Whitepaper Insider Threat: Policy Impact and Overview Center for Infrastructure Protection and Homeland Security George Mason University School of Law

Christopher Woolley, JD Mark D. Troutman, PhD

Cyber Security and Information Systems Information Analysis Center

Dr. Paul B. Losiewicz, Senior Scientific Advisor Draft: 19 June, 2014

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 moentary 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 recent 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."¹ 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 or information systems."² The SEI-CERT definitions and criteria will define what constitutes threat for this work.

1. 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, <u>https://www.cert.org/insider-threat/</u>

² Unintentional Insider Threats: The Non-Malicious Within, <u>https://www.cert.org/blogs/insider-threat/post.cfm?EntryID=169</u>

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,³ though the available evidence does not support this claim.⁴ 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."⁵ Whether or not he would have been protected at the time is still somewhat unclear, a fact which in itself is an issue. In a recent interview, Snowden proposed that the laws should apply to contractors and should "distinguish between people who sell secrets to foreign governments for their own gain and people who return information to public hands for the purpose of serving the public interest"⁶ This ultimately shows that when he believed the avenues of recourse were insufficient to provide redress, Snowden chose to provoke change by making restricted information public, ignoring his own understanding of law in favor of his ideas of what the law should be.

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.

³ Snowden's testimony before the EU Parliament, source:

http://www.europarl.europa.eu/document/activities/cont/201403/20140307ATT80674/20140307ATT80674EN. pdf

⁴ Jake Miller, "Edward Snowden didn't email surveillance concerns: Officials," *CBS News* (May 29, 2014). <u>http://www.cbsnews.com/news/edward-snowden-didnt-email-surveillance-concerns-officials/</u>

⁵ Snowden Testimony, 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.

⁶ Matthew Cole, Richad Esposito, Bill Dedman, and Mark Schone, "Edward Snowden's Motive Revealed: He Can 'Sleep at Night," NBC News (May 28, 2014). <u>http://www.nbcnews.com/feature/edward-snowdeninterview/edward-snowdens-motive-revealed-he-can-sleep-night-n116851</u>

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 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.

2. 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.⁷ 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.⁸ 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.

3. 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.⁹ 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

⁷ Insider Threat: Soldier Receives 16-year Sentence for Attempted Espionage, Federal Bureau of Investigation, http://www.fbi.gov/news/stories/2013/april/soldier-receives-16-year-sentence-for-attempted-espionage

⁸ Two Individuals and Company Found Guilty of Conspiracy to Sell Trade Secrets to Chinese Companies, Department of Justice, <u>http://www.justice.gov/opa/pr/2014/March/14-nsd-232.html</u>, referencing U.S. v. Liew

⁹ *IRS Employee Takes home Thumb Drive with Data on 20,000 colleagues*, Bloomberg News, <u>http://www.bloomberg.com/news/2014-03-18/irs-employee-took-home-data-on-20-000-workers-at-agency.html</u>

4. 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 Summary¹⁰:

- 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 actions¹¹:

- 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.
- 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 DoDComponents 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.

The Personnel Security Clearance Process and Personnel Security Investigations (PSI). DoD will be updating the personnel security clearance process under a forthcoming DoD Instruction 5200.02 in two parts: Volume 1, "DoD Personnel Security Program (PSP): Investigations for National Security Positions and Duties," and Volume 2, "DoD Personnel Security Program (PSP): Adjudications, Due Process, Continuous Evaluation, and Security Education." Anticipated changes include harmonization with the Federal Investigative Standards (FIS) revisions of December 2012 which will require:

¹⁰ Internal Review of the Washington Navy Yard Shooting, Under Secretary of Defense for Intelligence, Nov 20 2013, p.4.

¹¹ Ibid. p.5

"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."¹²

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.

Information System Vulnerability and Mitigation. 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 soon.

5. 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 8510.01.¹³ 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..."¹⁴

¹² Ibid. p.13

¹³ Risk Management Framework (RMF) for DoD Information Technology (IT) DoDI 8510.01 12 March 2014, p.3.

¹⁴ Ibid., p.37.

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 (RFM) for DoD Information Technology¹⁵. 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."¹⁶

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 information system = {(confidentiality, impact), (integrity, impact), (availability, impact)}¹⁷

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.¹⁸

6. 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

¹⁵ Ibid.

¹⁶ NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, p.xv, , <u>http://dx.doi.org/10.6028/NIST.SP.800-53r4</u>

¹⁷ Ibid, p.28.

¹⁸ Keynote Address at the 2013 Billington Cyber Security Conference, General Keith Alexander, September 25, 2013.

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.

7. Executive Order 13587.¹⁹ 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"²⁰ 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.²¹ 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 and technology to detect and reduce threats. For example, the Department of Defense recently submitted a solicitation for contractors to develop better forms of protecting, sharing, and storing classified information.²²

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

8. 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

¹⁹ Executive Order 13587, Oct. 7, 2011.

²⁰ Ibid.

²¹ Specifically, the National Insider Threat Policy, which defines standards from EO 13587 bounded by Executive Orders 12968 and 13526, available at <u>http://www.fas.org/sgp/obama/insider.pdf</u>.

²² For Government, a Long Road to Stopping Insider Threats, USA Today, Dec. 6, 2013, <u>http://www.usatoday.com/story/nation/2013/12/06/internal-security-threats-pentagon/3888993/.</u>

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.²³

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.²⁴ 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.²⁵ More recently, Chelsea (then Bradley) Manning leaked thousands of classified documents to the press, and was found guilty under the Espionage Act.²⁶

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.²⁷ 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.²⁸ It has been used against civilians or civilian entities with access to confidential or damaging information,²⁹ but more often it has been used against military personnel.

9. 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.³⁰

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

²³ 18 U.S.C. §§792, 793.

²⁵ United States v. Morison 844 F.2d 1057, (4th Cir. 1988).

²⁴ 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.

²⁶ Verdict in Bradley Manning Case, Washington Post, August 21, 2013, <u>http://www.washingtonpost.com/wp-srv/special/national/manning-verdict/?hpid=z1</u>.

²⁷ 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 dropped before conviction, including *U.S. v. Drake*, 818 F.Supp.2d 909 (D. Md. 2011) and *Liebowitz*. Several are still ongoing, including *United States v. Sterling*, No. 11-5028 (2013).

²⁸ 18 U.S.C. §792, 793.

²⁹ 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.

³⁰ United States v. Chung, 659 F.3d 815 (2011).

latter focuses on the theft of the trade secret in general, either for foreign or interstate use.³¹ 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.³² 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.³³

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 the EEA may not be used enough to serve as a deterrent for leaks.³⁴ As of 2012, only 120 cases had been brought under the EEA, a number which has not increased drastically.³⁵

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.

10. 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.³⁶ 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.³⁷ It has been used in several cases to prosecute insiders, including *Manning*.³⁸

³¹ 18 U.S.C. §§ 1831 & 1832(a), respectively.

³² Chung 631 F. 3d.

³³ United States v. Martin 228 F. 3d 1 (1st Cir. 2000).

³⁴ Analysis of Economic Espionage Act Prosecutions, Bloomberg Patent, trademark, and copyright journal, September 32, 2012, <u>http://petertoren.com/wp-content/uploads/2011/05/toren-eea2.pdf</u>.

³⁵ Ibid, since 2012, around 20 cases have been concluded or filed under the EEA. Some of those concluded were brought in years prior.

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

 ³⁷ 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).

³⁸ In re: Manning, Transcript, <u>https://pressfreedomfoundation.org/sites/default/files/07-30-13-AM-session.pdf</u>, See, *Shurgood Storage Ctrs. v. Safeguard Self Storage, Inc.*, 119 F.Supp.2d, 1121 (W.D. Wash. 2000) (denying a motion to dismiss based on the definition of exceeding access) See also *United States v. Nosal*, 2013 WL 4504652 (N.D. Cal. Aug. 15, 2013) (An ongoing case wherein a current employee gave her password to a former employee who then accessed data. The court ruled that only the employer has the right to grant access to its computer systems, not an employee).

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.³⁹ 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.

11. 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 Act,⁴⁰ 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.⁴¹

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.⁴²

12. 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

³⁹ 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).

⁴⁰ 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).

⁴¹ 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).

⁴² 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.

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.⁴³ This is a time consuming 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.

13. 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.⁴⁴ 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

⁴³ CERT estimates that in 2010, most insider threats went unnoticed by the employing company. *Interesting Insider Threat Statistics*, <u>http://www.cert.org/blogs/insider-threat/post.cfm?EntryID=60</u>.

⁴⁴ CERT 4th Common Sense Guide, SEI-CERT, 2012 <u>http://www.ncix.gov/issues/ithreat/docs/Common Sense Guide to Mitigating Insider Threats.pdf</u>.

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.⁴⁵ 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.⁴⁶ 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.⁴⁷

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.

14. 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

⁴⁵ As a contractor with Top Secret clearance, he would have gone through a personnel security investigation, including at minimum a Single Scope Background Investigation. *Internal Review of the Washington Navy Yard Shooting*, Department of Defense, 2013. <u>http://www.defense.gov/pubs/DoD-Internal-Review-of-the-WNY-Shooting-20-Nov-2013.pdf</u>.

⁴⁶ *Reflections on the Inside Threat,* Charles P. Pfleeger, the Pfleeger Group, 2007, <u>http://link.springer.com/chapter/10.1007%2F978-0-387-77322-3_2</u>.

⁴⁷ Ibid.

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.⁴⁸ 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.

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.⁴⁹ He did not feel heard, and did not believe the whistleblower protections available to government employees were available to him.⁵⁰ 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.⁵¹ However, even given the lack of legally mandated

⁴⁸ CERT 4th common sense guide, Supra Note 45.

⁴⁹ Snowden's testimony to the EU Parliament, *Supra* note.3.

⁵⁰ Generally, government employees are allowed to approach and disclose information to independent counsel within the government without fear of retributive action. The Whistleblower Protection Enhancement Act of 2012, 5 USC § 23, modifying the Whistleblower Protection act of 1989, 103 Stat. 16. With PPD 19, the Obama administration extended that protection to the intelligence community. Presidential Policy Directive 19, 2012.

⁵¹ Edward Snowden's Claim that He Had "No Proper Channels" for Protection as a Whistleblower, Washington Post, March 12, 2014, <u>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/</u>.

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 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.⁵²

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

⁵² Comments by Royht Belani, Mircon 2013, APT Mitigation, the Human Way, Nov. 6, 2013.

performance. Just like in those schemes, here a portion of compensation is connected to the organization's goal to make its information secure.

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.⁵³ 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.⁵⁴ 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

⁵³ As suggested in CSO Online's article 6 Technical Measures to Mitigate Insider Threats, <u>http://www.csoonline.com/article/2135532/network-security/6-technical-measures-to-mitigate-insider-threats.html</u>.

⁵⁴ Nuclear Weapon Personnel Reliability Program, DODD 5210.42 (Jan. 8, 2001, reissued Jul. 16, 2012)). The two person rule is discussed in Air Force Instruction 91-104, Nuclear Tamper Control and Detection Programs. The NSA has already begun implementing a similar system, NSA Implementing 'Two-Person' Rule To Stop The Next Edward Snowden, Forbes, http://www.forbes.com/sites/andygreenberg/2013/06/18/nsa-director-says-agencyimplementing-two-person-rule-to-stop-the-next-edward-snowden/

threat.⁵⁵ Rotation of teams and periodic activity reviews would strengthen the monitoring of sensitive functions.

15. "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.

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

⁵⁵ CERT offers this as one of its basic strategies for mitigating threat. <u>http://www.cert.org/blogs/insider-threat/post.cfm?EntryID=135</u>.

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.