013, which now serves as the baseline for the Risk Management Framework (RMF) for

\(^{11}\) Risk Management Framework (RMF) for DoD Information Technology (IT) DoDI 8510.01 12 March 2014, p.3.
\(^{12}\) Ibid., p.37.
DoD Information Technology. The NIST authored 800 series security instructions have now replaced DIACAP across the DoD by direction of the DoD CIO. Revision 4 states:

“…a more holistic approach to information security and risk management by providing organizations with the breadth and depth of security controls necessary … to systems that are more resilient in the face of cyber-attacks and other threats. This ‘Build It Right’ strategy is coupled with a variety of security controls for ‘Continuous Monitoring’ to give organizations near real-time information that is essential for senior leaders making ongoing risk-based decisions affecting their critical missions and business functions.”

A risk-based approach assumes a consequentialist calculus to estimate risk, as shown below. However, one assumption in the computation is that one knows the impact of the loss of confidentiality. If one does not know the extent of the disclosure, it is difficult to do actual post hoc damage assessments. The general practice is to calculate based on the worst case scenario. The underlying risk assessment leading the security category (SC) of an information system is estimated by the following formula:

\[ SC_{\text{information system}} = f(\text{confidentiality, impact), (integrity, impact), (availability, impact}) \]

For determining the types of access control commensurate with the level of risk associated with an information system, NIST and the DoD CIO direct that that information system will generate “overlays” to their baseline access policies based upon specific conditions associated with the information systems. Recommended control enhancements include Dual Authorization also known as two-person control. Dual Authorization mechanisms require the approval of two authorized individuals in order to execute an action. In response to the Snowden case, General Alexander has stated he will be initiating increased two-man control for sys-admins within NSA as well as looking at implementing autonomous system administration capabilities to lower the attack surface from within NSA IT systems, which will decrease the number of actions requiring Dual Authorization.

---

13 Ibid.
15 Ibid, p.28.
Research and Development Requirements. We have mentioned above that the time interval between recertification will drop from 10 to 5 years Continuous Evaluation Program will need to develop scalable solutions for continuous personnel evaluation. As stated above, NSA is looking for improved autonomous systems administration capabilities to lower the insider attack surface, which will no doubt have application within DoD at large. Another area that will need additional gap analysis and R&D is an effective coupling between the new capabilities for continuous personnel evaluation, automated access control, and continuous monitoring. This does not address the legal, policy, and process management issues regarding the increased coupling between these areas, only the resolution of the technical constraints of carrying out such a program.

Policy and Legal and Tools to Prevent Insider Threat

The following section outlines policy and legal measures that address insider threat situations and assesses their use and effectiveness.

Executive Order 13587. In 2011, prior to the Snowden leaks, the Obama Administration issued an executive order directing executive agencies to review and revise their sensitive information handling procedures. In some measure a reaction to the WikiLeaks scandal, the Order creates a Steering Committee to oversee information sharing, coordination, and security standards in the federal government. The Order charges each agency with the responsibility to maintain its own security standards and test compliance. The Order also creates an executive agent for safeguarding classified information on computer networks and establishes an Insider Threat Task Force. The Task Force is charged with determining a government wide system to mitigate insider threat, and specifically addresses “deterrence, detection, and mitigation” of insider threats. The Order covers those contractors that have access to classified information as well as the federal government.

The Order defines broad guidelines for responsibility and standards. The federal government has followed through with policies and regulations to implement guidelines, but the work is ongoing. The Order created the Classified Information Sharing and Safeguarding Office, which primarily focuses on monitoring, policing, and regulation of information sharing. Individual agencies are responsible for developing specific organizational procedures, but there still exist concerns. Agencies are continuously working to improve on their programs. Measures include procedures

18 Ibid.
19 Specifically, the National Insider Threat Policy, which defines standards from EO 13587 bounded by Executive Orders 12968 and 13526, available at http://www.fas.org/sgp/obama/insider.pdf.
and technology to detect and reduce threats. For example, the DoD recently submitted a solicitation for contractors to develop better forms of protecting, sharing, and storing classified information.²⁰

There is still concern in the government over what insiders can do, and for good reason. The Snowden case is instructive in that he was a contracted employee to the government with access to confidential information. The changes wrought by the Order were not enough to prevent or deter Snowden from leaking.

**Legislation as a Deterrent**

**The Espionage Act of 1917.** The Espionage Act is one of the oldest legal frameworks in place to protect against insider threat. Passed in 1917, it was enacted at a time when “insider threat” was not a ubiquitous concept. Still, the nation has used sections of the act to punish insiders who have leaked information to foreign powers. Sections 792 and 793 of the act specifically target people who have released defense information to foreign powers, and Section 798 concerns itself with the release of confidential information.²¹

This Act has been employed to level criminal charges against insiders who give access to or make public confidential or other information that the government deems important to defense, areas which can often overlap.²² In 1985, Samuel Morison was the first person convicted under the Act for conveying classified information to the press, but he was not the last.²³ More recently, Chelsea (then Bradley) Manning leaked thousands of classified documents to the press, and was found guilty under the Espionage Act.²⁴

Overall, the law has not been employed with great frequency to prosecute insiders leaking information. It has been used more often in recent years, but the number of cases remains small.²⁵

²² In United States v. Abu-Jihaad, 630 F.3d 102 (2d Cir. 2010), the Defendant was found guilty of leaking information which was both classified and related to defense.
²³ United States v. Morison 844 F.2d 1057,(4th Cir. 1988).
²⁵ The eight times the Espionage Act has been used in the Obama administration to prosecute insiders outnumbers all previous presidents’ uses of the statute in a similar manner. In addition to Snowden and Manning, cases include United States v. Jin-Woo Kim, 808 F. Supp. 2d 44 (D.D.C. 2011). In re Shamai Leibowitz, 72 A.D. 3d 1190 (N.Y. App. Div. 2010), U.S. v. Hitselberger, 909 F.Supp 2d 4 (D.D.C. 2012), and United States v. Kiriakou, 898 F.Supp. 2d 921 (E.D. Va. 2012). However, in 3 of these cases, the charges using the Espionage Act were
Its utility as a tool to prevent insider threat is further limited because of the type of information it protects; it is limited to safeguarding confidential information or information vital to the nation’s defense.\textsuperscript{26} It has been used against civilians or civilian entities with access to confidential or damaging information,\textsuperscript{27} but more often it has been used against military personnel.

**The Economic Espionage Act of 1996.** As the name implies, this statute aims to protect the intellectual property of businesses. It has also been used to punish insiders. The relevant portions of the Economic Espionage Act invoke protection of trade secrets, a broadly defined class of intellectual property. Those sections, §§ 1831 and 1832, have been used to bring mercenary insiders into federal court, though, the first conviction under §1831 occurred in 2010, fourteen years after the Act was passed.\textsuperscript{28}

The two sections are both worded to protect against economic espionage. The first section is directed at people who give or sell trade secrets to foreign agents, governments, and companies; the latter focuses on the theft of the trade secret in general, either for foreign or interstate use.\textsuperscript{29} Both sections target the individual who appropriates the secret rather than the receiving party.

§1832 has been used with some regularity since its passing, though §1831 has only attained convictions in the past several years. The first conviction under §1831 was in *United States v. Chung*, in which the defendant was found to have appropriated trade secrets for the People’s Republic of China.\textsuperscript{30} Had he appropriated the trade secrets for a domestic entity, he might have been found in violation of §1832, like the defendant in *United States v. Martin*, a case involving a conspiracy to appropriate trade secrets from a veterinary laboratory.\textsuperscript{31}

The Economic Espionage Act can be a useful tool against insiders that threaten the intellectual property of their employers, making it useful for many businesses. However, analysis indicates that

\textsuperscript{26} 18 U.S.C. §792, 793.
\textsuperscript{27} *New York Times Co. v. United States*, 403 U.S. 713 (1971) in which the New York Times and Washington Post were charged with having violated the Espionage Act for publishing confidential information.
\textsuperscript{28} *United States v. Chung*, 659 F.3d 815 (2011).
\textsuperscript{29} 18 U.S.C. §§ 1831 & 1832(a), respectively.
\textsuperscript{30} *Chung* 631 F. 3d.
\textsuperscript{31} *United States v. Martin* 228 F. 3d 1 (1st Cir. 2000).
the EEA may not be used enough to serve as a deterrent for leaks. As of 2012, only 120 cases had been brought under the EEA, a number which has not increased drastically.

With industrial espionage such a large problem, the dearth of cases brought under the act seems to suggest that the law is not being used as an effective deterrent. The EEA may have the capacity to be used more effectively; it is likely not being used enough.

**The Computer Fraud and Abuse Act.** The Computer Fraud and Abuse Act and its included Information Infrastructure Protection Act have both been used to bring criminal actions against turncoat insiders. The Act penalizes unauthorized use or exceeding permitted use on a computer, and includes a civil penalty for infractions which incur at least $5,000 damage. It includes a specific measure making it illegal to obtain information harmful to the United States and willfully communicates it, and one for penalizing taking information from a protected computer. It has been used in several cases to prosecute insiders, including Manning.

However, recently in two Federal circuits, courts have ruled that “exceed authorized access” does not apply to employees who had legitimate access to information and made improper use of it. By limiting the definition, these courts remove teeth from the act, giving more legal leeway to insider’s under it. Depending on how these rulings are interpreted, this opens the door for an insider with legitimate access to information appropriating it without consequence under this statute. These decisions create a circuit split which will likely need to be settled through further adjudication or acts of Congress.

**Other Law.** Some states have their own laws aimed at protecting companies with secure information. Many states have their own versions of the Espionage Act or Economic Espionage

---


33 Ibid, since 2012, around 20 cases have been concluded or filed under the EEA. Some of those concluded were brought in years prior.

34 18 U.S.C. §1030(a),(g), the Act also penalizes hacking and damage to a computer or network.

35 18 U.S.C. §1030 (a)(1), (2)(c),(3). Protected computers include any computers used by the United States Government, a financial institution, or is used in interstate or foreign commerce or communication. 18 U.S.C. §1030(e)(2).


37 See *WEC Carolina Energy Solution, LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012), and *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012).
Act, however, few, if any, cases have been brought under those specifically geared towards criminally punishing non-economic espionage. Instead, companies tend to opt for the civil remedies available under Trade Secret laws, though more often they pursue the receiving party for damages rather than the leaking party.

Civil claims allow the employer an attempt at mitigating loss through the pursuit of contracts. These can offer disincentives both to malicious and non-malicious actors, as damaged parties can pursue both through civil charges. Contractual obligations can punish accidental and deliberate security breaches with employment actions and decisions. However, breach of contract cases that target individual leakers may have limited utility simply because the economic remedies available under them are often not enough to make the employer whole.

**Discussion.** There is an array of legal tools available that can target insiders. Whether through private breach of contract actions, state anti-espionage laws, or the federal statutes, there is no lack of deterrent options. If recent trends are any indicator, it is likely the federal government will be more willing than ever to use laws to pursue malicious insiders. However, the utility of these options may be questionable as they punish after the fact, in some cases do not appear to be used to their fullest efficacy, and can be ultimately not cost effective to use. While use of available laws has increased, the number of cases brought suggests the federal statutes are not being used as an effective deterrent.

Legal action is brought only after an insider has sold or given away secure information. Further, the insider has to be discovered, apprehended, and brought to court. This is a time consuming

---

38 New Mexico, Florida, and Pennsylvania to name a few. N.M. Stat. Ann. §20-12-42 (something of a curiosity in that it falls under New Mexico’s military law and includes a death penalty option); Fla. Stat. §688.002 (part of the state’s Uniform Trade Secrets Act which includes espionage as an improper means of obtaining trade secrets); 12 Pa.C.S. §5302, economic espionage). Other states like Illinois have expanded their definition of property to include what would fall under trade secrets or other intellectual property, allowing espionage to fall under their theft statutes. (720 ILCS 5/15-1, discussing the definition of property, and 720 ILCS 5/16-1(2), delineating that theft includes theft by deception).

39 Of the statutes surveyed here, relatively few cases wherein a company levied charges solely against an employee who leaked information were found carrying a conviction. This may be because it is more economically viable to go after the company the information was leaked to for remedies. For example, when Dura Global Technologies alleged that former employees took trade secrets to a new employer, it filed charges against the new employer, Magna Donnelly Corporation. *Dura Global Techs., Inc v. Magna Donnelly Corp.*, 662 F. Supp.2d 855 (E.D. Mich. 2009).

40 The cost of leaked information can easily outstrip an individual employee’s worth, making the cost of litigation too high in comparison to the expected reward, though a variety of reasons or factors can lead to a company not pursuing civil claims. See 2011 CERT Cyberwatch Survey, [http://resources.sei.cmu.edu/asset_files/Presentation/2011_017_001_54029.pdf](http://resources.sei.cmu.edu/asset_files/Presentation/2011_017_001_54029.pdf).

requirement made more difficult if the subject has left the country. Criminal sanctions are usually only useful against malicious actors, as the legal system will find non-malicious actors lack the necessary mens rea to charge the insider with a crime. While civil actions can be used against either malicious or non-malicious actors, they too are only available after data has been released, and insiders may lack the economic means to make them viable targets for suit. The law cannot fix unauthorized disclosure; it cannot truly make the entity whole from its loss. It can only offer monetary damages and punish those who release information, provided the insider can be brought into court. The international nature of many information disclosures complicates this picture as other nation’s governments have different norms and laws.

While the criminal and civil sanctions can be viewed as a dissuasive force for malicious actors, the sheer number of malicious insiders, the relatively small number of cases that are prosecuted under the federal acts listed above, and the faults that all legal remedies bear indicate that the deterrence is arguably not as effective as it could be.

Risk-Based Prevention and Mitigation

There is no golden key to eliminating the insider threat. There will never be a way to completely protect entities from within. However, a multifaceted approach that educates innocent actors, raises the bar for access, aligns entity and insider ethical standards, and technologically strengthens protections can help mitigate the damage from insider threats.

A “Better Wall.” The first and easiest method of mitigation is “building a better wall”; making sure potential threats never get close to valuable information or systems. This is based on the idea that the fewer people who have contact with sensitive information, the less likely that information will be leaked. Moreover, measures taken before the fact provide a process to make a risk-based decision to provide access, the appropriate level to grant, and prudent control measures to ensure compliance with organizational norms.

One way to build a better wall is to employ rigorous hiring and promotion processes. In depth background checks, security clearances, and polygraph tests are all tools for potential employers. These methods might help weed out those who have previously had incidents with law enforcement or who have exhibited questionable moral action. However, this solution is not

without criticism. Snowden went through rigorous background checks to obtain his security clearance, and any flags that were raised were either dismissed or addressed in an ultimately ineffective way.\textsuperscript{43} As with any process that attempts to predict future human behavior based on an aggregation of previous data, individual deviations will occur from time to time. Despite these occasional “failures,” such practices are widely used and cannot be ignored as a key part of an ongoing evaluative process.

Another strategy involves aggressive psychological profiling. There were signs in Snowden’s behavior that could have signaled the leadership of Booz Allen that an employee was making plans to betray their confidence. Again, this is a rearward facing defense, and would mostly be helpful for weeding out malicious actors. Designing the appropriate sort of tests can also be challenging.\textsuperscript{44} Such screening might include aggregation of information on an employee from different sources. Social media behavior and behavioral data could be combined with personnel data to create a robust profile of an employee. Such a method would come with privacy concerns and legal risks, as the legal arena for using and combining this data is still being settled. However, more psychological screening in the hiring process might help keep potential insider threats out of the workplace, and regular psychological screening might catch insiders as they are becoming threats.\textsuperscript{45}

The system of security clearances in present use provides a framework to achieve these goals. A means to strengthen the security of these measures is to require a more rigorous clearance process and require more frequent review and recertification of those to whom the organization grants access to the most sensitive information or allows broad access to resources and several categories of information. Frequent review also provides added incentives for better behavior. Employees feel more connected to a company that checks on them regularly, and may be more willing to open up and feel heard given more opportunities to express concerns. Conversely, regular checkups might also increase the sense of being watched, potentially deterring an employee from leaking information for fear of being caught.


\textsuperscript{44} \textit{Reflections on the Inside Threat}, Charles P. Pfleeger, the Pfleeger Group, 2007, \url{http://link.springer.com/chapter/10.1007%2F978-0-387-77322-3_2}.

\textsuperscript{45} Ibid.
A “Better City.” No matter how thick, tall, and broad a wall is built, it can always be breached. Given that insider threats will occur, and data will be lost, it is important to “build a better city.” The goal then is to make the “city” appealing enough to turn potential threats to your side, well designed enough to prevent innocent actors from falling prey, and complex enough to make the data harder to reach or monitored so as to make capture an almost certain outcome of adverse activity.

A very simple solution to mitigate the threat posed by non-malicious actors is to teach employees what is appropriate behavior on their computers and secure systems. This will help mitigate the threat posed by inattentive or complacent employee. Effective instruction can help reduce susceptibility to malware through phishing and sheer carelessness. It can also reduce the physical risk associated with leaving a workstation unlocked, or using the same storage medium on work and personal computers. Reminders for who is allowed in secure areas, and specific restrictions thereto can be exceptionally helpful in keeping those areas under close guard.

The task of training is complex and requires mastery of cognitive techniques that exceed the scope of this review. It is easy to see when more training is needed, but can be difficult to divine specifically what sort of training will be most effective. There are countless companies offering products to help with this task, but there is no universal solution. Likely, training would need to occur at all levels of an organization. Upper management needs to provide and resource good security, but the lowest intern with lax security standards can prove just as much of a threat as a C level executive. Regular, automatic updates to security software also help mitigate the threat posed by non-malicious insiders. While seemingly obvious, these are low cost measures that security professionals frequently identify as contributing factors during reviews of security incidents.

Frequent re-certification through the course of employment offers the opportunity to revalidate and reevaluate employees as well as adjust access to secure information as information changes. This could take the form of a periodic meeting or interview where employee and supervisor review the employee’s agreement with the organization to ensure the employee had a solid understanding of what the agreement entailed, and to give the employee a chance to discuss any potential infractions and apply corrective actions. Checks like these might make spotting potential threats easier, and could help mitigate both malicious and non-malicious insiders.

__________

46 CERT 4th common sense guide, Supra Note 45.
A mitigation strategy relevant to the Snowden case employs an open door policy in which employees have access to supervisors. Snowden tried to report his dissatisfaction and the issues he saw with policies to supervisors on multiple occasions, and expressed frustration with the people and processes involved.\textsuperscript{47} He did not feel heard, and did not believe the whistleblower protections available to government employees were available to him.\textsuperscript{48} The psychological effect of having an open venue for discourse is valuable, in that it can give an employee a way to voice their opinions in a safe space and be heard. However, it can also be a double edged sword, leaving employees feeling frustrated and stagnant if they feel their grievances are not addressed. It cannot be lip service; there have to be legitimate avenues of change, and discourse about why ideas or issues remain at status quo.

An open door strategy flows naturally into whistleblower provisions, Snowden felt he did not enjoy as robust a protection as he might have because of his status as a contract employee, the fact of which some consider to be legally ambiguous.\textsuperscript{49} However, even given the lack of legally mandated recourse, a company can adopt internal policies which would allow for clear guidance about such protection. An insider such as Snowden in an organization with an open, legitimate avenue to affect change will have greater incentives to follow established avenues to resolve grievances. This avenue also gives the organization another means of being aware of employee access to information and provides insights into intents and beliefs, allowing leaders to take more informed steps. Open, clear whistleblower protection is as useful for government contractors as for governmental employees.

Avenues for redress, as with all identified solutions, will not catch every insider threat within an organization. Redress measures may be nominally less attractive than other solutions because they can bring into question fundamental policy decisions and beliefs of an organization. If implemented, not every employee grievance need result in change of policy or program. However, there needs to be a forum for concerns to be brought up and legitimately discussed. The institution

\textsuperscript{47} Snowden’s testimony to the EU Parliament, \textit{Supra} note.3.
\textsuperscript{49} \textit{Edward Snowden’s Claim that He Had “No Proper Channels” for Protection as a Whistleblower}, Washington Post, March 12, 2014, \url{http://www.washingtonpost.com/blogs/fact-checker/wp/2014/03/12/edward-snowdens-claim-that-as-a-contractor-he-had-no-proper-channels-for-protection-as-a-whistleblower/}.
should be able to defend and articulate its positions to any of its employees, doing so helps foster a culture of accountability and trust.

In sum, screening and frequent reaffirmation of expected organizational behavior create cultures of accountability and trust. These measures can be combined with reviews that give employers and employees the opportunity to review commitments and resolve differences between organizational and individual goals. These procedures provide a framework to align organization and individual goals in voluntary employment relationships.

**Compensation-Based Incentives and Disincentives**

Compensation structures can provide opportunities for both incentive and deterrence. At a minimum, organizations must review compensation to ensure it attracts required talent and presents the fewest opportunities for the development of monetary motives. However, compensation has limits that extend only to the periods in which it is offered. Likewise, incentives must be valued by employees. For example, we found instances in which firms offered competitions that awarded employees prizes and recognition for identifying improvements to security procedures or capabilities. The incentive quickly became the competition itself, and proved to be effective.\(^5\)

Another form of economic incentive ties a portion of compensation to compliance with security performance. Instead of offering bonuses to buy loyalty, leadership ties compensation to satisfactory security performance. One approach provides an employee her basic salary level, part of which is deferred until the employee’s performance can be reviewed. If the review is favorable, the remaining compensation is released to the employee. Promotions tied to performance reviews align individual behavior with desired organizational outcomes. Organizations can structure compensation with a significant portion deferred until after the employee departs the organization. Included in the employment agreement would be a provision that the deferred compensation would become available at a time after departure, sufficiently long that any information removed would be of no value, to ensure little or damage would come from a leak at that point. These compensation schemes are similar to the deferred arrangements found in the corporate world that tie compensation to long term firm performance. Just like in those schemes, here a portion of compensation is connected to the organization’s goal to make its information secure.

\(^5\) Comments by Royht Belani, Mircon 2013, APT Mitigation, the Human Way, Nov. 6, 2013.
Compensation approaches carry a downside, however, in that there is an incentive for the employee to suppress reports of unfavorable performance so that they do not lose compensation. Any such approaches must have clearly defined performance standards to limit the potential for disputes. Most valuable are those approaches that encourage individual employees to internalize the culture of security and accountability in their organization.

Compensation schemes invite compliance only during the time such schemes are available. More powerful are approaches that instill values aligned with those of the organization. A good example of a values based approach is the US Navy nuclear power program, which requires high quality and rigorous certification to join. The program offers non-monetary compensation to its members by offering membership to its respected and prestigious reputation. Personnel can lose certification through poor performance or misconduct. These attributes provide a strong draw to quality personnel and create incentives to perform well so membership in an elite community can continue.

Peer Monitoring and Multiple Party Monitoring

Still another strategy to build a better city is to link surveillance and monitoring to levels of access and authority. Organizations would employ such a strategy with high level insiders or those with unusually broad access to sensitive information. Snowden was able to access and move information in large part because he had unsupervised access to it. He was unobserved and trusted, and leveraged that trust to harm his institution.

The Personnel Reliability Program utilized by the United States military to control access to nuclear missiles provides another potential model for consideration. Nuclear devices required several steps to enable use. Key steps in this process had to be reviewed and authorized by two cleared and trained specialists who must validate the authorization to take steps. Where appropriate, an organization’s data structures would benefit from the same protection. An organization might consider a strategy whereby system administrators travel and work in pairs. One partner would monitor the actions of the teammate, and access to certain categories of


sensitivity or breadth would require positive authorization from leadership. This is an expensive solution, and likely would only be applied to those systems with the highest level of security. The program offers benefits beyond surveillance, as experience suggests the psychological effect of working in a team acts as a means of mitigating insider threat. Rotation of teams and periodic activity reviews would strengthen the monitoring of sensitive functions.

“Smarter Data.” The data structure itself can be part of making the city better. Making the data more easily traceable, and granting stronger accountability to those with access to it, makes any unauthorized movement of the data far easier to track.

Sensitive files and items which maintain metadata beyond standard elements of identification provide another means of security. Although it would be infeasible to protect all of an entity’s data through this means, the most sensitive material could be programmed to record whoever opens, sends, or copies it. With a date and time stamp of alert whenever the file is moved or copied, the data itself then becomes part of the protection system. As with other measures, periodic review of access logs generated by this highly sensitive data adds to security.

At a minimum, technological measures afford an ability to limit the volume and sensitivity of data compromised. As with any technology, there will be attempts to break or circumvent measures, so procedures and capabilities will need constant revision. However, if such a system had been in place on the data Snowden collected, there would be a more accurate picture of how and when he captured the data. Further, if the data alerted the system whenever it was changed or repositioned, Booz Allen would have had a much better chance at catching Snowden’s behavior before his actions caused significant damage.

Such technology comes with additional costs. The addition of information to a file by its nature increases the amount of computing resources necessary to interact with it. Therefore it would be useful to apply enhanced technology to only the most sensitive data, or to insiders with the most sensitive or broadest levels of access. An advanced metadata system would also play into the incentive structure of the “better city,” as it presents another avenue through which malicious actors would face detection. Employees aware of the existence of such a system but unaware of its specific application would face an additional deterrent to unauthorized use.

53 CERT offers this as one of its basic strategies for mitigating threat. [http://www.cert.org/blogs/insider-threat/post.cfm?EntryID=135](http://www.cert.org/blogs/insider-threat/post.cfm?EntryID=135)
Conclusion

Edward Snowden woke the world to what an intelligent and motivated person can do with the right access, but his type is far from the only insider threat we need to be aware of. Monetarily motivated and careless employees can cause leaks or provide opportunity for data to be sold just as easily as a single actor acting with ideological motives. The regulatory and legal schemes help mitigate damage by presenting disincentives to malicious and non-malicious actors both, but cannot rewind time to prevent loss. Threat mitigation is important, as is the recognition that individuals within an organization could act from motives that depart from expectations of the organization. Narrowing their abilities to access secure information, providing a culture and systems that invite compliance and having in place monitoring and tracking systems that tie incentives and disincentives to accountability for access to sensitive information and broad categories of information. Organizations must realize that granting access is a decision that carries risk and must employ a range of measures that address various categories of insider threat. They must monitor and revise these procedures to ensure that they account for technological, organizational, and workforce changes over time.
2.0 PERSONNEL BEHAVIOR PHYSICAL AND VIRTUAL: THE WHOLE PERSON INSIDER THREAT ANALYSIS PARADIGM

Authored by: Alan A. Andrews, DCSW, Maryjane Poulin, Matthew Sweeney

I. Executive Summary

Many previous studies have been performed as to the motivations and causes of insider threat activities. While personal traits, psychological conditions, and various other contributing factors have been explored, there is a gap between understanding the traits of a person related to personal trust (such as prescribed by the ONDI ICD 704.2 guidelines) and cyber behaviors as observed in enterprise environments. In this section we will present a method of whole person analysis for insider threat that addresses the relationships between personal traits and cyber behaviors along with methods of restricting cyber behavior where trust has already been granted. Our goal is to illustrate for the reader how to combine personnel and cyber security in a meaningful way based on observations of personnel behavior.

Addressing the Whole Person in Security Risk Assessment

Accurately assessing and predicting security risk is a challenging prospect in a technologically diverse world. Security indicators have historically included a variety of personal and interpersonal interests that, although they offer a broad perspective of security risk, fail to include cyber or online behaviors, a current and growing source of security risk indicators. The analysis of cyber behaviors as additional security indicators is an available but untapped resource with great potential. Other recent research has focused on the effects of Adverse Online Behaviors (AOB), especially as indicators of mental illness or mental health issues. Our primary research focus was the discovery of relationships between offline (physical) and adverse online behavior where strong, non-trivial associations were discovered. Building on our research, literature review, and expertise we created a tool to assess security risk, the Critical Cyber Behavior Assessment (CCBA). The CCBA was designed to determine a pattern or constellation of behaviors that indicate increased security risk, and could be useful for many types of pre-employment screening including but not limited to security clearance background investigations.

Anticipating the “human factor” has long been understood to be one of the most important aspects of protecting the security infrastructure. “Humans are often an organization’s weakest link for many aspects of security, from forgetting to lock doors to choosing a weak password to acting in counterintuitive or unanticipated ways” (Wyborne, et. al., 2009, 25). One of the recommendations presented by the Institute for Information Infrastructure Protection (2009) was to develop a
security protocol that takes into account human behavior, decision-making and the characteristics of the “bad actor” (2009, 29). Taking this a step further, Department of Defense agencies often require some level of security clearance and there has been greatly increased interest on aspects of AOB in relation to that process. This report is based in part on research performed for a government agency. In keeping with these concerns in the security realm, one of our goals was to develop a portrait of the “bad actor” using a constellation of behaviors that indicate poor decision-making skills and increased security risk.

**The Cyber Insider Threat Problem**

Due to the rampant growth and recognition of the insider threat problem as technology has advanced, there are a multitude of recent reports published (Capelli, et al., 2009 (Cappelli, Moore, Trzeciak, & Shimeall, 2009); Capelli, et al., 2008 (Cappelli, Caron, Trzeciak, & Moore, 2008), Hanley, et al., 2009 (Hanley, Moore, Cappelli, & Trzeciak, 2009); Spooner, et al., 2009 (Spooner, Cappelli, Moore, & Trzeciak, 2009); U.S. Secret Service & CERT, 2008 (United States Secret Service, & CERT / Software Engineering Institute, 2008); Weiland, et al., 2010 (Weiland, Moore, Cappelli, Trzeciak, & Spooner, 2010)) which note the types of missions and adversaries involved in insider threat. Included are espionage against the U.S., IT sabotage, embezzlement, and theft of various tangible or intangible items (e.g., intellectual property [IP], classified or sensitive information, or technology).

Increasingly insider activities are represented by malware that has gained access to the network. Numerous articles including those by Zetter (2011) (Zetter, 2011) and Keizer (2010) (Keizer, 2010) have chronicled the advent of Stuxnet and its impact on Iran’s nuclear weapons ambitions (Barnes, 2010) (Barnes, 2010). Closer to home, Sternstein (2011) (Sternstein, 2011) reported that a recent federal audit found Department of Homeland Security’ financial systems to be vulnerable to insider abuse including a social engineering attack that allowed malicious software to gain access and steal data from a contractor’s network.

Typically requiring manual review of multiple computer security data feeds, malicious insider activity is difficult to detect. The challenge of insider threat detection lies in the disparate information that must be managed in order to correctly determine the occurrence of insider threat activity. In order to effectively triangulate information related to insider threat missions, it is important to address the risk related to online and offline behaviors so as to mitigate circumstances that can present organization members an opportunity or motive to become insider threats, including “accidental” insider threat resulting from compulsive Internet activities while on the job.
Adverse Online Behavior

Adverse Online Behavior (AOB) is defined as activity which occurs in an electronically mediated format (e.g., the Internet), may involve one person’s interactions with online media or the interaction with other people participating in the electronically mediated behavior, and the behavior is either counterproductive, shows lack of judgment, or is directly harmful to those involved. In order to assess the meaning and categories of individual online behavior, we created an Adverse Online Behavior (AOB) taxonomy.

We compiled a library of research articles categorizing the prevalence of issues regarding online activities, examining each study for indications of not only what online behaviors were being catalogued, but also how those behaviors were determined to exist and the influence they had on the subjects and their social network. Based on our findings in the research we created an Adverse Online Behavior (AOB) taxonomy. As we explored the occurrence of adverse online behavior and the affect it has on individuals and the groups in which they participate, we determined that there is a significant psychological component to adverse online behavior that needed to be addressed. Therefore, we determined that some of our efforts needed to focus on the analysis of these behaviors from a mental health perspective in addition to a statistical perspective.

Assumptions

Answering the key research questions proposed in this effort involved making certain assumptions about the data being used, how to organize and categorize it, and how to assess the value of associations and patterns found in the data. The data collected for use in this study is constructed from personnel security case files from over an 8 year period with over 50,000 subjects and slightly more than 30,000 cases containing indicators as recorded by personnel security staff in their system of record. The information entered in the system of record is a summary of information collected during the adjudication process. One significant assumption we make is that if an adjudicator saw fit to report information on adjudicative criteria behavior for a case, then that information is relevant to personnel security risk. We place no judgment on the entries presented in the personnel security case data (hereafter referred to as cases). This case information is corroborated by at least two adjudicators, but their decision is also subject to organizational need. Our case data does not give us insight into all of those decisions, so we accept at face value and analyze behavior correlations in that light.

Each of the adjudicative indicators recorded in the system of record is referred to as “offline behavior” in this report. Offline behavior refers to the adjudicative criteria in the DCID 6/4
guidelines, which was the standard for adjudication used in collecting the data we used for this study. Any observations of offline behavior correspond to an instance of an adjudicative indicator being present in a personnel security case. This brings us to the meanings of “case” and “behavior.” A “case” is defined as all of the recorded adjudicative indicators, descriptions and associated adjudicative workflow information associated with one person’s criteria during the clearance vetting process. Each case corresponds to one person who was processed for gaining access to a security clearance and any subsequent re-investigations they may have undergone. “Behavior” refers to individual instances of offline or online behavior as observed in each case.

As we defined our taxonomy of adverse online behavior, we initially attempted to make various distinctions about online behaviors based on them occurring “at work” vs. “not at work,” but there is not enough information in our dataset to draw those conclusions in many cases, and it required intensive manual review. Additionally, we found that particular behaviors, regardless of physical location, were being recorded in support of broader personal conduct issues. Therefore, we concluded that it would not be possible to make such a distinction in our study.

**Research Methodology**

As stated previously, insight into human behavior is a key to understanding and predicting security risk indicators. For personnel working in national security positions, disparities between online and offline personas must be considered to ensure accurate security clearance adjudication decisions. Aspects of mental disorder traits and dysfunctional behaviors are routinely used as security risk indicators in security reviews and evaluations. The Director of Central Intelligence Directive (DCID) 6/4 *Personnel Security Standards* (1998) lists reportable personnel security risk behaviors that include:

- Sexual behavior that is criminal or shows lack of judgment
- Apparent mental or emotional disorder
- Alcohol abuse

---

54 The ICD 704.2 guidelines ([http://www.fas.org/irp/dni/icd/icpg704-2.pdf](http://www.fas.org/irp/dni/icd/icpg704-2.pdf)) are different in subtle ways but have not been revised since 2008 and do not contain any material to specifically address adverse online behavior.

55 DCID 6/4 has been replaced by Intelligence Community Policy Guidance 704.2 - Personnel Security Adjudicative Guidelines for Determining Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information, October 2, 2008. However we used the superseded DCID 6/4 because that was the current standard when information in our data set was collected.
• Criminal conduct
• Misuse of information technology systems

These security indicators point to a psychological component that connects decision-making and risk behaviors. Being diagnosed with a mental disorder, in and of itself, is not a sufficient indicator of risk; rather, a pattern or constellation of behaviors indicates higher risk. A constellation of behaviors and traits can include:

• Failure to follow medical advice for treatment
• Pattern of unpredictable behavior
• Pattern of anti-social behavior
• Pattern of aggressive or hostile behavior
• Pattern of irresponsible behavior
• Sexually inappropriate behavior

Adverse Online Behavior is defined as activity which occurs in an electronically mediated format (e.g., the Internet), may involve one person’s interactions with online media or the interaction with other people participating in the electronically mediated behavior, and the behavior is either counterproductive, shows lack of judgment, or is directly harmful to those involved. Offline behavior was defined as outlined within Director of Central Intelligence Directive 6/4 (DCID 6/4), Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information. For this study, Adverse Online Behaviors may have been indirectly discovered and reported during the security clearance application process via multiple possible sources, including the SF86 - Questionnaire for National Security Positions (U.S. Office of Personnel Management, 2008) national or local agency checks, personal interviews during background investigation reports, or polygraph interviews. For a reference to many of the issues addressed during the security clearance process, see the Security Clearance FAQ (Dice, Inc., 2009).

As part of our research study of AOB, we have acquired and refined a highly structured corpus of historical security clearance cases of personnel working in or seeking national security positions. To conduct this research in support of security clearance reform, we were authorized to leverage this corpus of over fifty thousand individual cases spanning the years 2000 to mid-2008. Of these, over thirty-three thousand included a full accounting of adjudicative history from initial application through reinvestigation; all relevant facts from data sources including SF86, Single
Scope Background Investigation, polygraph report, etc.; a structured breakdown of relevant risk indicators and security concerns based on the DCID 6-4 personnel adjudication guidelines; a record of the final adjudicative outcome and justification. When reading the following behavior observations, readers should keep in mind the data collection processes outlined above. No comprehensive questionnaire existed (nor is one currently in use) to ensure coverage of Adverse Online Behaviors. Therefore, lack of cases containing a particular AOB cannot be reliably interpreted to mean that the behavior did not exist or exist in greater numbers within a population. Conversely, one may conclude that reported AOB were associated with some offline behavior (adjudicative criteria) because there were no direct questions in the SF-86 (1995, 2010) which would have drawn them out. The questions in the current revision of the SF-86 (2010) regarding use of information technology systems only attempt to uncover information regarding potential hacking activities and do little to address the broader need for information such as a subject’s habits using the Internet, disregard or flexibility with regard to copyright and electronic content ownership laws, and means of communication that the subject engages in on a continuous basis, including regarding the type of groups that they associate with in virtual circles. As such, the following sections are intended as a guide for pre-employment decisions involving online behavior, illustrating where correlations existed with offline behavior as well as possible gaps in the (personnel security) data collection process.

As illustrated in Figures 1 below, we applied a research method that included five phases in order to discover adverse online behavior correlations, determine if offline behavior could have a meaningful association with online behavior, and assess the significance of the adverse online behavior to personnel security risk.
RiskTracer™, a decision support platform for personnel security risk assessment, was applied to develop correlation models and analyze their effectiveness in the context of behavior prediction.

We compiled a library of research articles categorizing the prevalence of issues regarding online activities, examining each study for indications of not only what online behaviors were being catalogued, but also how those behaviors were determined to exist and the influence they had on the subjects and their social network. Based on our findings in the research, we created an AOB taxonomy. See the Appendix for the AOB Taxonomy outline. By assigning categories from this taxonomy to instances of behavior in 33,000 personnel security cases, we are able to identify 2831 cases containing adverse online behavior spanning the 8 year period. Next, we performed a statistical analysis characterizing the frequency of each AOB in the case set compared to the type of clearance (TS/SCI or Secret), whether the case was approved or denied, and whether there were any psychological issues in the case.

**Analytical Results**
Our research shows that there are trends over the time period of analysis (as in Figure 2) there is a definitive increase in the presence of AOB in personnel security cases. Further, there is an indication that the areas of concern led to a requirement for more in-depth investigations and analysis based on the combination of offline and online behaviors that are present in the data, along with the additional steps in adjudicative process (background checks, psychological assessments, etc.) that occurred for these cases.

**Figure 2. Percentage of AOB cases proportional to overall case load**
Figure 3. Detailed look at percentage of AOB cases proportional to overall case load for the top 3 criteria.

Figure 4. Detailed look at percentage of AOB cases proportional to overall case load for lower prevalence concerns.
Applying association rule learning to analyze correlations between AOB and adjudicative indicators of risk, we discovered many associations at a general and detailed level that were too numerous to list completely. Table 1 provides summary results at a broad level. The most interesting correlations are those non-obvious ones where the offline behavior would not necessarily directly be linked to the online behavior, such as is the case between criminal conduct and initiating sexually oriented messages.

**Table 1. Interesting Higher Risk Offline / AOB Pairs**

<table>
<thead>
<tr>
<th>Offline Behavior</th>
<th>Adverse Online Behavior</th>
<th>Change in Personnel Security Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allegiance to the United States</td>
<td>Counterproductive Misuse of IT Systems</td>
<td>High</td>
</tr>
<tr>
<td>Criminal Conduct</td>
<td>Corrupting / Destroying / Encrypting / Manipulating / Transferring Cyber Assets / Data</td>
<td>Medium-High</td>
</tr>
<tr>
<td>Criminal Conduct</td>
<td>Initiating Sexually Oriented Messages</td>
<td>Medium-High</td>
</tr>
<tr>
<td>Criminal Conduct</td>
<td>Introducing Malware</td>
<td>Medium-High</td>
</tr>
<tr>
<td>Emotional, Mental, Personality Disorders</td>
<td>Playing Games / Social Networking / Virtual Role Playing</td>
<td>High</td>
</tr>
<tr>
<td>Emotional, Mental, Personality Disorders</td>
<td>Sending Defamatory Statements / Harassment</td>
<td>High</td>
</tr>
<tr>
<td>Misuse of Information Technology Systems</td>
<td>Counterproductive Misuse of IT Systems</td>
<td>Medium-High</td>
</tr>
<tr>
<td>Misuse of Information Technology Systems</td>
<td>Playing Games / Social Networking / Virtual Role Playing</td>
<td>Medium-High</td>
</tr>
<tr>
<td>Other Security Factors</td>
<td>Blogging / Chatting / Emailing</td>
<td>Medium-High</td>
</tr>
<tr>
<td>Other Security Factors</td>
<td>Contacting Unauthorized People</td>
<td>Medium-High</td>
</tr>
<tr>
<td>Other Security Factors</td>
<td>Counterproductive Misuse of IT Systems</td>
<td>Medium-High</td>
</tr>
<tr>
<td>Other Security Factors</td>
<td>Hacking into Another Computer/System/Website</td>
<td>High</td>
</tr>
<tr>
<td>Other Security Factors</td>
<td>Playing Games / Social Networking / Virtual Role Playing</td>
<td>High</td>
</tr>
<tr>
<td>Other Security Factors</td>
<td>Security Concerns</td>
<td>Medium-High</td>
</tr>
<tr>
<td>Outside Activities</td>
<td>Contacting Unauthorized People</td>
<td>High</td>
</tr>
<tr>
<td>Outside Activities</td>
<td>Other Serious Misuse of IT Systems</td>
<td>High</td>
</tr>
<tr>
<td>Offline Behavior</td>
<td>Adverse Online Behavior</td>
<td>Change in Personnel Security Risk</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------------------------------------------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Personal Conduct</td>
<td>Browsing / Buying / Selling Online</td>
<td>High</td>
</tr>
<tr>
<td>Personal Conduct</td>
<td>Distributing / Possessing Pirated Digital Materials</td>
<td>Medium-High</td>
</tr>
<tr>
<td>Security Violations</td>
<td>Corrupting / Destroying / Encrypting / Manipulating / Transferring Cyber Assets / Data</td>
<td>High</td>
</tr>
<tr>
<td>Security Violations</td>
<td>Counterproductive Misuse of IT Systems</td>
<td>Medium-High</td>
</tr>
<tr>
<td>Security Violations</td>
<td>Hacking into Another Computer/System/Website</td>
<td>Medium-High</td>
</tr>
<tr>
<td>Security Violations</td>
<td>Playing Games / Social Networking / Virtual Role Playing</td>
<td>Medium-High</td>
</tr>
<tr>
<td>Security Violations</td>
<td>Playing Games / Social Networking / Virtual Role Playing</td>
<td>Medium-High</td>
</tr>
<tr>
<td>Security Violations</td>
<td>Security Concerns</td>
<td>Medium-High</td>
</tr>
<tr>
<td>Sexual Behavior</td>
<td>Accessing / Downloading / Transmitting Pornographic Materials</td>
<td>High</td>
</tr>
</tbody>
</table>

**Conclusions Regarding Online Behavior**

As we explored the occurrence of Adverse Online Behavior and the affect it has on individuals and the groups in which they participate, we determined that there is a significant psychological component to AOB that needed to be addressed. Information being collected during the personnel security clearance process was not adequate for determining all of the online behaviors that contributed to the risk associated with a case. In particular, it was not directly tied to concrete behaviors indicating psychological characterizations that we hypothesize are related to security risk. Therefore, we determined that some of our efforts needed to focus on the analysis of these behaviors from a mental health perspective in addition to a statistical perspective.

Recent literature supports the premise that dysfunctional internet use is correlated to certain characteristics of mental disorders as defined in the DSM IV (American Psychiatric Association, 2000). Since the late 1990’s, a growing body of research has focused on negative internet behaviors as related to social and mental health problems. Literature has emerged that depicts pathological internet use utilizing an addictions model. The rising concern is that problematic internet use is related to poor decision-making skills and often interferes with necessary life activities, successful relationships, successful employment and accountability.
Counter to popular thought, internet addiction is not merely an excessive amount of time spent on the internet. Internet addiction encompasses behaviors that lead to loss of work time, sleep deprivation, decay of interpersonal relationships, depression, economic decline, etc. In other words, what you do while online is a more accurate indicator of pathology than the number of hours spent on the internet (Brenner, 1997). Kimberly Young, PhD defined internet addiction based on the Diagnostic and Statistical Manual of Mental Disorders (DSM-IV) criteria for gambling addiction.

Symptoms can include lying behavior about online activity, feelings of restlessness and irritability when cutting back on internet use, a preoccupation with the internet and using the internet to overcome mood disorder symptoms, i.e., depression (Young, 2004). Other research regarding pathological internet use compares dysfunctional Internet use to impulse disorder criteria (Aboujaoude et. al., 2006).

As with impulse control disorders, internet use can lead to short-term relief of anxiety or depression symptoms. Also similar to impulse control disorders, the long-term repercussions for impulsive or obsessive behaviors can be devastating. As noted previously, consequences range from lack of sleep and interpersonal relationship problems to loss of employment, economic struggles, legal issues, depression and anxiety. Of particular note is that Aboujaoude, et.al. (2006) found that the prevalence of problematic internet use was the same for males and females in the adult population sampled.
It has been established that mental health disorder traits can be expressed through cyber behaviors, particularly internet addiction behaviors, obsessive behaviors and expression of depression and dependency traits. Mental health disorder traits are also related to elevated security risk indicators, as exemplified in DCID 6/4 Personnel Security Standards (1998) and the PERSEREC Technical Report (Kramer, et al, 2005). As illustrated in Figure 4, the common link between adverse online behaviors and mental disorder traits is security risk assessment.

A tool using aspects of cyber behavior to capture elements of security risk in employees or potential employees would be a very valuable addition to the array of security screening tools now available to companies and agencies concerned with infrastructure security. Such a tool links cyber behaviors with personality and mood disorder traits to create an easily administered questionnaire that provides additional risk assessment information.

**Summary**

As a result of our analysis of AOB in a population of subjects undergoing security clearance adjudication, we can safely surmise that there is an increase in online behaviors over time relative to the size of the population desiring to obtain a clearance. Given that those who attempt to receive a government security clearance must be amenable to a rigorous process that can involve discussions with background investigators, adjudicators, and psychologists, we postulate that the population at large likely has an equal or higher percentage of individuals with these issues that may not be discovered during typical interview and personal background checks performed by organizations.

The proportion of cases involving psychological evaluation is also worthy of note, with 38% of all cases classified as containing AOB being referred in such a way. This appears to indicate that the psychological complications of online activity are real and growing as the prevalence of AOB issues increases. Employers should take seriously the need to provide resources such as mental health counseling, programs to curb Internet addictions, and incorporating initial and periodic analysis of employee virtual behavior, even at a surface level, through discussions with current and potential employees. These efforts, when coupled with well thought-out and communicated electronic monitoring programs, can help to counteract an employee’s sense that virtual behaviors can easily go unnoticed.

As in many insider threat cases, including Ames and Hanssen, critical information regarding employee attitude, performance, and critical life events are not reported immediately or tracked
and recorded in any electronic configuration management system that allows human resource professionals the opportunity to address employees.
3.0 PANEL QUESTIONS & ANSWERS TRANSCRIPT


Moderator:
- Michael Weir, Quanterion Solutions Incorporated

Panelists:
- Thomas “TJ” Vestal, AFRL/Rome
- Bruce Gabrielson, CACI
- Matthew Sweeney, SRC, Inc.
- Randy Trzeciak, Director CMU Insider Threat Group
- James Henderson, Cyber Security-Information Assurance Program Management/Counter-espionage Training Course Instructor

Michael Weir: I’d like to introduce our panel. Dr. Gabrielson you’ve met before and I’m reintroducing him again.

We have also Jim Henderson with us. Jim Henderson is the President of Counterespionage US and has over 15 years of experience in information technology departments, information system security programs and the DOD insider threat defense program. He specializes in integration of counter-espionage and insider threat concepts and provides the counterespionage insider threat defense program training course to Government and other personnel.

Matt Sweeney works with SRC in Syracuse, he is a Program Manager and Lead Engineer in information analytics, and he recently completed an analysis report that he’ll be talking about some of the content of that later on this afternoon in his presentation, and that will be on the whole person insider threat analysis paradigm.

And then Randy Trzeciak, who you’ve also met earlier, with Carnegie Mellon in the Software Engineering Institute in the CERT.

And then lastly, Tom “TJ” Vestal with the Air Force Research Lab, here in Rome, focusing on cyber security and mission assurance. In addition to focusing on some of the policy-based frameworks and some of the other work that he’s done, I need to point out he is also a very strong proponent of event cyber security education. He is involved in quite a few of those initiatives that get younger folks up to a working condition where they can help out in the cyber security community, which is a hard problem and it’s good to have folks focusing in on that. That’s a very good thing.
So what we’ve got is a set of questions, the objective for this panel is to step through and have each one make some sort of a discussion comment on the flavor of the question, maybe not specifically the question, because I know they are opinions and those are, those are great things in a forum like this, is to take the question and move a little bit beyond it. So what I’d like to do is to go through six or eight questions, depending on how the time goes out, and we’ll try to make our lunchtime, which is about one hour from now, but we can take whatever time makes sense and then have lunch and participate in some side discussions.

We’re going to delay some discussion of metrics until we have an opportunity, towards the end of the day, to talk in great detail about that, but it’s certainly a fair topic, a lot of folks are using it. The general topic is to focus on good guys and bad guys and the insider threat and what are trends, what or what direction are we headed, what makes the most sense? So I’ve got a set of questions here, I’ll go ahead and ask the questions and we can step through and have Bruce and then Jim, Matt, Randy and TJ just a quick summarized perspective on the question. Take it a little bit different direction and then please, if we have some discussion for the audience that certainly is welcome.

So, here we go, in terms of the growth over the last 10 years in publicly available tools for assessing or prosecuting network level vulnerabilities, that is network-based security, there’s exemplars like tools such as backtrack and things that are tool sets that are germane to the network security domain. Now the insider threat doesn’t appear to be quite so similar, there doesn’t exist a particular bespoke toolkit and what, what would you folks think, as panelists, about the likelihood of a toolkit being a valid thing for the insider threat, is it, is it a nonstarter because you don’t have those crosscutting tools, is, is the insider threat too varied, what do you think about the toolsets that might be used in insider threat?

**Bruce Gabrielson:** Ok the tools sets that might be used, there are a lot of tools out there, and it’s interesting at least in the academic environment, a lot of people say, “oh yea, I’ve got an idea for some new way of hacking in,” and as Artie pointed out, that it’s not always somebody hacking in and impersonating, it’s actually an insider. If you’re going to look at toolsets, especially in a cloud environment or anything else, you’re talking about being able to look at massive amounts of things in a very short amount of time. I really think at the network level, we’re going to start looking more towards not, not analyzing those massive amounts of data and look more towards what is an individual doing, and focusing down more at a host level or a boundary of that host or that particular enclave rather than looking just at a network boundary on a large-scale.
James Henderson: Thank you, Bruce. My belief on the tools are, the tools are, they’re out there, there are different tools out there, Raytheon, Verdasys, but sometimes the tools that we discussed earlier won’t catch the stuff because the activity, there is no profile, just the person just decides that particular day they’re going to go bad. So a lot of it to me, just starts with basic principles of I.A. and, and the people should know what they should, shouldn’t do, looking existing tools in the network, what they have, content filters for email, web sense, some of the just different tools out there and using what you have. Organizations that I’ve worked with when I’ve gone around and I’ve asked to talk to them about insider threat and I asked them what tools they have, do you have a content filter, do you have a sim tool, do you have this, do you review your Windows event logs? I get those blank stares in the face so to me a lot of it starts with looking at the existing tools you have and the data feeds and then moving from there.

Matthew Sweeney: I think a lot of the, from a toolset standpoint, I would agree, there are some commercial tools but there is a lot of disparity because there are research tools that have certain capabilities that will make their way, I like the comment about HPSS as a framework and there is a need for it, that sort of thing, I think to help researchers and other commercial entities plug in capabilities. But I think there’s, I guess a need for a basis of understanding and meaning, as far as what is going on within an organization or to build some of those tools and have them work across the organization as well, and I don’t think that necessarily exists in a lot of organizations. So protecting data is a part of that policy, Insider Threat Program, being able to understand, you know, I, I can combine information about my personal security risks with, you know, security information events, other kinds of activities, there’s not a holistic treatment of that from a toolset standpoint yet.

Randy Trzeciak: OK, my comment might be slightly different. Certainly recognizing the number of tools that are out there that could prevent certain activity or detect certain activity. Traditionally, organizations have stood up the security controls that will protect the perimeter. Would certainly protect folks from the outside getting in or someone from the outside doing something to us inside the organization. But there seems to be a cultural reluctance to apply tools and technologies that’s really protecting us from ourselves, in terms of, I’m deploying a tool that’s looking for suspicious activity on employees that are trusted within the organization. With recent events and the high-profile incidents that have come out, we’ve seen a number of organizations that are starting to look internally, applying the tools they traditionally have deployed at the perimeter to protect outside from coming in to actually start looking for inside going out or inside going across different boundaries and enclaves within the organization.
So in terms of at least the history of the 13+ years of insider threat research we’ve done, there tends to be that cultural reluctance to, you know, really distrust employees where we’ve vetted them coming in. We’re trying to deploy ways to protect data and at least historically, hasn’t been protected from us, in terms of that protection strategy so… but going on to the comments that were made before, there are certainly tools and technologies. The goal of an organization should be to identify what is different from what’s normal activity and the sooner the core mantra of the security program should be the acceptable level of inconvenience but not getting in the way of whatever your business objectives are. And that’s really struggles most IT departments have just with the organization as a whole. How can we secure something but not necessarily get in the way?

**Michael Weir:** Any, any primary discussion points? Cool. Did you, did you want a microphone, okay.

**Audience Member:** (Missed Vocals…) they will try to damage. And this is a good example which you gave, and this is what I was describing in case of power that it could be very similar thing that may have happen as well. So I think we shouldn’t lose this aspect of the insider threat because many of the techniques and many, several of the techniques in which we used to detect attacks coming from outside could apply in this context as well, because the insider has to do something in this system and we can observe to see, we can monitor this, we can, we can perhaps flag it before the damage happened to the system.

**Michael Weir:** Thank you very kindly. Let me, get to the next question, and then we’ll need to go through the panel, together, thank you. Alright, the next question is has to do with approaches to finding out what the bad guys doing, there’s a, there’s a couple of standard approaches in the, in the repertoire and they’re kind of, kind of two camps, you either have a signature-based, a very statistically oriented approach and you have anomaly-based kinds of things and in the typical network security computed community there are exemplar statements such as a signature-based tool will find exactly what it’s supposed to, high probability, really good tool, an anomaly or behavior loosely termed-based tool will probably find things the signature-based tool won’t, but the false alarm rate gets crazy after a while. So the question is, for the insider threat, which seems to be an interesting combination of trying to do technical things and behavioral things, is, is there something more natural about the insider threat analysis that would lead you to believe there’s not quite this chasm between signature versus anomaly, or is it kind of the same thing over again and we still have to fight that battle with false alarms?
Bruce Gabrielson: OK, remember, my background is more the I.A. side than the intelligence side, but a signature, let’s talk about what a signature is, are we talking about a profile that’s been developed that will detect bad behavior or are we talking about something like a virus that is a signature that you could look for real easily. You know a profile is hard to develop but once you get it, it is very useful and you can analyze it and you can compare it against somebody else’s profile. So, to me, I would call that a signature-based approach but it’s really looking for anomalies over and above what the normal activity is, so I don’t know, do we call that a signature base or anomaly base? OK? I would call that looking for anomalies that are different than what the signature should be.

James Henderson: Thank you, Bruce. I agree there are a lot of different tools out there, as I said a minute ago, but I agree with some of what Bruce said that it’s almost like a signature-based stuff will catch stuff that’s been seen but what you do about the insider that’s like a zero day vulnerability. He comes up with a new concept and he’s not doing anything that’s really way off the mark, it’s just enough to ex-filtrate the data, using a WebCam or something. You know people might say that there is no WebCam software, well, you can go to any meeting.com, I just sometimes look at it from a higher level. What’s the base stuff they’re doing? Is it outside the norm? That’s the way I look at it.

Matthew Sweeney: I think from the combination of technical and non-technical approaches that there’s definitely aspects of personal security, just knowledge in general, about you know, has been indicated before, behavior patterns, other aspects of risk that are definitely relevant, that need to be brought into the context of how am I assessing the risk? How am I driving cyber insider threat forensic analysis and that from an anomaly and signature perspective standpoint, I know that, you know, we’ve, we’ve been involved with research with DARPA and programs, you know, involving both anomaly detection, misuse detection, outlier detection and being able to, you know see, ourselves and others combine those detection methods synergistically so that you’re looking at misuse as your trigger but you’re able to combine that knowledge with other aspects of anomaly detection so your false alarm rate it, it goes away because you’re really keying in on a combination of behaviors rather than looking at, okay here’s purely the signatures I’m looking for and you’re able to do some that profiling, profiling as far as use of the information technology system itself, so not just user profiling but looking at profiling. How would we expect, as I’m deploying a system what would I expect the usage to look like and then being able to define anomalies based off that.
Randy Trzeciak: So, in terms of the data that we’ve analyzed, we say that we have a lot of data in terms of incidents, over 800 incidents. When we starting looking across those, there are some patterns that could be identified but that really gets to the organization events, actions, conditions. It goes to possibly the motive of the individual. But when we start looking for the technical patterns that could be included in the signatures of these particular tools, we don’t have a clear indication of that a consistent signature would apply across different organizations to identify something that’s anomalous in one organization compared to a different organization. If we go back to the definition that was stated before about the malicious insider that Patrick Ready uses, is the authorized individuals to authorized applications but with malicious intent. That’s where we start being able to see the challenges from an organization standpoint of deploying a tool that gets to the malicious intent and then when we can try to find that within an organization, maybe we can start to develop what are anomalies in an organization. But when we try to play that across an organizations that’s where we’re seeing some of the challenges that organizations, where they buy a tool, they deploy a tool and it’s either identifying everything or nothing in terms of what’s suspicious activity. And it really does take time for organizations to develop what are common patterns by the individuals, individuals within groups, groups within departments and departments across the organizations. And again, you do want to be able to compare individuals to themselves but also to peers or other groups across the organization. So it certainly is a challenge and I think some of the delays in deploying some of these tools is that, that the organizations are not able to take the time, at least initially, to develop these patterns and to identify anomalies based at the individual departments and organization-wide.

Bruce Gabrielson: Yeah I, I just thought of something else, don’t get confused by a trigger something that detects and at what an insider is. Yeah, some things if an insider does, are definitely detectable but you know you can get a threat indicator from just somebody all of a sudden took a trip someplace and happened to talk to a foreign individual. That is not saying that you don’t need the other aspects but like the other people mentioned, all you’re looking for something to kick off some other type of investigation or to watch somebody a little closer.

Michael Weir: We’re going to have the MPT folks help us, if you’ve got a question, grab the mic. Questions? We’ve got room for one Charlie. (Missed Vocals…)

Audience Member 2: (Missed Vocals…) My name is Charlie Flynn, some of you know me, most of you don’t. A graduate of 42 years working for the Air Force, 37 of it here in Rome. I left AFRL in 2008. Amongst my many projects, one of them was a client/server environment system services program to get and clean up the 17 different flavors of UNIX that DIA was using when I took over
that program. And we worked very closely with all the manufacturers, all the people that wrote operating systems to homogenize system administration and security settings. Microsoft was one of those companies, Sun, the rest of them; I don’t even know if they’re still in business, they’ve all disappeared. Silicon Graphics and I guess Hewlett Packard is still working, but one of the things you might want to think about is going to the vendors who build the operating systems to build in the controls the application program interfaces and the handshakes to do the auditing analysis, pattern analysis and the rest of the things. That’s where we had to go to get the audits, then, you’ve also got to find a box to analyze the audits.

**Bruce Gabrielson:** I can respond to that one easy. I happened to meet the chief engineer at Red Hat a couple years ago and Red Hat has a very close relationship with certain organizations. When you find something that you think needs to be added, they do include it in the operating system. The Red Hat Seven, I don’t know if you’re familiar with what they’re working on, but it has an extensive auditing profiling application built in now, so that’s there, they stay, work very close with organizations that do detect certain kinds of problems and, and say you know we’d like to fix this little better. Now that’s, that’s just one organization when you get to very large commercial organizations where security might not be the main thing that they’re looking at, they’re a little more reluctant to add those kinds of things in, but certainly some operating systems are adding those kinds of things in now.

**Michael Weir:** OK the next, the next question touches on some of the things that have been discussed a little bit earlier this morning. Detecting triggers in near-real-time audit data has received increased emphasis in the past three years; however, the storage and bandwidth impact has hindered the implementation of many potential tools. With new technologies being implemented to overcome this handicap, do you see increased applications for this particular solution set?

**Bruce Gabrielson:** Boy that sounds familiar to my presentation. Yeah, well we are getting increased bandwidth all the time and, as you know, we are getting massive repositories now so we can look at stuff pretty quickly. You know the Internet gets better based on needs, okay, if somebody says we want more faster, you know whatever, then it seems like there are organizations out there that will build it better, faster, so forth. So as we evolve, yes, a lot of those things start getting implemented. Now, I don’t know if I’m in favor of a pie-in-the-sky repository that collects everything that goes on, on networks but I certainly can see if you take a look at some of things even done right here in Rome, we start looking more at what is really needed for a detection, you don’t need all that data. Just out of curiosity, how many people ever look at the logs as they’re
coming through? You know I, I turned on HVSS the other day and I saw so many lines I couldn’t even follow them and that was nothing going on the operating system, just lines of, of log data. You know, it’s nice to say we want to collect everything and then go through and see what’s there and maybe you’ve heard some of my presentation before it’s also nice to say I don’t want to collect everything in real-time just what’s needed.

James Henderson: Thank you. What prior work that I’ve done for the government, what I’ve seen is a lot of organizations, some of what Bruce said is they don’t necessarily understand what a trigger is. It’s what, what at a minimum should we be looking at? Some people will point back to rags and say, “Oh we collect that.” But what are you collecting from an insider threat perspective? What, at a minimum, do we need to look at? Not we don’t need to look at everything. For example, do we need to look at print jobs? Do we need to look at web surfing habits? What are the minimum things we need to look at, and then build from there? You know, coming up with a list of triggers, I found, when I worked some organizations it just, you know, made it stand out, are you collecting triggers on email, print jobs, as I said, and various other things, databases.

Matthew Sweeney: I definitely think that tools are available, you know, everyone throws around the term “big data” but the, I know that within our team, we’ve been using real-time, stream processing-type analysis tools in combination with batch to process large amounts of data, and the key is, what’s been indicated here is that you can’t keep every, well you can if you’ve got enough servers, but, but that the real challenge is reasoning about that information so the consistency of common information models, each tool itself has its own common information model, and then you have to normalize those common information models, and then you have to reason about the data from there, and I think that’s really the big challenge is, even in, you know, cyber threat information sharing communities and things like that, there’s a challenge in people agreeing on how to communicate this information so the problem isn’t necessarily that the data is not there or the system can’t, isn’t big enough or fast enough to analyze it, it’s that, I want to make sure I know the what the system is saying is the same as what that system is saying and that the timeframe in which it’s being collected, I understand what’s actually occurring in order. There’s a lot of challenges there, so I think it’s, it’s more about understanding how the data is being reasoned about.

Randy Trzeciak: Yeah, I would try to like to echo the three comments that were made before in terms of the organizations. Certainly organizations that we’ve worked with are usually collect everything. Everything being just in case we ever need something, we’ll have the data available. But to be able to actively mine that data for items of interest, which get into the triggers, is where
organizations tend to struggle in terms of our opinion. Identifying what is something that should be triggered upon and something that acting upon is where organizations don’t necessarily have insights in terms of what is considered an observable that should be plugged into and in combination with other observables, to raise a level of something that should be investigated. So it’s certainly something that, that organizations do and we’re also seeing that organizations just due to, again, I mentioned my presentation, limitations in time, resources or money, again, we have all the data collected but we don’t necessarily have the resources to write the triggers, to ploy triggers and it’s not necessarily a justification of why it’s not being done but, honestly, the limitations of the people that are available and knowledge of, is, is a limiting factor in terms of why the triggers aren’t necessarily being deployed across a very large data set to a data set that is just everything and not necessarily the data, that was said before, that is of importance.

**Audience Member 1:** I have perhaps a question, Randy, you said that the organizations of the people done and there is a lot of data coming but they don’t really know what to monitor, right? This is pretty much what you stated, so my question is, how do we learn what to monitor or how do we make, you know, step forward and say, yeah perhaps we learned from the past. You know we know what had happened, bad thing happened then from this we can, maybe, figure out what we should monitor for so this bad thing would not have happened, right? So is it the way to go or there is some other way to figure out what should we monitor to get early detection of, of insider or any attacks in the system as well.

**Randy Trzeciak:** Yea, I certainly think that that’s a great question and we may go back to the presentation that I made this morning, and I know most of you are technologists at heart or have a degree of affection for technology but it really goes back to the organization deciding what you’re trying to protect. So if you trying to protect your data from leaving your network, that’s a particular strategy that you could use certain tools to detect leaving, information leaving, whether through email, through removable media or other exfiltration paths. If that’s the case, and we had that scenario of try to protect data from leaving, there’s certainly different types of data we can observe and look for different tools that can be deployed to try to prevent that particular activity from happening. So again, it goes back to the strategy of what you’re trying to protect. Going back to the scenario that was presented before of the critical infrastructure sectors where a sabotage event by an insider would cause physical harm and harm to the IT systems, that’s another protection strategy that would be ultimately different from the data exfiltration scenario. So any odd number of tools to be deployed, general sim-type tools, changes in configuration files, changes in operating system files, deployment of certain code, that’s a different strategy that would be for data
exfiltration, and then from organizations that are in a financial type environment or protection of fraud, again, different tools would be implemented in a business process environment that would identify suspicious activity, suspicious transactions, so, again, many organizations aren’t necessarily able to identify what they’re trying to protect, and what the potential impacts are, and if you can do that, that might give you a head start on what you should look and the types of data that would support your prevention or detection of that suspicious activity, based upon that potential impact to the organization.

**Audience Member 3 (Trent):** So, I hear a lot of stories about, what insider threats, the, the devastation that they’ve caused companies and organizations but I’m more interested in, all the experience that is on the panel, are there any stories where the technologies and tools were deployed and you actually caught somebody, like, you know, we, we found this guy because we deployed this and we did our statistical analysis, he fessed up, he knew that, you know, do you know, do you see what I’m getting at? It seems like we have a lot of stories about what, what’s gone wrong but I’d be more, more interested to hear of how things are going right.

**Michael Weir:** I, I think the answers would be interesting, clearly, and I don’t think we can cover too much of that here unless is anybody that wants to step up. Okay we could, we could discuss that in another venue, cool. Alright, so, let me, let me ask, I think we’re set, let me ask the next question, and, Randy, thanks for the, the lead-in, great lead-in on your answer there. Talking about the, what you’re attempting to do with the insider threat is an important aspect of how you attack the problem. So, in some instances, your objective may be to prevent insider threat activities from happening. In other instances, your focus may in fact be on prosecution of an event because something bad happened and in either of those situations you may think a little bit differently, and that’s part of the poser for the panel, you may think a little bit differently about your approach to implementing tools. Whether you attach the information to the data itself so you can see where it went, or you maintain the information about what is being done outside so you can, after-the-fact, come back and actually prosecute somebody. So the question is, “Would the differentiation between attempting to prevent or attempting to prosecute, which presumably could lead to prevention if enough people get their hands slapped, would that make you think differently about one approach versus another to in a mitigating insider threat?”

**Bruce Gabrielson:** I would say there are organizations that use both approaches, and a lot of it might be the sensitivity of the data, but certainly if you can tell the extent of a particular organization that’s ex-filtrating your data, that’s very useful to certain groups that do the investigative work. So, it’s not always just because there’s a trigger out there that you want to stop
something. In fact, usually there’s a trigger which basically initiates other actions and those other actions would be looking for who the particular person is that the data is going to. Now on the commercial side, that might be very useful as well, one of the things that was suggested a few years ago is phone home software added on to documents to see who ended up got, getting the documents. In the commercial world, that works a little better than in the DoD world, but, I think that was even developed here at Rome labs. The person who was working on it left already, he was sitting over there while ago. But, yes, it, it depends on the sensitivity of the data, certainly want to stop things real quick, but if you’re in certain environments, you want to follow the trail to see where it goes.

**James Henderson:** Pretty much agree with Bruce, no other comment on that.

**Matthew Sweeney:** I may have a little bit different perspective; I guess just from the analysis of what, how does the insider threat happen? Why does it happen? You know, in my mind the, the insider threat problem is just as much about sort of a workforce optimization, optimizing trust, optimizing understanding, helping people to know that they can reach out to psychological professional when they need help, and not, you know, and do that in a confidential way and get help, and so there’s, you know, prevention strategies from that end, on the, on the detection side of things, I mean, there’s trust that’s establishing when people know that when I’m operating, I’m accountable for what I’m doing and everyone else is too and so there’s a baseline level of trust there and protecting the organization so that I know what I’m working on won’t get lost. So I think there, there are definitely beneficial when indicated before. But I think that just that, that view of, you know, if we establish the whole, it’s not a necessarily a technological solution, plays, plays a lot into the back-and-forth there because as litigious as our society is, you know there is, in the case I might talk about a little bit later, Citibank where, you know, they had all the right controls in place but nobody observed them, nobody paid attention and so you get slapped with, you know, people breathing down your neck that way and if you don’t have those things in place then everybody’s upset at you, so it’s, you got a balance things there.

**Randy Trzeciak:** Just a quick comment on the prevention, it’s certainly easy to prevent folks on the outside, or at least that the goal to prevent someone from the outside from doing something, but when we move into the internals of an organization, prevent an insider from doing something, a lot of times that gets into the prevention of their day-to-day job activities. So, when we move from the external to internal protection, a lot of times, unfortunately, it has to be from a detection stand point and that detection might be configured to alert on something that could be considered suspicious, not always malicious, but something that could be implemented to alert when
something happens. Certainly the trust but verify model, as, traditionally has been conveyed, should be something applied internally to individuals inside the organization with authorized access, but unfortunately, the prevention of insider activity may prevent some of the day-to-day activities that are needed to do their job so, certainly recognize that it’s a challenge, so, it needs to be a combination of both is, as what was said before, prevention and detection or learning when something’s happened and then following up consistently with the investigations is certainly something that should be followed through as well.

Michael Weir: Biometrics offers a means of direct identification of a user in a fairly short period of time, and fairly accurately, even if the user is remote. So the question would be, “Why would there be a reluctance to deploy these technologies further or to integrate them with other technologies, or do you see a direction for that actually in place?”

Michael Weir: Well, I think maybe scalability might be a reluctance, or funding, I’m not really sure there, there are biometric solutions out there that are deployed a lot of places, in the intelligence community there’s a lot of biometrics deployed, so I, to me, I would think it’s very handy if you could identify an individual real quickly. You also get a pretty good indicator that it’s maybe not that individual and that allows you to take a look at all the actions going on, but again, that’s just one piece of insider. That’s a malicious insider, maybe a real trusted insider who wants to do some things and is going to impersonate somebody else that’s already in the network, rather than somebody outside hacking in. But other than that, I’m not sure the reluctance, other than budgetary reasons or scalability.

James Henderson: Thank you. I think that biometrics have a good use for insider threat, um, I still go back to starting with the basics of what tools you have in the organization, before you go with too many tools because it seems like what happens in a lot of organizations, people just run out, run out and buy tools and tools, can’t implement them, don’t know how to use them, don’t emblem property, before you know you have too much data. So I say, you start with what you have in the organization, look at the data feeds, the data you need and then move into some of the additional tools that can help, like biometrics and other types of software.

Matthew Sweeney: Yeah, this is more a personal opinion, I guess based on observation, but just that it seems like a monetary and time impediment to most organizations that if you have to integrate two factor authentication and everything and people lose, he’s gone, people lose the devices and that sort of thing then there, there’s just too much of this initial push to make that happen and with the cost, organizations just don’t do it.
Randy Trzeciak: Yeah, I certainly agree don’t, not much to add, obviously, the biometrics should be applied on the most critical assets and it should be factored into your enterprise-wide risk assessment of what you’re trying to protect and certainly if that’s an extra level of security that doesn’t impede the business operations and protects the critical assets, certainly that should be applied. Where it’s not broadly adopted, hopefully that’s a cost benefit or the risk associated with the asset you’re trying to protect is not begin deployed at the less critical assets that wouldn’t cause a significant impact to the organization.

Michael Weir: Next question, there’s been a significant research investment in use case analysis as a means of identifying potential malicious insiders. However, the amount of personal data that would need to be collected on an individual might have serious privacy issues. There’s also been significant progress in artificial intelligence during the past few years and if there was a means to automate more the background processing, so that you don’t actually have a human in the loop until the point that you need to actually make some decision point. The private information would be extremely limited; do you think that that would have an impact on the public privacy concerns regarding that potential tool set?

Bruce Gabrielson: I’d like that question answered, I’m not really sure, if you look at the privacy laws, you know it’s a, you need to court order really, to go investigate somebody and you can’t just look for data or look at data and then say oh I found a problem now I’m, now we’re going to really look at that person. It would be nice if we had a lot of background processing going on that just only showed us that threat indicator and at that point, I think I mentioned in my presentation, you would now justify the use of going and looking at the real data. So I think there probably would be a way of um staying within the legal framework of the privacy act and still be able to collect a lot of data and have some means of processing that data before you’d ever look at it so that you could limit what you really going to be exposed to, or who’s going to see it.

James Henderson: I echo that, I feel that there is a lot of data out there on individuals, especially that are working for the government, that could potentially be used as indicators, I mean there have been numerous cases out there of individuals that have come to work for the government that have shown clear indicators beforehand of um, not um, not behavior that would be conducive to working in the government, but it was ignored, overlooked or couldn’t be used. So then again, these persons come to work for the organization and then, then we realize later down the road, there’s problems. I mean, I think I even read an article last night; something came out of the Manning trial about stuff that was posted on Facebook that just kept getting ignored. I know that gets into a sensitive issue now I know a lot of state laws come out now that the government can’t
look at, you know, Facebook and other type of public information but I think it would definitely be helpful in, in, you know, possibly weeding out bad actors that would come into an organization.

**Matthew Sweeney:** I would, I would echo the public information that is out there, I know that some, some folks want to get into folks private Facebook accounts and things like that, and that’s over stepping definitely, but the, the concept of people trusting machines, just look information, everyone knows that there is still a human who can access the data on that machine, so I think there’s just can be inherent lack of trust there. If, if you’re housing a lot of private and personal information, and as far as about using public information, you know, the government might not be able to access certain levels of information, private corporations, on the other hand, have a little bit more leeway there in you know, HR recommendations saying, you know, it’s prudent to look at what’s publicly available so that you can understand what an employee or potential employee might be doing. But, a bigger issue might be a lot of this information becomes stale, we’ve talked about several times, you know that once somebody is trusted, then they are forever trusted. In case, and the case where there was reinvestigation of his clearance and I think there’s a lot of issues around placing initial trust without understanding the evolution of life events and a lot of that information can be collected, you know if someone had DUI or other kinds of things that are public record, those are things that can be taken into account.

**Randy Trzeciak:** I certainly echo the, the challenge that organizations have with collecting potentially private data and using that for some analysis. I might want to take just a little bit different approach; on our team we do have a lawyer who works for me, specializing particularly in monitoring and strategies from an organizational standpoint and one of the things that she challenges us, with from an organizational standpoint, is to consider certainly when employees log into a system, they are presented with a log in banner. They accept that they’re going to be monitored and she really challenges us to consider the expectation of privacy on the systems. Certainly, if you ask, you, as the operational folks, is there any expectation of privacy on the systems? Most people, by seeing that banner, would say there’s no expectation of privacy, but from an organization standpoint, that expectation of privacy should include a consistent monitoring of activity, and if individuals are allowed to do things on your network that might constitute that there is some expectation of privacy to include, using your networks and system to go to check their bank account, or to send email, personal email, on your accounts and systems, and that email may be going between them and their lawyer or their doctor or their union rep that, in that cases, are information your collecting as part of your log-in strategy but that might be protected communication that in some cases could not or should not be collected and used for any type of
Michael Weir: The panel did a great job, you guys, thanks for discussing, as well. This last one is a fairly easy question that I’d like to get a comment on. If the good guys are the folks trying to prevent the insider threat, are the good guys on a winning trend, losing trend, or is it kind of a draw, at this point? Complete opinion.

Bruce Gabrielson: And I’m the first who has the answer. Pretty much a draw. I think the good guys are making progress and I think the bad guys are still able to do their thing until we’ve got complete control of the threat and know what’s going on, I think we’ll continue to have the same problems we’ve had.

James Henderson: I agree, I think we’re starting to make progress with insider threat, I think there’s still a lot of people out, not so much maybe government, but an industry don’t understand it, this uncharted world, but I definitely think we’re making progress and it’s just going to be education and in time, we’ll get there.

Matthew Sweeney: I don’t know if this will be popular or not but I think the good guys are losing and, and I think that because A, there’s cultural shifts that indicate people want information to be free and they’re trained from an early age to think that it’s okay to, whether it’s downloading music even if they’re not trying to get profit from it to just feeling like it’s the immediacy of electronic communications, makes my brain more lenient about what I’m willing to do morally. So that’s a huge challenge, it’s going to, because that’s really the basis for insider threat, is can I trust my employees, can my employees trust me, and then, as things move in to more virtualized environments as I can get access to my own virtual private network and send things as you know you try and integrate more technologies and things continue to accelerate, it’s going to be more of a challenge keep up with that.

Randy Trzeciak: Certainly from the reporting standpoint, we’ve noticed a lot more in terms of the media reporting of people being caught or people being prosecuted so obviously that’s a good thing. We’ve been doing a survey since about 2004 to try to identify cyber security activity and
how organizations handle that. Since about 2004 we’ve been consistently hearing from organizations at about three quarters, or about 75%, of the insider incidents are handled internally and don’t involve law enforcement so from a standpoint of the reporting we see it’s getting better but we still certainly believe that it’s underreported and if an individual goes from one organization to the next and they’re not prosecuted for a previous incident, many times that’s information that’s not being able to be used as a screening deterrent from one organization to the next. Many organizations are only allowed to report they worked for an organization for a time period to time period, and they can’t really comment on the reason they left except for so, to answer the question we’re not sure, reporting is getting better but we still seem to think that it’s stiffly underreported in terms of insider malicious activity.
### Internal Threat Policy & Practice Resources

<table>
<thead>
<tr>
<th>Source</th>
<th>Title</th>
<th>Release Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.cert.org/">http://www.cert.org/</a></td>
<td>The CERT Division, Software Engineering Institute, Carnegie Mellon University</td>
<td>-</td>
<td>Website offering a myriad of resources and strategies for insider threat mitigation in various situations, especially those relating to cybersecurity. The insider threat portion of the site includes publications and research freely available to the public.</td>
</tr>
<tr>
<td>Pfleeger, Shari Lawrence et al., “Insiders Behaving Badly: Addressing Bad Actors and Their Actions,” <em>IEEE Transactions on Information Forensics and Security</em> 5, no. 1 (March 2010): 169-79.</td>
<td>Insiders Behaving Badly: Addressing Bad Actors and Their Actions</td>
<td>2010</td>
<td>Overview that describes insiders and their actions based on factors at all levels ranging from work environment to the individual so that potential threats may be identified and solutions crafted based on individual circumstances.</td>
</tr>
<tr>
<td>Center for Infrastructure Protection (cip.gmu.edu); Unpublished Report</td>
<td>Army Response Plan to Protecting the Force: Lessons from Fort Hood</td>
<td>2010</td>
<td>Drawing from lessons learned from the Fort Hood shooting, this source offers recommendations to mitigate physical insider threat, specifically through stronger communication ties, increased situational awareness, and interoperable courses of action.</td>
</tr>
<tr>
<td>NIST Special Publication 800-53 available at <a href="http://dx.doi.org/10.6028/NIST.SP.800-53r4">http://dx.doi.org/10.6028/NIST.SP.800-53r4</a></td>
<td>Security and Privacy Controls for Federal Information Systems and Organizations</td>
<td>2013</td>
<td>A detailed discussion of the standards and practices promulgated by NIST for the protection of government information systems. This source includes a broader range of information than that which applies directly to insider threat, but includes recommendations for dealing with both malicious and non-malicious insiders.</td>
</tr>
<tr>
<td>New Mexico Counterintelligence Working Group Unpublished Newsletter</td>
<td>Edward Snowden - The Untold Story</td>
<td>2014</td>
<td>Extracts of a Wired article that provide a more in-depth look at Edward Snowden's background than previously released into the open source.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
</tbody>
</table>
5.0 ABSTRACTS

5.1 Personnel Behavior Physical and Virtual: The Whole Person Insider Threat Program

*Prepared by: Matthew Sweeney*

An abstract for this presentation is not included here as Matthew Sweeney’s paper is contained within the previous Section 2.0.
5.2 Insider Threat Workshop Keynote

Prepared by: Dr. Bruce Gabrielson

The first Insider Threat SOAR described the problem and the solutions that existed 7 years ago. A lot changes in 7 years. Visible insiders have caused great harm to our country while at the same time new technologies and tools have been fielded.

Not only have the tools and techniques available to detect insider threats improved, but the challenges of new technologies, such as Cloud Computing, Bring Your Own Device (BYOD), multiple VM environments, tactical SIGINT systems, etc. have resulted in the need for developing new tools to detect and otherwise mitigate the insider threat.

The current challenges relate to enhancing techniques for personal profiling, activity profiling, and behavior profiling.

**Personal Profiling**

Personal profiling incorporates the research from organizations like Carnegie Mellon, Pacific Northwest Labs (PNNL) and others who have looked at the precursors and indicators of potential malicious insider activities.

Developed from actual instances, these models are often associated with ethical or practical lifestyle issues or developed by integrating employee data, including psychological or social data with audit data.

One area of threat starting to emerge is the correlation between age/family stability and potential for major insider exposures such as in the case of Manning and Snowden.

**Activity Profiling**

Activity profiling is an interesting area of research. This includes taking a look at what an individual does in relation to their job function.

Let’s consider a person who works in a particular skill set technical area. If we first segment the job description by say focus area and then by technical concentration, we might come up with a couple of visual mappings that look like this.

Other individuals working in the same area would have similar but not necessarily the same profiles.
Over time these profiles would expand but still retain the same overall shape unless the employee changed to a different technical area or expanded their skill set. Now what happens if an individual’s profiles didn’t fit the norm?

This might be cause for additional monitoring or investigations.

**Behavior Profiling**

From the suspicious activity perspective, in August 2011 NSA released a report, COMPILED MALICIOUS ACTIVITY AND ATTACK USE CASES AND EXAMPLES. Over 83 suspicious activities were identified that are potentially detectable as they are taking place. The audit log data sequence for many of these use cases were developed right here in Rome.

Another area I’ve personally followed related to insider impersonation is biometrics including keyboard identification and mouse movement identification. Mouse movements, even with latency over remote connections, has come a long ways towards identifying an individual in a very short time period.

A different focus area is the identification of trusted remote connections from an individual in multiple locations at the same time or from a connection in a location different from the normal location during normal working hours. This activity would indicate that perhaps an individual’s credentials have been compromised.

I might also mention that normal users perform certain routine activities when they login each day. A remote login from a user who does not follow this sequence is cause for suspicion.

I disagree with those who continue to say the problem is not well understood. The problem is understood just not easy to solve.

Some continue to say data on insider attacks is difficult to obtain. There are massive amounts of information available on what happened and how it happened. Even the existing SOAR spent considerable time proving this. I personally think quality time on the next SOAR should be spent to focus areas for research and potential solutions, including the fusion of multiple technologies, and less on trying to prove that it is a problem or build new databases with examples.
5.3 Security Attacks and Cyber Crime: Computing through Failures and Cyber Attacks (Insider Threat Workshop Presentation Summary)

*Prepared by: Zbigniew Kalbarczyk*

**Introduction**
Imperfections in engineering current generation computing systems make failures (due to either accidental faults or malicious attacks) inevitable. Such systems must be designed to operate through failures and cyber-attacks. Many successful attacks are conducted by attackers that enter the system with known (or stolen) credentials, i.e., they log in as legitimate users and essentially become insiders. In such a scenario one must monitor the attacker activities to allow detecting anomalies and triggering appropriate response mechanisms to prevent system damage.

The following briefly discusses some of the current security threats and then presents examples of real threats in the context of real computing systems.

**Current Security Threats**
Advanced Persistent Threats (APT) are a real danger. APTs represent targeted attacks that combine social engineering and malware to target individuals in companies/organizations with the objective of stealing confidential information, e.g., trade secrets or customer data. APTs often use custom-written malware and exploit zero-day vulnerabilities and hence, are highly infective and hard to detect (42% increase in 2012), e.g., a *watering hole attacks* represent a recent innovation in the targeted attacks.

Another area with increasing security threats are mobile devices. Businesses are increasingly allowing staff to “bring-your-own-device” (BYOD) to work. As a result employees use personal computers, tablets, or smartphones for work and companies by allowing use of consumer technology (e.g., file-sharing websites) and devices reduce the cost. While this is good for business, it also brings a greater risk due to mobile device vulnerabilities and often lack of security features, e.g., encryption, access control, and manageability, e.g., attackers have an easier task to harvest users’ credentials.

**Examples Real Threats in the Context of Real Systems**
*Analysis of Security Incidents in a Large Computing Organization*
An in-depth study of the forensic data on security incidents that have occurred over a period of 5 years at the National Center for Supercomputing Applications (NCSA) at the University of Illinois shows that nearly 26% (32/124) of the incidents analyzed involved credentials stealing i.e., an attacker enters with already-stolen credentials of a legitimate user and hence, the behavior is the same as that of a malicious insider [1], [2].
Although this analysis has focused on a NCSA network, a good portion of the analyzed incidents pertain to other campus or open research networks. In a fully closed environment, e.g., a corporate network with firewalls on perimeter, types of attacks and type of misuses identified may be different. However, incidents due to compromised credentials could happen in virtually any network which is accessible from the Internet (e.g., social networking sites, email systems, corporate networks allowing VPN access) or from an intranet or a business network managed by an IT department within a corporation.

Therefore, insights from this analysis are representative of many different environments and can be used to guide better design and organization of defense mechanisms. Stuxnet Reported June 2010Dequ Reported October 2011Flame Reported May 2012Gauss Reported August 2012 designed to sabotage an industrial process not destructive looks for information useful in attacking industrial control systems descendent of the Stuxnet (probably) created by the same authors as Stuxnet, or people with access to the source code of Stuxnet written purely for espionage collects technical diagrams for intelligence purposes: AutoCAD drawings, PDFs, and Text files can record audio, screenshots, keyboard activity, network traffic, Skype conversations written for cyber espionage campaign directed at a specific banking system seems to be created by the same authors as Flame acquire logins for e-mail and instant messaging accounts, social networks and, accounts at certain Lebanon’s banks along with Citibank and PayPal.

**Critical Infrastructure: Characterization of Resiliency of Power Grid Substation Devices**

Power grid is a crucial infrastructure where a failure could have catastrophic impact on each citizen and on the society as a whole. Use of IEDs (Intelligent Electronic Device) in substations to monitor the power grid and communicate between the control centers and substations makes this infrastructure vulnerable to accidental errors and malicious attacks (including insiders who obtained illegitimate access to the SCADA (Supervisory Control and Data Acquisition) system.

We use error insertion to mimic consequences of accidental errors and/or malicious attacks in power substation devices and characterize system resiliency to such events. The experiments show that Silent Data Corruption (SDC) is the most severe outcome for applications. SDC corresponds to a situation where the application does not crash, however it does not pass the corresponding validation process. For example, due to SDC in the control software executing in the power substation, a control command issued by the SCADA Master cannot be successfully passed to the relay. As a result incorrect sensor data (from the substation) are retrieved by the SCADA Master and an operator in the Control Center (where the SCADA Master operates) can lose control over the equipment in the substation, which may result in a blackout or damage of the equipment [3].
**Example of Industrial Espionage in Cyberspace**

Stuxnet (discovered in July 2010) is the first publicly known malware intended to damage industrial control system, with specific focus on Iranian uranium enrichment facility. The malware is of unprecedented sophistication: (i) four zero days vulnerabilities exploited (first time any threat has done this), (ii) drivers signed using stolen certificates, (iii) professionally written code, (iv) more than 100,000 infected machines before malware discovery, and (v) 1000 centrifuges withdrawn from the service.

**Conclusions – What’s Ahead?**

Targeted attacks and APTs will continue to be an issue. The foundation for the next Stuxnet-like APT attack was established Frequency and sophistication of these attacks will increase. The last few years indicate that Stuxnet is only the beginning and as indicated in Table I:

- New targeted attacks have already arrived; malware authors and spammers will increase their use of social networking sites
- Mobile phones and tablets will become more and more vulnerable to malware
- The insider threat will grow, as employees act intentionally or unintentionally to leak or steal valuable data

**References**


Chapter 4 Localized Encryption Groups

The Localized Encryption Groups (LEG) kernel driver is a data loss prevention (DLP) solution that automatically protects data at rest and in transit without interrupting the user’s workflow. This effort, currently funded through AFRL as a Phase II SBIR award (FA8750-13-C-0003), addresses the insider threat by making unauthorized data exfiltration events extremely difficult to achieve. Prior to development, our research examined several techniques in which mass exfiltration can be quietly thwarted without interfering with user workflow. The result led to the development of a system containing two major components. The first is a Windows kernel driver that intercepts read and write system calls and ensures that files are accessed by appropriate white-listed applications. The second component of LEG is a user-level application that operates in the background and maintains an attribute-based cryptography service for each file. This service encrypts all sensitive file types defined by the organization with a symmetric AES key that is stored in the file header. The AES key is then asymmetrically encrypted with a public key.

LEG is installed on a network supporting Active Directory and works on a per file basis by attaching a special LEG file header that contains information about who is authorized to access a particular file. This header is read by the kernel driver, which acts as a policy enforcement mechanism. Furthermore, the LEG kernel driver only allows authorized applications to access the file. The insider threat is stymied by not allowing users or processes to access sensitive data without sufficient privileges. Finally, LEG prevents files from ever being stored to external media unencrypted. It intercepts all computer actions that write data to disk or send data over the wire, so even the most surreptitious data exfiltration techniques will not be able to extract sensitive data—even if attempted by authorized personnel.

This topic is presented to illustrate how low-level software techniques can be applied to the insider threat. Because LEG operates just above the kernel, its proximity to the hardware allows it to act as a first line of defense dictating who may successfully decrypt a particular file and ensuring that the file is never stored in plaintext to any media. Technologically, LEG is simply a per-file encryption tool, but it also acts as an insider threat deterrent.

We conclude that products intended to address the insider threat are met with hesitation if they interfere with user workflow or impede productivity. What makes LEG unique from other cryptographic solutions is that a user’s private key is generated using credentials held by the user.
on an Active Directory server. When a user meets all of the policy criteria for access to a given document, it is only then will she be able to successfully decrypt it. If the user does not possess the proper credentials for opening a given file, she will be denied access to the data altogether. This process of data protection is performed in the background and doesn’t require any additional steps from the user.
5.5 Insider Threats Current Events: The Critical Infrastructure Security Perspective: Cutting Costs or Cutting Our Throats?

Prepared by: Mark D. Troutman, Ph.D., and Paul B. Losiewicz, Ph.D.

An overview of factors influencing Return on Investment (ROI) decisions by the U.S. Government in combating Insider threat. Foremost is the influence of sequestration on DoD budgets. The increase in outsourcing to consultants and contractors to reduce personnel costs has increased reliance on HR systems that are over-stressed in dealing with turnover and lack of oversight in personnel security management, monitoring and reporting. This prescient brief was given before the full impact of the Snowden revelations was understood or the Navy Yard shooting occurred.
5.6 Generation Y Insider Threat

Prepared by: Richard Cook

The focus of “Generation Y: Insider Threat” was to convey some character traits in Gen-Y’ers that may pose a threat to the confidentiality, integrity, and availability of sensitive information. This presentation outlined attributes which are common to Generation Y, and how these attributes affect the security of both commercial and government entities as they relate to the insider threat. Research was also presented on the motivations behind this group how this threats stemming from this group can be mitigated.

The purpose of this presentation was NOT to cast this subset of the populace in a poor light, or to brand them as a threatening entity that should be avoided, only how their values may affect information security from the standpoint of the insider.

This information was presented because Generation Y is the fastest growing segment of the population currently flooding the workforce, and will continue to do so for the foreseeable future. Their behaviors, views, and values are in direct relation to how strictly they follow security procedures, and therefore, will determine the overall state of information security as they replace former generations in the workforce.

Polling revealed that the majority of Generation Y’ers do not adhere to security policies and common practices, or were unaware that any such standards even existed in their place of work. Their security posture is a direct reflection of common values found in this generation. These values include a culture of open information sharing, instant gratification, and entitlement.

These ideals directly reflect their security practices and can lead to risky activity both at home and in the workplace. Polls show that Generation Y’ers regularly engage in the following:

- File sharing
- Downloading “warez” from illegal sites including torrents
- Responding to pop-up ads and participating in online surveys and promotional contests
- Leaving workstations in a logged-on state

This generation cannot, and should not, be avoided. Instead, by understanding their motivations and principles, information security policies and practices can be molded and evolve to better suit the future workforce, thus mitigating this form of insider threat.
APPENDIX A – PRESENTATIONS
We’re discussing issues of trust as they relate to personnel risk and insider threat
• Especially applicable to security clearances, just as pertinent to hiring decisions and continuous employee monitoring
• Understanding more about what we don’t know when it comes to cyber behavior
  • Behavior patterns relating to work and non-work activities
Raise awareness of the behavioral and psychological trends as they relate to insider threat

Key questions
• What are the trends in adverse online behaviors?
• What online behaviors most often occur with respect to offline behaviors?
• How can online behavior analysis be incorporated into personnel security and insider threat detection?
**Insider threat examples**

- **Espionage**
  - Ames, Hansen
    - Lied under polygraph and got away with it (for a time)
  - Moral obligation, disaffection?

- **Theft**
  - Citigroup Employee (2011)

---

**Cyber Behavior and Employee Trust**

- Anderson et. al (2004) engaged in a systems dynamics / game theoretic approach to analyzing insider threat. Some underlying assumptions:
  - Improving trust as a means of decreasing rate of insider threat
  - Must not be ignorant of threat or it enables malicious attackers
  - How to find the appropriate level of monitoring?

- Participation in web-based illegal activity (e.g. procurement and distribution of pirated materials, guessing others passwords etc.) or engaging in deviant or rule-breaking cyber-behaviors with disregard to others.
  - 38% of undergrads self-reported engaging in at least one deviant cyberbehavior in past 3 years (Rogers et al., 2006).

- Inappropriate disclosure of proprietary, confidential, privileged, or secure information in email, chat rooms, personal web pages, blogs, etc.
  - People report disclosing more in their internet relationships compared to in-person relationships (Floyd, 1996).

- Computer-mediated activities that provide potential for exploitation or suggest disloyalty (e.g. involvement in computer groups allied to stigmatized practices).
  - People belonging to a stigmatized group were more likely to be involved in an internet-based group of similar others (McKenna & Bargh, 1998).

- Web behavior of an addictive nature
  - More likely to reveal personal concerns (Whang et al., 2003)
  - Internet addictions are more common among those with mental disorders (Shapira et al. 2003) and who use internet as an escape mechanism (Cooper et al., 2001).

- Providing false or derogatory information within computer-mediated communications about oneself or others
  - Men may use identity deception to be reveal secrets, while women use identity deception for safety reasons (Utz, 2005).
Slide 5.

Identifying indicators of risk and resilience

- Sensation seeking is positively associated with posting hostile and/or insulting messages
  - More so for men than women; (Alonzo and Aiken, 2004)
- People high in psychotocism showed a lack of interest in the social communal aspects of internet use but demonstrated an interest in more sophisticated and deviant use (distribution of pirated materials, pornography)
  - (Amiel & Sargent, 2004)
- Internet addiction is associated with shyness, social anxiety, and loneliness
  - (Morahan-Martin, 2007)
- Computer deviants display personality and moral decision-making characteristics that are significantly different than those not reporting deviant cyberbehaviors
  - (Rogers, Smoak & Liu, 2006)

Slide 6.

Holistic Security Awareness

Slide Notes:
Our team sees the landscape of personnel security, workflow and collaboration, and cyber security all being related because they all involve people and their behavior.
Slide 7.

Adverse Online Behavior Study

- Goals and Objectives
- Approach
- Results & Findings
  - Characterization
  - Trends
- Limitations
- Recommendations

Slide 8.

Goals and Objectives

- Understand how online behavior relates to personnel security and insider threat
  - Rates of prevalence for categories of behavior
  - Relevance to granting, maintaining, loss of clearance
  - Baseline of adverse online behavior in particular org. population, including trends over time
- Identify robust indicators of adverse online behavior
  - Psychological analysis and questionnaire
  - Behavior association analysis
  - Develop models that can be used for automated and assistive analysis/QA
- Enable more effective prevention and mitigation of insider threats
  - Focus on finding adverse online behaviors
  - Better information for the organization security operations
  - Provide opportunities for organizations to engage before incidents occur
Slide 9.

**Approach**

- Analyze a 50,000+ adjudicative case file set
- Identify all occurrences of Adverse Online Behavior (AOB)
- Determine combinations of high risk behaviors and characterize all AOB
- Analyze trends over time in AOB at a general and detailed level
- Develop predictive models for AOB given Adjudicative Criteria and other AOB

**Slide Notes:**

Occurrences of AOB are based on the newly defined AOB Taxonomy, which is based on our experience with personnel security adjudication risk assessment and an extensive literature review of online behavior studies. Note that general means at the top level categories for adjudicative or AOB taxonomy criteria, while detailed means any of the leaf nodes in those taxonomies.
Defined 47 categories of adverse online behavior
Categorized over 3000 cases as having instances of AOB
Effectively applied automated characterization techniques

### Examples of Adverse Online Behavior

<table>
<thead>
<tr>
<th>Problematic Cyber Behaviors</th>
<th>Security Risk Indicators</th>
<th>Mental Disorder Traits</th>
</tr>
</thead>
</table>

- Accessing Others Email, Computer Network
- Accessing Pornographic Materials
- Blogging, Chatting, Emailing
- Browsing, Buying, Selling Online
- Counter-Productive Misuse IT Systems
- Distributing Processing Pirated Materials
- Hacking Into Computer System, Website
- Illegally Download Copy Media
- Initiating Sexually-Oriented Messages
- Introducing Malware
- Involving Oneself with Subversive Computer Groups
- Playing Games, Social Networking
- Sending Defamatory Statements, Harassment

---

**Slide Notes:**
Reference the list of adverse online behaviors for those associated with denied cases as those definitely being associated with higher security risk:

- **Manic – Mood Disorder**
- **Sexual obsession and explicit sexual usage**
- **Online gambling – excessive**
- **Shopping – excessive**
- **Auction site usages – excessive**
- **Time on cyber sites – excessive**

The goal is to understand / discover any links between cyber behaviors, mental disorder traits, and security risk indicators. We believe that these relationships exist based on our survey of literature and our observations of the data sets we held.
AOB is a growing issue - there is an increase in AOB prevalence in personnel security cases
Based on literary research there are key behaviors that can be observed to determine tendency toward AOB
Many AOBs pose an increased security risk when present, particularly when coupled with other adjudicative criteria
Better data collection regarding AOB needs to occur in order to consistently assess the risk related to cases involving AOB
AOB Guidelines Example

- **Definitions of AOB behavior**
  - Misrepresenting Self / Stealing Another’s Online Identity - This General behavior covers misrepresenting yourself online, for example by creating a false identity or assuming another’s online identity by using their online account or authorization.

- **Examples of AOB**
  - Creating false accounts, including banking, credit, and names / addresses
  - Hacking into system to send information from another account

- **Associated Offline Behaviors**
  - Misuse of Information Technology Systems, Sexual Behavior, Personal Conduct

- **Relevance to personnel security risk**
  - Medium-Low change when found with:
    - Alcohol Consumption, Criminal Conduct, Drug Involvement / Use, Emotional, Mental, and Personality Disorder, and Foreign Influence

---

Slide 14.

**Behavior Association Examples**

<table>
<thead>
<tr>
<th>Offline Behavior</th>
<th>Adverse Online Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allegiance to the United States</td>
<td>Counterproductive Misuse of IT Systems</td>
</tr>
<tr>
<td>Criminal Conduct</td>
<td>Corrupting / Destroying / Encrypting / Manipulating / Transferring Cyber Assets / Data</td>
</tr>
<tr>
<td>Emotional, Mental, Personality</td>
<td>Initiating Sexually Oriented Messages, Introducing Malware</td>
</tr>
<tr>
<td>Disorders</td>
<td></td>
</tr>
<tr>
<td>Misuse of Information Technology</td>
<td>Playing Games / Social Networking / Virtual Role Playing</td>
</tr>
<tr>
<td>Systems</td>
<td></td>
</tr>
<tr>
<td>Other Security Factors</td>
<td>Counterproductive Misuse of IT Systems</td>
</tr>
<tr>
<td></td>
<td>Hacker into Another Computer/System/Website</td>
</tr>
<tr>
<td></td>
<td>Counterproductive Misuse of IT Systems, Hacker into Another Computer/System/Website</td>
</tr>
<tr>
<td></td>
<td>Security Concerns</td>
</tr>
<tr>
<td>Outside Activities</td>
<td>Contacting Unauthorized People</td>
</tr>
<tr>
<td>Personal Conduct</td>
<td>Other Serious Misuse of IT Systems</td>
</tr>
<tr>
<td></td>
<td>Browsing / Buying / Selling Online</td>
</tr>
<tr>
<td>Security Violations</td>
<td>Distributing / Possessing Pirated Digital Materials</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Sexual Behavior</td>
<td>Accessing / Downloading / Transmitting Pornographic Materials</td>
</tr>
</tbody>
</table>
**Slide Notes:**

When AOB case count is normalized against the number of cases reviewed as a whole, these are the top percentage concerns.

**Examples of other serious misuse of IT systems:**

- Distributing / Possessing Pirated Digital Materials
- Accessing / Downloading / Transmitting Pornographic Materials
- Engaging in E-commerce Disreputable / Deceitful Practices
- Furthering Private Business Enterprise
- Illegally Downloading / Copying / Music / Movies / Other Media
- Involving Oneself with Subversive Computer Groups
- Initiating Sexually Oriented Messages
- Internet Gambling
- Plagiarizing
- Sending Defamatory Statements / Harassment
Slide Notes:
When AOB case count is normalized against the number of cases reviewed as a whole, these are the lower percentage concerns.

Slide 17.

Slide Notes:
When looking only at AOB cases, the percent distribution is as provided. People appear to become less careful about what they install on their machines over time.
AOB Trend Observations

- Period of analysis is from over the course of 8 years
- Other Serious Misuse of IT Systems trend upward, while security concerns and counterproductive trend downward
- Increase in illegal downloading / copying of media, social network / virtual worlds
- Counterproductive misuse and security concerns were biggest issues at general level
  - Mostly relates to contacting foreign nationals
- Interesting note – small but perceivable increase in hacking-related activities from 2005 onward

AOB Trends

High-Occurrence Detailed AOBs

- Contacting Unauthorized People
- Blogging Chatting Email
- Illegally Download Copy Media

High-Occurrence Major-Level AOBs

- Counterproductive Misuse IT Systems
- Security Concerns
- Other Serious IT Systems

Anomalous AOBs

- Hacking into Computer System Website
- Transmitting Classified Information
### Results

- Documented taxonomy of adverse online behavior (AOB)
- Categorized AOBs in nearly 3000 clearance cases
- Discovered trends over time and behavior associations in AOB
- Developed guidelines for relevance of each AOB to personnel security
- Psychological questionnaire developed with goal of determining security risk for online behaviors
- Developed predictive model that can identify likely AOBs given offline behavior

### Limitations

- Data collection needs to improve regarding online behavior in order to support better modeling of this risk
  - AOB instances are based on descriptions of DCID 6/4 criteria
- Models and analytical results are based on past adjudicative decisions – gaps in data regarding certain AOBs can occur due to lack of training / understanding regarding AOB from investigator / adjudicator standpoint
  - Having exact cause for denial of clearance directly attributed would aid in prediction
- Policy on handling AOB is not consistent, therefore predictions of risk that are based on past decisions will reflect that

---

**Slide Notes:**

The data samples that we used exhibit bias in that the questions asked by background investigators, adjudicators, and polygraphists are targeted toward the ICD 704.2 guidelines. These guidelines do not contact a sufficient sample of criteria and examples regarding online behavior.
Develop a policy for communication with current and potential staff that involves discussion on online behavior
- Focus on behavior as a whole, not purely aspects that might cause dismissal
- Gather AOB information through questionnaires and voluntary disclosures
- Provide capabilities for those in HR or security clearance vetting positions (e.g., investigators, polygraphists, and adjudicators) to correlate information from multiple sources in order to observe and assess severity of adverse online behaviors
- Coordinated policies between personnel and network security may aid security risk management

**Slide Notes:**

Gather more online behavior information through questions in the SF-86 and distinct questions in background investigation process.

Develop a consistent policy for the handling of AOB.

Apply information developed in this study to provide augmentative capabilities for investigators, polygraphists, and adjudicators.

Growing trends in online behavior issues mean professionals from personnel security and network security should be talking more and have coordinated policies for dealing with insider threat issues.
Continuous Employee Assessment

- Enables risk-based prioritization of insider threat forensic analysis and renewed background check information
- AOB Taxonomy
  - Integration into existing security standards would provide a uniform guide for capturing online behaviors relevant to security risk
  - Assists with electronic adjudication and data analysis
- Cyber Risk Assessment Questionnaire
  - Provides concise means to determine online behaviors related to personnel security risk
  - Can be validated using other proven validity studies
- Develop AOB Observations and Best Practices

Questions?

- Matthew Sweeney
  msweeney at srcinc dot com
Background

- Five years since the release of the first Insider Threat State of the Art Report
  - In reality, it's been almost 7 years since the data was current.
- While many exciting changes and innovations have taken place since that time in a number of detection areas, we've still been hit with Manning, Snowden, and others less visible.
- Newer tools are now available for general and focused monitoring plus models have been validated for predicting personal behavior.

Slide Notes:

We have a job to do during the discussions today. Not only have the tools available improved, but the challenges of new technologies, such as Cloud Computing, Bring Your Own Device (BYOD), multiple VM environments, tactical SIGINT systems, etc. have resulted in the need for developing new tools to detect and otherwise mitigate the insider threat.

A cloud insider is normally thought of as a rogue administrator of a service provide, but you could also have an insider who exploits a cloud-related vulnerability to steal information from a cloud system, and the insider who uses cloud systems to carry out an attack on an employer's local resources. I want to start this workshop off by highlighting a few areas that I hope will be discussed.
**Profiling**

- **Personal Profiling**
  - The precursors and threat indicators of potential malicious insider activities often associated with unhappiness, ethical or practical lifestyle issues

- **Activity Profiling**
  - What an individual does in relation to their job function

- **Behavior Profiling**
  - Specific activities that are suspicious in nature

---

**Slide Notes:**

Since my personal background and focus has been on the development of IA tools that help initially identify a potential insider problem, I have naturally slanted my presentation towards this area and the models or triggers that can be developed.

I first want to break down the advancements in three primary research areas, each of which can have both an IA and a behavior component. This is my breakdown and might not be the same as others would look at the various issues.
Personal Profiling

- Developed from actual instances and case studies
  - These are often associated with ethical or practical lifestyle issues or developed by integrating employee data, including psychological or social data with audit data.
- Profiling has been a primary focus of several research organizations over the past few years.

Slide Notes:
Personal profiling incorporates the research from organizations like Carnegie Mellon, Pacific Northwest Labs (PNNL) and others who have looked at the precursors and indicators of potential malicious insider activities.

Developed from actual instances, these models are often associated with ethical or practical lifestyle issues or developed by integrating employee data, including psychological or social data with audit data.

One area of threat starting to emerge is the correlation between age/family stability and potential for major insider exposures such as in the case of Manning and Snowden. The DoD has also had a recent change in the requirements for PRIVIC access, primarily as a result of these two individuals.
People tend to perform their work in a particular way on a regular basis.

By segmenting job descriptions into unique areas of activity, graphic models can be developed.

**Slide Notes:**
Activity profiling is an interesting area of research. This includes taking a look at what an individual does in relation to their job function.

Let’s consider a person who works in a particular skill set technical area. If we first segment the job description by say focus area and then by technical concentration, we might come up with a couple of visual mappings that look like this.

Other individuals working in the same area would have similar but not necessarily the same profiles.

Over time these profiles would expand but still retain the same overall shape unless the employee changed to a different technical area or expanded their skill set. Now what happens if an individual’s profiles didn’t fit the norm?

This might be cause for additional monitoring or investigations.
Behavior Profiling

- Primarily IA detectable suspicious activities related to hacking, masquerading, compromised credentials, exfiltration, bad behavior, etc.
  - Use case examples compiled and published by NSA
    - Potentially detectable in near real time through audit data sequence analysis or other means
  - Biometric analysis of keyboard profiling or mouse movements
  - Multiple trusted remote login detection of compromised credentials

In the SIGINT World

- Protecting data isn’t always the problem.
- Sometimes it’s the software and capabilities that need protecting.
  - In the tactical data collection world, is the user the same as the remote user who initially logged on?
  - What happens if a trusted user is logged on and the system is suddenly compromised by an untrusted insider with malicious intent?

Slide Notes:
SIGINT support in the tactical environment has come into focus in recent times. Say you have an intelligence collection activity going on in a remote vehicle and the vehicle is compromised. What can you do to determine if the remote user is still the same as the individual who logged on to the system, particularly when you may not be in real time contact with the system?
Slide Notes:
In conclusion, I have a couple of last comments to make. I disagree with those who continue to say the problem is not well understood. The problem is understood just not easy solutions.

Some continue to say data on insider attacks is difficult to obtain. There are massive amounts of information available on what happened and how it happened. Even the existing SOAR spent considerable time proving this. I personally think quality time on the next SOAR should be spent to focus areas for research and potential solutions, including the fusion of multiple technologies, and less on trying to prove that it is a problem or build new databases with examples.

Again, I thank you all for attending this workshop and let’s get to work on creating the most current and comprehensive state of the art report available on insider threats.
Security Attacks and Cyber Crime: Computing through Failures and Cyber Attacks

Dr. Zbigniew Kalbarczyk
Coordinated Science Laboratory
Department of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign
kalbarcz@illinois.edu

Outline

- Internet landscape
- Current security threats
- Examples of Real Systems and Real Threats
  - Analysis of Security Incidents in a Large Computing Organization
  - Emerging Technologies: Cloud Computing
  - Critical Infrastructure: Characterization of Resiliency of Power Grid Substation Devices
  - Industrial Espionage In Cyberspace
Slide 4.

Advanced Persistent Threats (APTs)

- **APTs do represent a real danger**
  - **Targeted attacks that** combine social engineering and malware to target individuals in companies/organizations with the objective of stealing confidential information, e.g., trade secrets or customer data
  - Often use custom-written malware and exploit zero-day vulnerabilities
  - Hard to detect
  - Highly infective
  - 42% increase in 2012 (global average per day: 116)

- **Emergence of watering hole attacks** -> recent innovation in targeted attacks

Watering Hole Attack: Injection Process

1. Attacker hacks legitimate web server and injects IFRAME in Web pages
2. User browses to legitimate Website
3. Returned Web pages contain IFRAME pointing to server hosting exploit kit

The attacker knows that victims will eventually come to the compromised server - just like a lion waiting at a watering hole


Attacks by Size of Targeted Organization

- Targeted attacks for Small Businesses (1 to 250 employees) account for 31% of all attacks
- Easy to breach defenses of small businesses
- Many small businesses have close collaboration with the attacker’s ultimate target

Threats Against Mobile Devices

• We see a proliferation of mobile devices
  - Businesses are increasingly allowing staff to “bring-your-own-device” (BYOD) to work
    • Employees use personal computers, tablets, or smartphones for work
    • Companies use consumer technology, e.g., file-sharing websites, and devices (e.g., consumer laptops or tablets) to reduce costs

• A greater risk to businesses from mobile devices
  - Often lack security features, e.g., encryption, access control, and manageability
  - Easier to harvest users’ credentials


Mobile Threats

• Significant increase in mobile malware (58%) and vulnerabilities (32%)

• Android (72% market) dominates the malware 97% of new threats

• iOS (14% market) dominates the vulnerabilities
  - with 93% of those published

• Example mobile phone attacks:
  - Privacy leaks that disclose personal information
  - Mobile botnets
  - Premium number fraud where malicious apps send expensive text messages
    • One mobile botnet could generated $0.5 to $3.2 millions per year

Spam, Phishing, Malware Activity Trends

• Email spam in 2012 dropped to 69% of all email (from 75% in 2011)
  - Still global spam volume was about 30 billion spam emails per day

• Email phishing in 2012 dropped to one in 414 emails (from one in 299 in 2011)
  - Attacker change the tactics and use more other forms of online communications, e.g., social networking

• One in 291 emails contained a virus in 2012 (from one in 239 in 2011)
  - 23% contained URLs to malicious websites


Examples of Real Systems and Real Threats
Analysis of Security Incidents in a Large Computing Organization

Magnitude of the Problems: Five-Minute Snapshot of In-and-Out Traffic within NCSA

(a) (b)
Key Problem: Credentials Stealing Attacks

- Nearly 26% (32/124) of the incidents analyzed involved credentials stealing.
- 31 out of 32 incidents attackers came into the system with a valid credential of an NCSA user account:
  - Attackers rely on their access to an external repository of valid credentials to harvest more credentials.
  - Availability of valid credentials makes boundary protections (e.g., reliance only on a firewall) insufficient for this type of attacks.
  - More scrutiny in monitoring user actions needed.

Incident Distribution
(124 real Incidents + 26 investigations)

- Majority of incidents (55% out of 124 real incidents) are due to attacks on authentication mechanisms:
  - e.g., bruteforce ssh, credentials compromise, application/webserver compromise.
- 24% of investigations with no compromises:
  - These are not false positive alerts, rather credible alerts which could not be discarded until fully investigated.

27% of incidents went undetected.
Conclusions

- In-depth security data analysis can help to characterize detection capabilities of security monitoring system
- No single available tool can perform the kind of analysis needed
- Need to correlate:
  - data from different monitors
  - system logs
  - human expertise
- Need to develop techniques to pre-empt an attacker actions
  - potentially let the attacker to progress under *probation* (or tight scrutiny) until the real intentions are clear

Emerging Technologies: Cloud Computing
Cloud Computing Layered Architecture

- **Physical resources** - desktop machines, clusters and datacenters
- **Core middleware** - manages physical infrastructure and provides run time environment for applications
- Core middleware relies on *virtualization technologies* to provide advanced services, e.g., such as application isolation, quality of service, and sandboxing
- **User level middleware** - provides access to services delivered by the core middleware

Cloud Computing - Growing Interest vs. Security Problems

- Jul’08 - Spammers set up mail spamming instances in the Amazon’s EC2 cloud.
- Sep’10 - Google Engineer Stalked Teens, Spied on Chats
- Apr’09 - Texas datacenters operations are suspended for FBI investigation.
- Dec’10 - Microsoft BPOS cloud service hit with data breach
- Nov’09 - Side channel attack of Amazon’s EC2 service.
- June’11 - Dropbox: Authentication Bug Left Cloud Storage Accounts Wide Open
- Dec’09 - Zeus crime-ware using Amazon’s EC2 as command and control server.
- Dec’10 - Anonymous hacker group failed to take down Amazon
Cloud Computing - Growing Interest vs. Growing Number of Outages

- Providing a higher level of availability and security is one of the biggest challenges of Cloud computing.

Critical Infrastructure: Characterization of Resiliency of Power Grid Substation Devices
Motivation and Objective

• Power grid is a crucial infrastructure where a failure could have catastrophic impact on each citizen and on the society as a whole

• Use of IEDs (Intelligent Electronic Device) in substations to monitor the power grid and communicate between the control centers and substations makes this infrastructure vulnerable to malicious attacks and transient errors

• Objective: Characterize consequences of errors (due to accidental events and/or malicious attacks) in power substation devices

Slide Notes:
Before we go into our evaluation, let’s first talk about why we want to do this. As we know, power grid is a crucial infrastructure. So an error might have some serious impact on everyone in the society. For example, a blackout can cause millions of loss for some company and also cause some inconvenience for every citizen. Also, a failure may also have cascading effect. So one failure may cause another failure. For example, if one transmission line is overloaded and thus cause the breaker to be open, it might cause other transmission lines to be overloaded.

And nowadays we use a lot of intelligence electronic device in substations to control and monitor the power grid. They are also responsible for communicating between control center and substations. However, this kind of computer-based devices face the same problem that every computer-based device will face. That is, they are vulnerable to transient errors and malicious attacks. By transient errors, I mean the state of the device is changed due to the physical environment such as changing temperature or exposed to cosmic rays. For example, if one electron in the air hit the semiconductor, it will cause the state of the semiconductor to change from 0 to 1 or from 1 to 0. We call this situation accidental errors. And also, all computers suffer from malicious attacks. Since we need to connect these devices to network, attacker can come to subvert your devices.
Here I list two of top 10 vulnerabilities in the control system to show that this situation is possible to happen in the control systems. The first one shows that if you don’t maintain or scrutinize your software or system administration mechanisms well, say, you don’t constantly check the consistency of the data, then when accidental errors happen or attacker come, the error or the attack can cause your software to crash. Also, if you don’t design or implement your critical infrastructure very well, the systems are also vulnerable to accidental errors or malicious attacks.

Slide 22.

Slide Notes:
This is the testbed we create to mimic the real setup of the power grid systems. It contains three major parts, control center, substation, and field. The Data aggregator plays two important roles. One is data aggregator and the other is a gateway. It gathers data from each of the Relay. As a gateway, it’s responsible for the communication between the SCADA Master in the control center and the relay in the substation. All communications go through DNP3 Protocol, which is a protocol widely used in the utility companies in United States. The relay is used to monitor the current and voltage of some transmission lines. So the relay is connected to the field. Our field here uses the field simulator to simulate the current and the voltage of a transmission line. The relay will trip the breaker if the transmission line is overloaded to prevent the damage of power equipment. The SCADA Master in the control center has two responsibilities. One is to monitor the health status of all the substations by getting data from the data aggregator and it can also control the Relay through the data aggregator if needed. Since the data aggregator here is very important, we want to explore the consequence if transient errors or malicious attacks happen in it. So we try to inject faults into the data aggregator to see whether the power grid systems can still survive and work properly.
The Data Aggregator

- Three important applications
  - DNP3 Client
  - DNP3 Server
  - Monitor App

Use SW implemented fault/error injection to mimic the impact/consequence of errors and malicious attacks on the substation

<table>
<thead>
<tr>
<th>Processor</th>
<th>Memory</th>
<th>Storage</th>
<th>OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>PowerPC 533MHz</td>
<td>512MB DDR2 ECC</td>
<td>4GB (2GB Reserved)</td>
<td>Linux</td>
</tr>
</tbody>
</table>

**Slide Notes:**
Since the data aggregator is very important in our setting, our target device is the data aggregator. It is just an embedded device which runs Linux on it. It has a PowerPC processor. The table on the bottom shows specification of our data aggregator. There are three important applications running on the data aggregator. Here I show the relationship between these three applications. The DNP3 Client is responsible for the communication between the relay and the data aggregator. And the DNP3 Server is responsible for the communication between the SCADA Master and the data aggregator. For example, when the SCADA Master wants to send a breaker control command to the relay, it will first pass the command to the DNP3 Server. DNP3 Server then forwards the command to the DNP3 Client inside the data aggregator. And then the DNP3 Client passes the command to the Relay. And the relay execute the command to either open or close the breaker. Also, the DNP Client will gather sensor data from the relay and transmit the data back in similar but reverse path.
Key Findings: Silent Data Corruption

- Silent Data Corruption (SDC) is the **most severe outcome** for applications (given an error 13% for DNP3 Client, 7% for DNP3 Server)

- For example, SDC in DNP3 Client
  - The control command issued by the SCADA Master cannot be successfully passed to the Relay
  - The sensor data retrieved by the SCADA Master may not be correct
  - Hard to detect *when* and *where* the failure happens

- An operator in the Control Center can lose control over the equipment in the substation
  - Lost control over the substation may result in a blackout or damage of equipment

**Slide Notes:**

Here is our outcome distribution for those 4 types of outcomes for these three applications. Not surprisingly, we can see that the application crashes dominate the outcome categories for all the applications. 57%, 54%, and 45% for dnpclient, dnpserver, and monitor_app respectively. It’s because when we inject a fault, we change the semantic of the application so it usually crashes. Even though application crash occupies a large portion of the outcome, it’s easy to recover. You can simply restart the application within one second. And that’s the job of monitor_app. But Silent Data Corruption represents the most severe outcome for all three applications because it doesn’t crash the application but the application cannot work properly. And it occupies not a small portion of the outcome. It occupies 13% for dnpclient, 7% for dnpserver, and even for the simplest application like monitor_app, it occupies 2% of outcome. I will explain more in detail about Silent data corruption in the next slide. In some cases, the injected fault will propagate the error to cause deadlocks of system resources. For example, in one case, after the fault is injected, we can use kill command to restart the corrupted application because there’s a deadlock in the system. And the only way to solve this problem is to reboot the system, which takes more than 20 seconds and will affect the availability of the system a lot. But this type of error only occupies 2% for dnpclient and 0.6% for the monitor_app, which is relatively small compared to SDC. So let’s talk about the impact of the SDC.
Industrial Espionage In Cyberspace: Stuxnet

- **Stuxnet** is the first publicly known malware to intend real-world damage
  - discovery disclosed in July, 2010
- Attacks industrial control systems
  - targeting mainly in Iranian uranium enrichment facility
- Modifies and hides code on Siemens PLCs (programmable logic controller) connected to frequency converters
- Contains 7 methods to propagate, 4 zero day exploits, 1 known exploit, 3 rootkits, 2 unauthorized certificates, 2 Siemens security issues

**Slide Notes:**
VirusBlokAda adding detection on June 17, 2010 and published knowledge of the threat on July 12, 2010. Frequency converters control the speed of motors.

**Slide Notes:**
Why 6 modules? With 5 modules (31 motors per module) = 155 motors. A cascade has 164 motors (centrifuges). Thus, 6 are needed (6*31 = 186) as 164 is between 155 and 186.
**Slide 27.**

**Attack Execution**

1. Initial Delivery
   - Corporate LAN

2. Network Exploits
   - Internet Etc

3. Reporting Updates

4. Bridge AirGap

5. Deliver Payload

Stuxnet copies itself to inserted removable drives. Industrial control systems are commonly programmed by a computer that is non-networked. Operators often exchange data with other computers using removable drives.

Based on L. Murchu presentation

**Slide 28.**

**Centrifuge Manipulation**

- Checks Centrifuges are operating between 807Hz and 1210Hz
- If so,
  - Spins Centrifuges up to 1410Hz
  - Spins them down to 2 Hz
  - Then back to 1064Hz

From L. Murchu presentation
Slide 29.

Success

- 1 year undiscovered - first released in June 2009
- 4 zero days vulnerabilities - first time any threat has done this
- Reliable code - professionally written code
- PLC codes appears to work
- Signed drivers - stolen certificates
- > 100,000 infected machine before discovery mostly in Iran
- IAEA report 1000 centrifuges withdrawn from service
  - ?????????

From L. Murchu presentation

Slide 30.

New Targeted Attacks

<table>
<thead>
<tr>
<th>Stuxnet Reported June 2010</th>
<th>Dequ Reported October 2011</th>
<th>Flame Reported May 2012</th>
<th>Gauss Reported August 2012</th>
</tr>
</thead>
</table>
| designed to **sabotage** an industrial process | not destructive **looks for information** useful in attacking industrial control systems | written purely for **espionage**
- collects technical diagrams for intelligence purposes: AutoCAD drawings, PDFs, and Text files
- can record audio, screenshots, keyboard activity, network traffic, Skype conversations | written for **cyber espionage campaign directed at a specific banking system**
- seems to be created by the same authors as Flame
- acquire logins for e-mail and instant messaging accounts, social networks and, accounts at certain Lebanon’s banks along with Citibank and PayPal |

From L. Murchu presentation
Conclusions: What’s Ahead?

- Targeted attacks and APTs will continue to be an issue
  - frequency and sophistication of these attacks will increase
- Malware authors and spammers will increase their use of social networking sites
- Cloud computing will require to revisit how we build and protect large computing infrastructures against malicious users
- Mobile phones and tablets will become more and more vulnerable to malware
- The insider threat will grow, as employees act intentionally - and unintentionally - to leak or steal valuable data
- The foundation for the next Stuxnet-like APT attack was established
  - Duqu, Flame, Gauss …… show somewhat scary picture

Future Growth: Computing for Societal Impact

Cloud computing infrastructure

Robust computing at low-cost, “pay-as-you-go”

Assuring security and safety of the nation
Global vigilance and Reach

Large volume of data
Phones, Sensors Smart cars

Intelligent Eco Systems:
Trustworthy, Cost effective Environment friendly

Analysis

Integration

HMI

Individuals & enterprises
Human expertise Innovations Education Research

Benefits to individuals & society
Modern health care Adaptive Power Grid Efficient transportation (air, ground, sea) Preservation of water New age agriculture
Acknowledgments

Cuong Pham
Kuan-Yu Tseng
Daniel Chen
Aashish Sharma
Ravi Iyer

Sponsors: NSF, DOE, DHS, AFRL
Boeing, IBM
The necessity for increased information sharing across organizations complicates the methods required to detect and prevent the exfiltration of sensitive data. The problem of detecting and preventing all possible data exfiltration paths has become nearly insurmountable with the changing landscape in data file formats, network protocols, and data sharing technologies.

- **Current approaches are limited by:**
  - **File Locker**
    - Files are only safe while stored in the secure folder, not if data is stored elsewhere on HD or portable media or during data transfer.
  - **DoD Encryption Wizard and Microsoft Encrypting File System**
    - Manual process that interferes with user workflow.
    - Does not protect files in transit.
  - **File Vault**
    - Data protect while computer is logged out or shut down.
Objectives

Create automated encryption service that never leaves data at rest or in transit in cleartext.

Approach the data exfiltration problem on a per-file basis at the origin of creation and provide per-file metadata to track the data files.

Perform all cryptography and policy enforcement behind the scenes and not interfere with user productivity.

LEG Architecture

- Monitors the file system for reads and writes.
- Handles encrypted/decrypted traffic between application and LEG Enterprise component.
- Communicates to LEG Enterprise processes that can read/write.
- Maintains a whitelist of applications.
- Handles cryptographic operations.
- Checks whitelisted processes from kernel driver.
- Builds header.
- Creates cryptographic keys from user certificates.
- Handles communication between Enterprise systems.
- Monitors the file system for reads and writes.
- Handles encrypted/decrypted traffic between application and LEG Enterprise component.
- Communicates to LEG Enterprise processes that can read/write.
LEG File Diagram

Current header implementation

- Users in the header will be searchable via public keys
- Each block of the header has a length and type
  - Length: length of the block
  - Type: Public key or Symmetric key

File Content

Additional Developments

CAC Capabilities
- LEG extracts:
  - CHUID: User and agency identification
  - x509 Certificates for encryption purposes
- Will be able to decrypt data with stored private keys
- Can hold up to 20 retired private keys

clipboard Restrictions
- LEG notified when user updates clipboard
- LEG receives name/dir. of active application
- Global hooks to be implemented to handle paste/print actions
LEG Demo

Certificates for encryption and decryption

- The application queries active directory for the LEG certificate.
- Authorized LEG users are given access to the certificate, unauthorized users are not.
- A random symmetric key is generated to encrypt the file.
- The certificate is used to encrypt and decrypt the symmetric key.
- The symmetric key is encrypted and stored in the header for later decryption.

LEG Driver Demo

- All file types default to “Out-of-Policy”
- “In-Policy” Files have an Application Whitelist and Graylist
  - Programs opening “In-Policy” Files are implicit deny
  - A whitelisted application may encrypt/decrypt the file
  - A graylisted application may move the “raw” file
- Explorer.exe should be universally graylisted
  - Responsible for moving, copying, zipping and accessing files

<table>
<thead>
<tr>
<th>In-Policy File Type</th>
<th>Whitelisted Apps</th>
<th>Graylisted Apps</th>
</tr>
</thead>
<tbody>
<tr>
<td>*.txt</td>
<td>Notepad</td>
<td>Explorer, Internet Explorer</td>
</tr>
<tr>
<td>*.rtf</td>
<td>Word, Wordpad</td>
<td>Explorer, Firefox</td>
</tr>
<tr>
<td>*.sd0</td>
<td>Notepad</td>
<td>Explorer, Internet Explorer</td>
</tr>
<tr>
<td>*.sd1</td>
<td>Notepad</td>
<td>Explorer, Internet Explorer</td>
</tr>
</tbody>
</table>
Slide 9.

**Commercialization Activities**

- LEG is being developed to run on Microsoft® Windows operating systems, supporting enterprise systems in both government and industry.
- Integration with existing applications may reduce time to market and ensure LEG’s diverse availability within multiple markets:
  - Considering integration with McAfee Host Based Security System (HBSS) and the McAfee Vendor Alliance.
  - Exploring partnership with Wetstone Technologies to leverage relationships with industry leading security providers.

Slide 10.

**Questions**

Thank You
“Cutting Costs or Cutting Our Throats?”

Mark D. Troutman, Ph.D.
Associate Director
Center for Infrastructure Protection/Homeland Security
George Mason University

Paul B. Losiewicz, Ph.D.
Senior Scientific Advisor
Cyber Security and Information Systems Analysis Center

15 August 2013

Overview

- Recent Events
- Technology Increases Risk from Insider Threat
- Government Resource Constraints
- Costs Incurred by Lack of Due Diligence
- Implications and Policy Responses
Recent Events

- Recent incidents of Pvt Manning and Edward Snowden highlight risk of “insider threat.”
- Snowden had classified access due to his status as a contractor, as well as advanced computer training.¹
- Employed by Booz-Allen Hamilton under contract to NSA. Previous CIA experience and an incomplete military career (left before completing Special Forces training).
- There were some questions about facts relating to his background check but Snowden was hired and granted clearance with access anyway.²
- Subsequent statements indicate Snowden sought employment in order to gain access with the intent of making public practices with which he disagreed.³

- Summary: Government agency depended on contract employee for specific skills and access, but screening failed to raise red flags regarding individual’s background and motivations

Technology Increases Risk from Insider Threat

- Computing capacity continues to increase while embedded systems proliferate.
- Operating systems gain efficiency and capability with more sensors and distributed controls linked to other operating systems.
- Infrastructure is capital intensive and expensive to operate. Efficient and cost minimizing approaches have great emphasis. SCADA systems have evolved to meet this need.
- Combination of greater computing power and reach afforded by linked information systems affords greater span of influence; asymmetric threats increase.
- Greater span of control allows fewer personnel to monitor a greater range of control systems – with lower personnel cost. Personnel costs are the highest business costs.
- Similar dynamic holds in intellectual property and knowledge management systems. Less expensive cloud storage allows for more information to be available to more collaborative processes by small to mid-size businesses
Government Resource Constraints


- DoD budget sustained $487B of cuts by end of Secretary Gates’ tenure (2011). BCA 2011 identified an additional $500B over 10 years; total could reach $1T.\(^4\)

- DoD costs for uniformed personnel have increased 57% in real terms (per person) over previous decade.\(^5\)

- Contract resources offer government an opportunity to reduce expenses and find specialty skill sets; personnel costs are the concern of the contract firm.

- US Government has greatly increased use of contracted personnel in last decade to extend its capabilities, despite directions to the contrary.

- Contract organizations have a potentially different set of incentives from the government – minimize costs. Potentially reduces resources associated with vetting and oversight. Snowden case seems to illustrate this.

Costs incurred by Lack of Due Diligence

- The Cost of Cutting Corners with Infrastructure
  - Sony fined $400K by the UK for failure to protect PII, on top of the $171M in outage losses by a hack of their interactive gaming network\(^6\)
  - PII maintained on five year old servers, non-updated software, poor security

- Cost of failure in Personnel Reliability
  - Manning’s release of diplomatic cables to WikiLeaks had "a chilling effect that will go on for some time" on foreign officials’ willingness to speak candidly to U.S.\(^7\)
  - 855 man-hours estimated by the Army to review the posted Wikileaks documents, WITH computer aided analysis\(^8\)
  - Civilian Arsonist costs the Navy $94M in direct costs and the loss of an Attack Sub\(^9\)
  - Information Technology & Innovation Foundation: Snowden may cost U.S. cloud industry $35B in losses to foreign competitors because of PRISM revelations\(^10\)

- SEC and mandatory disclosure of Cyber Self Assessment\(^11\)
  - Fines for compliance failure?
## Implications and Policy Responses?

- **Risk to intellectual property protection and innovation**
  R&D collaboration requires access to information, but greater access raises the risk of unwanted disclosure and economic damage to innovative firms, hampering economic competitiveness

- **Some policy responses?**
  - Greater resources for personnel vetting and oversight – difficult in constrained environments; Individual privacy concerns as well
  - Higher access standards – but this imposes costs on collaboration and span of control
  - Limits of access by any one individual or group – this drives up personnel costs

- **Conclusion:**
  - In a Technologically riskier environment there is greater need for new technological solutions and system responses
  - Other non-technical (e.g. cognitive) approaches to Personnel Reliability
Before we get started

Disclaimers:
- AIS employs many “Gen Y’s”
- Perceptions outlined within this presentation are not fact and are by no means meant to be interpreted as negative
- Every generation has its own perceptions
- Gen Y’s are often tech savvy, collaborative, team-oriented individuals who can help your organization in many ways, including more effectively leveraging outlets such as social media
Established in 2001, headquarters in Rome, NY
- Offices in MD, OH, CO, TX and OR
- Approx. 180 employees

Work closely with government, regional businesses and academic institutions
- Pursue development of next generation cyber security capabilities
- Recruiting and hiring

Provide government and commercial customers with cyber security technologies and services
- The Air Force Research Laboratory (AFRL) in Rome, NY is AIS's largest customer

AIS develops capabilities, analyzes data and breaks lots of ‘things,’ all focused on advancing the state of cyber security.

Research Analyst
- Responsibilities include:
  - Research and assessment of emerging cyber security trends and threats
  - Testing and validation
  - Training
- Education:
  - Bachelors degree in Cyber-Security, concentration in Computer Forensics
    - Utica College
- Military
  - Prior-service Army veteran, serving as Communications Chief and Electronics Warfare Officer (EWO)
Who is Generation Y?

- Generation Y, or Millennials, most commonly refers to persons born from 1982 through 2004
- The first generation to grow up with the internet
- Note: The assumptions about Generation Y have been taken from societal views and do not reflect everyone born during this period

Who is Generation Y?

- Society often characterizes Gen Y as being:
  - Entitled
  - Tech savvy
  - Prone to information sharing
  - Team oriented
  - Connected
  - Resourceful
  - Peer dependent
  - Multi-taskers
  - Problem solvers
- Most loved generation*

- Note: The assumptions about Generation Y have been taken from societal views and do not reflect everyone born in this generation
  - Can you tell we are nervous about making Gen Y’s upset?!!!
Many members of Generation Y grew up with their base needs met. Their participation in organizations is more likely to be driven by the top three areas of needs.

(1) Conditioned to a world of instant gratification

Examples include:
- Smart phones
- Transportation
- Credit cards
- Internet
  - Online Shopping – Amazon one-click
  - Piracy

Workplaces are not always as accommodating; Generation Y may look for shortcuts or they may self-organize to meet their needs

---

**Slide Notes:**
Generation Y grew up with the basic Physiological and Safety. Their participation in organizations is more likely to be driven by the top three areas of needs.

http://www.talentedheads.com/2013/04/04/generation-y-s-hierarchy-of-needs/

They also had “Everything at hand”.

---

**Slide Notes:**
For instance, they would rather download their own software rather than create trouble-tix with IT to install.
What is an insider threat?

- Insider threat: trusted and privileged individuals within an organization that have the opportunity for malicious action

- Examples include:
  - IT personnel
  - Finance and accounting
  - Human resources
  - Any privileged users

- 14% of all data breaches were perpetrated by insiders - a more than 10% increase from 2012 (2)

What is an insider threat?

Continued

- Insider threats can effect an organization either while employed or after employment

- An insider threat may not have malicious intentions
  - Innocent acts designed to promote productivity may actually result in the bypassing of critical security mechanisms
    - Bringing work home
    - Third party email (such as webmail)
    - File sharing (such as Dropbox)
    - Installing unapproved software on work computers or cell phones

  *This may appear to deviate from the definition of insider threat but none the less, it can still be a threat on the inside*
What is an insider threat?

Continued

- Threats may include:
  - Theft:
    - Intellectual property
    - Customer records
    - Unique operations procedures
    - Employee information
    - Sensitive information
  - Destruction:
    - Physical property
    - Digital records
  - Disruption:
    - Interruption of data or services
    - Critical communications

Generation Y in the Workforce

- Fastest growing segment of the workforce today

- Estimated 70 million entering the workforce
Slide 13.

Generation Y in the workforce

Who are Generation Y and Where Do They Fit in the Workforce?

- ambitious
  56% of expect to be in a managerial role within 3 years of starting
- competitive
  An average of 83 compete for one job
- connected
  63% are on LinkedIn, and they're using it to look for work
- mobile
  90% are willing to relocate within the UK or even overseas to land a job
- waiting for employers to impress them
  Although 75% of recent say they're proud to work for their employer, 57% expect to leave within 2 years

Slide 14.

Generation Y and security

Observations

- Information should be shared and in the open
- Utilize technologies and social media to instantly share information
- Willingness to disregard security concerns
- Ignorance to security as a whole
Information sharing
And here’s why…

- Generation Y’s are connected through:
  - Twitter
  - Facebook
  - Instant messaging
  - Texting
  - Google plus
  - Email
  - Instagram
  - Vine
  - Youtube
  - Pintrest
  - Tumblr

And here’s why…

Generation Y
Security averse (4)

THE FUTURE OF WORK: SECURITY EXPECTATIONS, DEMANDS, AND BEHAVIOR OF THE WORLD’S NEXT-GENERATION WORKFORCE

ADHERING TO IT POLICIES

70% (7 of 10) OF EMPLOYEES ADMITTED TO BREAKING POLICY WITH VARYING REGULARITY

61% (>3 of 5) OF EMPLOYEES BELIEVE THEY ARE NOT RESPONSIBLE FOR PROTECTING INFORMATION ON DEVICES

80% (4 of 5) OF EMPLOYEES SAID THEIR COMPANY’S IT POLICY ON SOCIAL MEDIA AND DEVICE USAGE POLICY WAS OUTDATED — IF SUCH A POLICY EXISTED AT ALL (4)

Source: 2017 Cisco Connected World Technology Report
Security averse

- 71% of Generation Y polled said that they are not careful when posting or accessing online information
- Poll also showed that Generation Y regularly engages in risky activity at home and work, such as:
  - File sharing
  - Not logging out of computers, email, and social media
  - Downloading “warez” from illegal sites
  - Responding to pop-up ads
  - Enter online contests/promotions
- Most also post their personal information (phone number, address, place of work . . . ) on publicly available sites (5)

Security ignorance

- 71% of Generation Y’s reported that they don’t obey IT security policies (6)
- Generation Y undervalues personal data including personally identifiable information (PII) (7)
- A study performed by ZoneAlarm showed that Generation Y is the most at risk group prone to online security threats (8)
The popularity of smartphones as an extension of the office is growing across all generations, but none so much as generation Y.

But what else is on that smartphone?

Android app malware is up 40% in 2013 (9).

---

Leaked classified information to the site Wikileaks - believed to be the largest disclosure of classified material in US history. Convicted on 5 accounts of espionage.

Prior to the Wikileaks disclosure, PFC Manning was disciplined for disclosing a video of his training on YouTube.
Real world examples

**WikiLeaks**

Wikileaks founder Julian Assange’s fame stems from publicly posting countless leaked documents provided by insiders.

**Edward Snowden**

Allegedly leaked classified information gathered from the NSA including a surveillance program (PRISM) that intercepted communication information of US and European civilians.
Real world examples
US Army

Soldiers have historically put themselves and others at risk by communicating their location and activities online (10)

Enemy combatants have historically leveraged this activity

What can be done?
Mitigating the insider threat

- Generation Y is a tech-savvy, fast moving, intelligent group with unlimited potential
  - Avoidance is not an option

- Blocking access to applications and websites is also not a good option
  - Recently, the US Army embraced social media use on the NIPRNet.
  - Announcement was made via a tweet

Slide Notes:
We mean to paint a bleak image of Generation Y. Their skills and expertise are an asset, but these flaws must be pointed out.
What can be done?

- Educate them and work with them
  - Their knowledge of information outlets can be a valuable asset if utilized correctly
- Ensure security policies are briefed upon hiring and briefed again on a scheduled basis
- Consider limiting the use of email as a means to communicate security policies
  - Emails often get ignored
- Ensure all user accounts are disabled upon separation of employment
  - Prior employees can access an organizations’ internal network and sensitive information after separation

What can be done?

- Mold security practices to apply to Generation Y
  - Some ways this can be accomplished include creating an interactive method of briefing such as a game or video
- Consider in-person training sessions or work with Gen Y’s to help prepare delivery methods that will appeal to their senses
- Create a policy, or add to an existing one, that includes proper use of smartphones, tablets, and other personally owned technology
**References**

12. [http://faculty.mwsu.edu/psychology/dave.carlston/Writing%20in%20Psychology/Academic%20Dishonesty/new/adnurs2.pdf](http://faculty.mwsu.edu/psychology/dave.carlston/Writing%20in%20Psychology/Academic%20Dishonesty/new/adnurs2.pdf)

---

**Questions**

**Recap**

- Generation Y is quickly filling the ranks of corporate America
- Their connected nature and technical prowess make them both an asset and a liability
- Understanding their motivations and tailoring security education to Generation Y will help ensure adherence to security practices
- Educate them and let them educate you
  - Your business can benefit greatly
Thank you for your time

Presenter: Richard Cook
Assistant Engineer
cookr@ainfosec.com
315.336.3306 x445

Assured Information Security (AIS)
153 Brooks Road
Rome, NY 13441

www.ainfosec.com
CSIAC is a DoD Information Analysis Center (IAC) sponsored by the Defense Technical Information Center (DTIC).

Presentation to: Insider Threat SOAR Workshop

Dr. Paul B. Paul Losiewicz
Senior Scientific Advisor
Cyber Security and Information Systems Information Analysis Center

15 August 2013
Technology Increases Risk from Insider Threat

- Computing capacity continues to increase while embedded systems proliferate.
- Operating systems gain efficiency and capability with more sensors and distributed controls linked to other operating systems.
- Infrastructure is capital intensive and expensive to operate. Efficient and cost minimizing approaches have great emphasis. SCADA systems have evolved to meet this need.
- Combination of greater computing power and reach afforded by linked information systems affords greater span of influence; asymmetric threats increase.
- Greater span of control allows fewer personnel to monitor a greater range of control systems – with lower personnel cost. Personnel costs are the highest business costs.
- Similar dynamic holds in intellectual property and knowledge management systems. Less expensive cloud storage allows for more information to be available to more collaborative processes by small to mid-size businesses.

Recent High Level R&D topics

- **Critical Infrastructure Security and Resilience (CISR)**
  - CSIAC input to Department of Homeland Security (DHS) EO13636/PPD-21 R&D WG
  - Problems of complex system interdependencies must be adequately researched at the basic research level
  - Cross-domain interfaces and influences must be thoroughly understood, represented and modeled at the applied research level
  - Well-defined metrics must be appropriated from, and shared across, multiple domains and CI Sectors, to include Human Systems Interactions

- **8 Aug - NSA plans to eliminate 90% of Sys Admins using smart networks**
  - "Using technology to automate much of the work now done by employees and contractors would make the NSA's networks "more defensible and more secure," as well as faster"
  - "These efforts pre-date Snowden's leaks, the agency has said, but have since been accelerated."
Recent R&D initiatives

- **Insider Threat Identification** (Network Anomaly Detection)
  - Chief Information Officer/Defense Information Systems Agency (CIO/DISA) CIO_DISA-13-BAA-RIF-0001
  - Demonstrate the ability to analyze trends, patterns and other relevant data to identify insider threats that exist on DoD networks.

- **SBIR N132-132: Cognitive Modeling for Cyber Defense**
  - Develop and validate a computational model of the cognitive processes from cues to actions of the attackers, defenders, and users to create a synthetic experimentation capability to examine, explore, and assess effectiveness of cyber operations.
  - But has **NOT** yet been extended to Insider Threat profiles

Implications and Policy Responses?

- Technologically riskier environments require new solutions
  - New system monitoring, data mining, and anomaly detection methods are being pursued

- Risk to Privacy by Big Data Mining and Cognitive Modeling?
  - Congressional and public opinion divided post-Snowden, regardless of recent Administration defense of bulk data collection under Section 215 of the USA Patriot Act
  - Greater transparency vs. improving threat detection a challenge

- Cognitive (Smart) Networks development accelerated
  - will require corresponding advances in Secure Hardware and Protocols
  - may require advances in distributed High Performance Computing and Modeling and Simulation for Test and Evaluation before fielding

- New anomaly detection and cognitive approaches in Personnel Reliability need investigation
  - E.g. “Is Steganography and Steganalysis useful as a deterrent?”
Best Practices in Insider Threat Mitigation Presentation

Slide 1.

Best Practices in Insider Threat Mitigation

CSIAC Insider Threat Workshop

Randall Trzeciak

15 August 2013

http://www.cert.org/insider_threat/

Slide 2.

Notices

© 2013 Carnegie Mellon University

Except for the U.S. government purposes described below, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

This material was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The U.S. government's rights to use, modify, reproduce, release, perform, display, or disclose this material are restricted by the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Alternate I) contained in the above identified contract. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this slide.

Although the rights granted by contract do not require course attendance to use this material for U.S. government purposes, the SEI recommends attendance to ensure proper understanding.

THE MATERIAL IS PROVIDED ON AN "AS IS" BASIS, AND CARNEGIE MELLON DISCLAIMS ANY AND ALL WARRANTIES, IMPLIED OR OTHERWISE (INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, RESULTS OBTAINED FROM USE OF THE MATERIAL, MERCHANTABILITY, AND/OR NON-INFRINGEMENT).

CERT ® is a registered mark owned by Carnegie Mellon University.
What is CERT?

Center of Internet security expertise

Established in 1988 by the US Department of Defense on the heels of the Morris worm that created havoc on the ARPANET, the precursor to what is the Internet today

Located in the Software Engineering Institute (SEI)
• Federally Funded Research & Development Center (FFRDC)
• Operated by Carnegie Mellon University (Pittsburgh, Pennsylvania)

What is the CERT Insider Threat Center?

Center of insider threat expertise

Began working in this area in 2001 with the U.S. Secret Service

Our mission: The CERT Insider Threat Center conducts empirical research and analysis to develop & transition socio-technical solutions to combat insider cyber threats.
Goal for an Insider Threat Program

Opportunities for prevention, detection, and response for an insider incident

CERT’s Unique Approach to the Problem

Research Models

Deriving Candidate Controls and Indicators

Our lab transforms that into this…

Splunk Query Name: Last 30 Days - Possible Theft of IP
Terms: 'host=HECTOR [search host="zeus.corp.merit.lab" Message="A user account was disabled. ** | eval Account_Name=mvindex(Account_Name, -1) | fields Account_Name | strcat Account_Name "@corp.merit.lab" sender_address | fields - Account_Name] total_bytes > 50000 AND recipient_address="*corp.merit.lab" starttdaysago=30 | fields client_ip, sender_address, recipient_address, message_subject, total_bytes'
The Insider Threat

There is not one “type” of insider threat
  • Threat is to an organization’s critical assets
    • People
    • Information
    • Technology
    • Facilities
  • Based on the motive(s) of the insider
  • Impact is to Confidentiality, Availability, Integrity

There is not one solution for addressing the insider threat
  • Technology alone may not be the most effective way to prevent and/or detect an incident perpetrated by a trusted insider

Separate the “Target” from the “Impact” from the “Actor”

<table>
<thead>
<tr>
<th>Target</th>
<th>Impact</th>
<th>Actor(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical Assets</td>
<td>Confidentiality</td>
<td>Employees</td>
</tr>
<tr>
<td></td>
<td>Availability</td>
<td>• Current</td>
</tr>
<tr>
<td></td>
<td>Integrity</td>
<td>• Former</td>
</tr>
<tr>
<td>WHAT</td>
<td>HOW</td>
<td>Contractors</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Subcontractors</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Suppliers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Trusted Business Partners</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
What is a Malicious Insider Threat?

Current or former employee, contractor, or other business partner who
- has or had authorized access to an organization’s network, system or data and
- intentionally exceeded or misused that access in a manner that
- negatively affected the confidentiality, integrity, or availability of the organization’s information or information systems.

What is an Unintentional Insider Threat?

Current or former employee, contractor, or other business partner who
- who has or had authorized access to an organization’s network, system, or data and who, through
- their action/inaction without malicious intent
- cause harm or substantially increase the probability of future serious harm to the confidentiality, integrity, or availability of the organization’s information or information systems.
### Types of Insider Crimes

<table>
<thead>
<tr>
<th><strong>Insider IT sabotage</strong></th>
<th>An insider’s use of IT to direct specific harm at an organization or an individual.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Insider theft of intellectual property (IP)</strong></td>
<td>An insider’s use of IT to steal intellectual property from the organization. This category includes industrial espionage involving insiders.</td>
</tr>
<tr>
<td><strong>Insider fraud</strong></td>
<td>An insider’s use of IT for the unauthorized modification, addition, or deletion of an organization’s data (not programs or systems) for personal gain, or theft of information which leads to fraud (identity theft, credit card fraud).</td>
</tr>
<tr>
<td><strong>National Security Espionage</strong></td>
<td>The act of stealing and delivering, or attempting to deliver, information pertaining to the national defense of the United States to agents or subjects of foreign countries, with intent or reason to believe that is to be used to the injury of the United States or to the advantage of a foreign nation.</td>
</tr>
</tbody>
</table>

### Insider Crime Profiles
TRUE STORY:

SCADA systems for an oil-exploration company is temporarily disabled…

A contractor, who’s request for permanent employment was rejected, planted malicious code following termination
Other Cases of IT Sabotage

Financial Institution customers lose all access to their money from Friday night through Monday

- Fired system administrator sabotages systems on his way out

A subcontractor at an energy management facility breaks the glass enclosing the emergency power button, then shuts down computers that regulate the exchange of electricity between power grids, even though his own employer had disabled his access to their own facility following a dispute.

- Impact: Internal power outage; Shutdown of electricity between the power grids in the US.

Former employee of auto dealer modified vehicle control system after being laid off

- Searched for known customers and sent out unwarranted signals to vehicle control devices…disabled ignitions and set off alarms

A security guard at a U.S. hospital, after submitting resignation notice, obtained physical access to computer rooms

- Installed malicious code on hospital computers, accessed patient medical records

Summary of Insider Threats

<table>
<thead>
<tr>
<th>Current or former employee?</th>
<th>Former</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type of position</td>
<td>Technical (e.g. sys admins, programmers, or DBAs)</td>
</tr>
<tr>
<td>Gender</td>
<td>Male</td>
</tr>
<tr>
<td>Target</td>
<td>Network, systems, or data</td>
</tr>
<tr>
<td>Access used</td>
<td>Unauthorized</td>
</tr>
<tr>
<td>When</td>
<td>Outside normal working hours</td>
</tr>
<tr>
<td>Where</td>
<td>Remote access</td>
</tr>
</tbody>
</table>
TRUE STORY:

An undercover agent who claims to be on the “No Fly list” buys a fake drivers license from a ring of DMV employees...

The 7 person identity theft ring consisted of 7 employees who sold more than 200 fake licenses for more than $1 Million.
Other Cases of Fraud

An accounts payable clerk, over a period of 3 years, issued 127 unauthorized checks to herself and others...

- Checks totaled over $875,000

A front desk office coordinator stole PII from hospital...

- Over 1100 victims and over $2.8 M in fraudulent claims

A database administrator at major US Insurance Co. downloaded 60,000 employee records onto removable and solicited bids for sale over the Internet

An office manager for a trucking firm fraudulently puts her husband on the payroll for weekly payouts, and erases records of payments...

- Over almost a year loss of over $100K

Summary of Insider Threats

<table>
<thead>
<tr>
<th>Current or former employee?</th>
<th>IT Sabotage</th>
<th>Fraud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current employee?</td>
<td>Former</td>
<td>Current</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type of position</th>
<th>IT Sabotage</th>
<th>Fraud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical (e.g. sys admins, programmers, or DBAs)</td>
<td>Non-technical (e.g. data entry, customer service) or their managers</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Gender</th>
<th>IT Sabotage</th>
<th>Fraud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Male</td>
<td>Fairly equally split between male and female</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Target</th>
<th>IT Sabotage</th>
<th>Fraud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network, systems, or data</td>
<td>PII or Customer Information</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Access used</th>
<th>IT Sabotage</th>
<th>Fraud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized</td>
<td>Authorized</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>When</th>
<th>IT Sabotage</th>
<th>Fraud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outside normal working hours</td>
<td>During normal working hours</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Where</th>
<th>IT Sabotage</th>
<th>Fraud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote access</td>
<td>At work</td>
<td></td>
</tr>
</tbody>
</table>
Theft of Intellectual Property

TRUE STORY:
Research scientist downloads 38,000 documents containing his company’s trade secrets before going to work for a competitor…

Information was valued at $400 Million
Other Cases of Theft of IP

A technical operations associate at a pharmaceutical company downloads 65 GB of information, including 1300 confidential and proprietary documents, intending to start a competing company, in a foreign country…

- Organization spent over $500M in development costs

Simulation software for the reactor control room in a US nuclear power plant was being run from outside the US…

- A former software engineer born in that country took it with him when he left the company.

Summary of Insider Threats

<table>
<thead>
<tr>
<th>Current or former employee?</th>
<th>IT Sabotage</th>
<th>Fraud</th>
<th>Theft of Intellectual Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>Former</td>
<td>Former</td>
<td>Current</td>
<td>Current (within 30 days of resignation)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type of position</th>
<th>IT Sabotage</th>
<th>Fraud</th>
<th>Theft of Intellectual Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical (e.g. sys admins, programmers, or DBAs)</td>
<td>Technical (e.g. scientists, programmers, engineers) or sales</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Non-technical (e.g. data entry, customer service) or their managers</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Gender</th>
<th>IT Sabotage</th>
<th>Fraud</th>
<th>Theft of Intellectual Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>Male</td>
<td>Male</td>
<td>Fairly equally split between male and female</td>
<td>Male</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Target</th>
<th>IT Sabotage</th>
<th>Fraud</th>
<th>Theft of Intellectual Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network, systems, or data</td>
<td>PII or Customer Information</td>
<td>IP (trade secrets) –or customer info</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Access used</th>
<th>IT Sabotage</th>
<th>Fraud</th>
<th>Theft of Intellectual Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized</td>
<td>Unauthorized</td>
<td>Authorized</td>
<td>Authorized</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>When</th>
<th>IT Sabotage</th>
<th>Fraud</th>
<th>Theft of Intellectual Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outside normal working hours</td>
<td>During normal working hours</td>
<td>During normal working hours</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Where</th>
<th>IT Sabotage</th>
<th>Fraud</th>
<th>Theft of Intellectual Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote access</td>
<td>At work</td>
<td>At work</td>
<td></td>
</tr>
</tbody>
</table>
Mitigation Strategies

Our Suggestion

- Continuous Logging
- Targeted Monitoring
- Real-time Alerting

No Insider Threat
Slide 27.

Common Sense Guide to Mitigating Insider Threats

http://www.sei.cmu.edu/library/abstracts/reports/12tr012.cfm

Slide 28.

Best Practices for Insider Threat Mitigation

- Consider threats from insiders and business partners in enterprise-wide risk assessments.
- Clearly document and consistently enforce policies and controls.
- Incorporate insider threat awareness into periodic security training for all employees.
- Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.
- Anticipate and manage negative issues in the work environment.
- Know your assets.
- Implement strict password and account management policies and practices.
- Enforce separation of duties and least privilege.
- Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.
- Institute stringent access controls and monitoring policies on privileged users.
- Institutionalize system change controls.
- Use a log correlation engine or security information and event management (SIEM) system to log, monitor, and audit employee actions.
- Monitor and control remote access from all endpoints, including mobile devices.
- Develop a comprehensive employee termination procedure.
- Implement secure backup and recovery processes.
- Develop a formalized insider threat program.
- Establish a baseline of normal network device behavior.
- Be especially vigilant regarding social media.
- Close the doors to unauthorized data exfiltration.
The CERT Top 10 List for Winning the Battle Against Insider Threats

1. Create an Insider threat program NOW!
2. Work together across the organization
3. Address employee privacy issues with General Counsel
4. Pay close attention at resignation/termination
5. Educate employees regarding potential recruitment
6. Recognize concerning behaviors as a potential indicator
7. Mitigate threats from trusted business partners
8. Use your current technologies differently
9. Focus on protecting the “crown jewels”
10. Learn from past incidents

CERT’s Insider Threat Services
Insider Threat Assessment (ITA)

**Objective:** To measure an organization’s level of preparedness to address insider threats to their organization.

**Method:** Document Review, Process Observation, and Onsite interviews using insider threat assessment workbooks based on all insider threat cases in the CERT case library.

**Outcome:** Confidential report of findings with findings and recommendations.

**Areas of Focus:** Information Technology/Security; Software Engineering; Data Owners; Human Resources; Physical Security; Legal / Contracting; Trusted Business Partners.

---

CERT Insider Threat Workshops

**Goal:** participants leave with actionable steps they can take to better manage the risk of insider threat in their organization

½ day, One day, Two days - Presentations and interactive exercises

Addresses technical, organizational, personnel, security, and process issues

Exercises

- Address portions of the insider threat assessment
- Purpose: assist participants in assessing their own organization's vulnerability to insider threat in specific areas of concern
Building an Insider Threat Program

**Goal:** CERT staff work with senior executives from across the organization to develop a strategic action plan, based on actual cases of insider threats at the participating organization and research by CERT staff, to address and mitigate the risk of insider threat at the organization.

- Key differences from standard workshop
  - Tailored course material based on actual insider incidents at the organization.
    - Cases are provided in advance by the organization, and treated with strict confidentiality.
    - Workshop is preceded by a 3-day onsite by CERT staff to work with the organization’s staff to familiarize themselves with the provided case material.
  - Second day of workshop CERT staff and executives work together to create the Organization’s strategic plan for preventing, detecting and responding to insider threats.

CERT Resources

- Insider Threat Center website (http://www.cert.org/insider_threat/)
- Common Sense Guide to Mitigating Insider Threats, 4th Ed. (http://www.sei.cmu.edu/library/abstracts/reports/12tr012.cfm)
- Insider threat workshops
- Insider threat assessments
- New controls from CERT Insider Threat Lab
- Insider threat exercises

The CERT® Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud) (SEI Series in Software Engineering) by Dawn M. Cappelli, Andrew P. Moore and Randall F. Trzeciak
Point of Contact

Insider Threat Technical Manager
Randall F. Trzeciak
CERT Program
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-3890
+1 412 268-7040 – Phone
rft@cert.org – Email

http://www.cert.org/insider_threat/