



**NAVAL  
POSTGRADUATE  
SCHOOL**

**MONTEREY, CALIFORNIA**

**THESIS**

**THE VULNERABILITY OF SOCIAL NETWORKING  
MEDIA AND THE INSIDER THREAT:  
NEW EYES FOR BAD GUYS**

by

John J. Lenkart

September 2011

Thesis Advisor:

Chris Bellavita

Second Reader:

Robert Josefek

**Approved for public release; distribution is unlimited**

THIS PAGE INTENTIONALLY LEFT BLANK

<b>REPORT DOCUMENTATION PAGE</b>			<i>Form Approved OMB No. 0704-0188</i>
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
<b>1. AGENCY USE ONLY (Leave blank)</b>	<b>2. REPORT DATE</b> September 2011	<b>3. REPORT TYPE AND DATES COVERED</b> Master's Thesis	
<b>4. TITLE AND SUBTITLE</b> The Vulnerability of Social Networking Media and the Insider Threat: New Eyes for Bad Guys		<b>5. FUNDING NUMBERS</b>	
<b>6. AUTHOR(S)</b> John J. Lenkart		<b>8. PERFORMING ORGANIZATION REPORT NUMBER</b>	
<b>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</b> Naval Postgraduate School Monterey, CA 93943-5000		<b>10. SPONSORING/MONITORING AGENCY REPORT NUMBER</b>	
<b>9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)</b> N/A		<b>11. SUPPLEMENTARY NOTES</b> The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. government. IRB Protocol number NPS.2011.0070-IR-EP7-A.	
<b>12a. DISTRIBUTION / AVAILABILITY STATEMENT</b> Approved for public release; distribution is unlimited		<b>12b. DISTRIBUTION CODE</b> A	
<b>13. ABSTRACT (maximum 200 words)</b> Social networking media introduces a new set of vulnerabilities to protecting an organization's sensitive information. Competitors and foreign adversaries are actively targeting U.S. industry to acquire trade secrets to undercut U.S. business in the marketplace. Of primary concern in this endeavor is an insider's betrayal of an organization, witting or unwitting, by providing sensitive information to a hostile outsider that negatively impact an organization. A common existing technique to enable this breach of sensitive information is social engineering—the attempt to elicit sensitive information by obscuring the true motivation and/or identity behind the request. Social engineering, when coupled with the new and widespread use of social networking media, becomes more effective by exploiting the wealth of information found on the social networking sites. This information allows for more selective targeting of individuals with access to critical information. This thesis identifies the vulnerabilities created by social networking media and proposes a mitigation and prevention strategy that couples training and awareness with active surveys and monitoring of critical persons within an organization.			
<b>14. SUBJECT TERMS</b> Social networking media, social engineering, insider threat, Sarbanes-Oxley Act		<b>15. NUMBER OF PAGES</b> 85	
		<b>16. PRICE CODE</b>	
<b>17. SECURITY CLASSIFICATION OF REPORT</b> Unclassified	<b>18. SECURITY CLASSIFICATION OF THIS PAGE</b> Unclassified	<b>19. SECURITY CLASSIFICATION OF ABSTRACT</b> Unclassified	<b>20. LIMITATION OF ABSTRACT</b> UU

THIS PAGE INTENTIONALLY LEFT BLANK

**Approved for public release; distribution is unlimited**

**THE VULNERABILITY OF SOCIAL NETWORKING MEDIA AND THE  
INSIDER THREAT: NEW EYES FOR BAD GUYS**

John J. Lenkart  
Unit Chief, Federal Bureau of Investigation  
B.S., United States Military Academy, West Point, NY. 1990

Submitted in partial fulfillment of the  
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES  
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL  
September 2011**

Author: John J. Lenkart

Approved by: Chris Bellavita  
Thesis Advisor

Robert Josefek  
Second Reader

Harold A. Trinkunas, PhD  
Chair, National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

## **ABSTRACT**

Social networking media introduces a new set of vulnerabilities to protecting an organization's sensitive information. Competitors and foreign adversaries are actively targeting U.S. industry to acquire trade secrets to undercut U.S. business in the marketplace. Of primary concern in this endeavor is an insider's betrayal of an organization, witting or unwitting, by providing sensitive information to a hostile outsider that negatively impact an organization. A common existing technique to enable this breach of sensitive information is social engineering—the attempt to elicit sensitive information by obscuring the true motivation and/or identity behind the request. Social engineering, when coupled with the new and widespread use of social networking media, becomes more effective by exploiting the wealth of information found on the social networking sites. This information allows for more selective targeting of individuals with access to critical information. This thesis identifies the vulnerabilities created by social networking media and proposes a mitigation and prevention strategy that couples training and awareness with active surveys and monitoring of critical persons within an organization.

THIS PAGE INTENTIONALLY LEFT BLANK



# TABLE OF CONTENTS

<b>I.</b>	<b>INTRODUCTION.....</b>	<b>1</b>
<b>A.</b>	<b>PROLOGUE.....</b>	<b>1</b>
<b>B.</b>	<b>PROBLEM STATEMENT—SOCIAL NETWORKING MEDIA INCREASES VULNERABILITY.....</b>	<b>2</b>
<b>C.</b>	<b>RESEARCH QUESTION(S).....</b>	<b>7</b>
<b>D.</b>	<b>HYPOTHESIS AND TENTATIVE SOLUTIONS.....</b>	<b>7</b>
<b>E.</b>	<b>SIGNIFICANCE OF RESEARCH.....</b>	<b>7</b>
<b>F.</b>	<b>RESEARCH METHOD.....</b>	<b>8</b>
<b>G.</b>	<b>INTERVIEW RESPONDENTS.....</b>	<b>8</b>
<b>H.</b>	<b>INTERVIEW QUESTIONS.....</b>	<b>8</b>
	<b>1. General Background.....</b>	<b>9</b>
	<b>2. Social Networking Media Vulnerabilities.....</b>	<b>9</b>
	<b>3. Social Engineering and the Insider Threat.....</b>	<b>9</b>
	<b>4. Polices or Programs Regarding the Vulnerability Mitigation of Social Networking Media.....</b>	<b>9</b>
<b>II.</b>	<b>LITERATURE REVIEW.....</b>	<b>11</b>
<b>A.</b>	<b>LITERATURE THAT IDENTIFIES THE INSIDER THREAT AND THE USE OF SOCIAL NETWORKING MEDIA.....</b>	<b>12</b>
	<b>1. Summary of Social Engineering and Social Networking Media Threat Literature.....</b>	<b>16</b>
<b>B.</b>	<b>IDENTIFY SECURITY METHODOLOGIES THAT MITIGATE THE INSIDER THREAT AND THE VULNERABILITY OF SOCIAL NETWORKING MEDIA.....</b>	<b>17</b>
<b>C.</b>	<b>CONCLUSION.....</b>	<b>23</b>
<b>III.</b>	<b>RESEARCH METHODOLOGY.....</b>	<b>25</b>
<b>IV.</b>	<b>RESULTS.....</b>	<b>29</b>
<b>A.</b>	<b>GENERAL BACKGROUND.....</b>	<b>29</b>
	<b>1. What is Your Professional Background?.....</b>	<b>29</b>
	<b>2. What is Your Personal Familiarity with Social Networking Media? Which Sites, If Any, do You or Your Family Use?.....</b>	<b>29</b>
<b>B.</b>	<b>SOCIAL NETWORKING MEDIA VULNERABILITIES.....</b>	<b>30</b>
<b>C.</b>	<b>SOCIAL ENGINEERING AND THE INSIDER THREAT.....</b>	<b>35</b>
<b>D.</b>	<b>POLICES OR PROGRAMS REGARDING THE VULNERABILITY MITIGATION OF SOCIAL NETWORKING MEDIA.....</b>	<b>37</b>
<b>E.</b>	<b>SUMMARY.....</b>	<b>39</b>
<b>V.</b>	<b>CONCLUSIONS.....</b>	<b>41</b>
<b>A.</b>	<b>HOSTILE ACTOR METHODOLOGY FOR INFORMATION COLLECTION, TARGETING, AND SOCIAL ENGINEERING TO ENABLE THE INSIDER THREAT.....</b>	<b>43</b>

<b>B.</b>	<b>POTENTIAL PROGRAMS, POLICIES, AND TECHNOLOGY TO HELP LESSEN THE VULNERABILITY TO SOCIAL NETWORKING MEDIA.....</b>	<b>48</b>
<b>C.</b>	<b>LIMITATIONS AND OPPORTUNITIES FOR FURTHER RESEARCH.....</b>	<b>51</b>
<b>D.</b>	<b>SUMMARY.....</b>	<b>52</b>
<b>E.</b>	<b>EPILOGUE.....</b>	<b>53</b>
<b>APPENDIX.</b>	<b>VULNERABILITY ASSESSMENT AND RISK MITIGATION REPORT FOR JOHN Q. PUBLIC, NEXGENCF TEAM, US AEROSPACE.....</b>	<b>57</b>
	<b>LIST OF REFERENCES.....</b>	<b>61</b>
	<b>INITIAL DISTRIBUTION LIST.....</b>	<b>67</b>

## LIST OF FIGURES

Figure 1.	The Infamous “Robin Sage” (From Waterman, 2010) .....	13
Figure 2.	Steps to Exploit Social Networking Media of Information-Gathering .....	34
Figure 3.	The Vulnerabilities and Consequences of Certain Industries or Segments of an Organization (From Tailored Solutions & Consulting, 2010) .....	45
Figure 4.	Existing Threat Process to Acquire an Organization’s Insider Information....	46
Figure 5.	New Threat Process to Acquire an Organization’s Insider Information Using Information from Social Networking Media.....	47
Figure 6.	Training Creates a Barrier to the Volume and Type of Information Found on Social Networking Media .....	49
Figure 7.	Training Limits the Effectiveness of Social Engineering Techniques.....	50

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF TABLES

Table 1.	Relevant Biographical and Professional Information of the Subject Matter Experts .....	27
Table 2.	Cumulative Summary of the Expertise These Interviewees Possess .....	27
Table 3.	Summary of Types of Potential Vulnerabilities Created by Certain Features of Social Networking Media .....	31
Table 4.	Hypothetical Conversation Between a Social Engineer and the Target Individual .....	36
Table 5.	The Respondents' Organization's Insider Threat Mitigation Programs .....	37

THIS PAGE INTENTIONALLY LEFT BLANK

## **LIST OF ACRONYMS AND ABBREVIATIONS**

DHS	Department of Homeland Security
FBI	Federal Bureau of Investigation
IT	Information Technology
NPS	Naval Postgraduate School
SEC	Securities and Exchange Commission
SOX	Sarbanes-Oxley Act
SSN	Social Security Number
USSS	United States Secret Service

THIS PAGE INTENTIONALLY LEFT BLANK



## **ACKNOWLEDGMENTS**

First and foremost, I must thank my wife, Julie, for her keeping up with three children, including a newborn, during my time in this program. I know she is quite happy and relieved that this thesis is complete. I wish to acknowledge the sage and patient guidance of Chris Bellavita and Bob Josefek while they suffered through the difficult process of reading my rough drafts and disjointed musings. I need to highlight the in-depth expertise provided to me for this thesis by Jeffrey Berkin, Keith Bolcar, Matthew Doherty, Michael Gelles, Natalie Lehr-Lopez, Gabriel Whalen, and others who must remain covert; their openness and intelligence was extraordinary. Finally, I must express my gratitude to the Federal Bureau of Investigation for funding my participation in the Master's Program at the Center for Homeland Defense and Security at the Naval Postgraduate School.

THIS PAGE INTENTIONALLY LEFT BLANK

## I. INTRODUCTION

### A. PROLOGUE

After a night of drinking and some good laughs, John opened his eyes at the crack of 11:15 am. He threw on some clothes, grabbed his iPad and headed to the coffee shop up the street for a much-needed medicinal cup from the Roaster. Time to check *Facebook* to see the plan for tonight. His two-bedroom apartment lies in a trendy neighborhood in Seattle, which, like his native Chicago, is a great city for the young and single. John is enjoying life. He is three years into a good paying job and gets to work on some really interesting stuff. But being a junior engineer at a huge company like US Aerospace can be a grind; it is very “old-school” where promotions are based on seniority and not production. In spite of the decent pay, especially when compared to his 20-something friends, John is always itching for a bit more cash because skiing, dating, and a new car can tax a man’s budget and the credit cards are starting to max out.

While milling about waiting for his coffee, John catches the eye of an attractive woman wearing a Chicago Bears jersey. He thinks he might have seen her before but he is not sure. Never one to pass on a chance to chat, John compliments the woman on her fine choice of attire. As it turned out, Robin grew up near Chicago, was a big Bears fan, and seemed very friendly. She was in Seattle for a few months working as a business consultant for a small foreign company. While chatting, Robin mentioned the possibility of two free club seats for the Chicago Bears-Seattle Seahawks game that fall. They exchanged e-mail, talked a bit more, and parted ways.

John bumped into Robin again at the Roaster two weeks later. This time, they sat and talked for at least an hour. In the course of the conversation, Robin mentioned she had a software services client that was sponsoring an anonymous IT survey for better market understanding (e.g., what operating system does your company use? what version? what anti-virus; how is any sensitive data protected? what are the log-in protocols). Survey takers would get \$100 cash for about 10 minutes of effort. She was

very clear that the survey did not record any identifiers of the survey-taker. John jumped at the chance and Robin e-mailed the survey so John could record the answers at work. They agreed to meet again the following weekend.

Next week, over yet another cup of coffee, Robin examined the completed survey and paid John the \$100. She explained that her work was taking her overseas again but she was able to lock-in the two Bears tickets. The tickets were from a business client who, coincidentally, worked at a materials engineering firm. Robin told John that she would make the e-mail introduction to ensure John got the tickets. Robin promised to keep in touch and would try to make it back out to Seattle soon. John never heard from Robin again.

A year later, US Aerospace was forced to acknowledge a huge security breach in its IT system in which a hacker gained access to the secure databases housing the most sensitive advanced carbon-fiber trade secrets planned for use in the next generation of fuel-efficient passenger jets. These incredibly strong, very lightweight aircraft were to be the key to US Aerospace's market dominance for the next 10 years. In addition, it seemed one of the junior engineers, now working overseas, downloaded reams of information regarding the unique manufacturing processes for this advanced material. US Aerospace stock plummeted. It fell even further when a Chinese aircraft manufacturer debuted a small, corporate jet made entirely of a similar advanced carbon fiber. US Aerospace never fully recovered from the loss of market-changing technology worth several hundred million dollars.

## **B. PROBLEM STATEMENT—SOCIAL NETWORKING MEDIA INCREASES VULNERABILITY**

The problem I will investigate in this thesis is the examination of a potential new vulnerability to U.S. business created by the widespread use of social networking media (e.g., *Facebook*, *LinkedIn*) while exploring mitigation strategies that may decrease this threat. The immense aggregation of personal and professional data found in social networking media may be exploited by hostile actors to acquire sensitive information at the exact point of insider access to affect damaging financial consequences upon the

victim organization. Identifying an effective mitigation strategy should limit the potential unwanted access, gained by the exploit of social networking media, to an organization's sensitive or proprietary information. Prevention of this loss is critical as the theft of trade secrets and intellectual property is ongoing challenge to U.S. businesses and has a severe negative impact on the long-term health and competitiveness of the U.S. economy.

In principle, a safe and secure homeland has a positive macroeconomic effect on the U.S. economy as any systemic reduction of risk and uncertainty allows companies to become more aggressive in growing business. According to the U.S. Chamber of Commerce, "American business has a multifaceted stake in a strong national defense and a homeland security policy that safeguards Americans while also protecting their mobility, their freedom and their way of life" (U.S. Chamber of Commerce, 2010). The Department of Homeland Security's 2010 *Quadrennial Homeland Security Review Report* (QHSR) spells out quite explicitly the need for private industry to be a full partner in the homeland security community by stating:

We must secure the system of networks and information upon which our prosperity relies while promoting economic growth, protecting privacy, and securing civil liberties. Both public- and private-sector efforts are required to achieve those aims. (Department of Homeland Security [DHS], 2010b, p. 54)

National Infrastructure Advisory Council's report on the *Insider Threat to Critical Infrastructures* outlined the problem as one whose goal is to prevent terrorist attacks (Noonan & Archuleta, 2008). While preventing terrorist attacks will always be a homeland security priority, there is an ongoing and far more damaging "attack" on the U.S. economy: the theft of proprietary information and trade secrets, which helps to erode U.S. economic health.

Although the specific amount is somewhat difficult to measure, the loss from theft of intellectual property is estimated to cost the U.S. economy \$58 billion in total output, 375,000 jobs, \$16.3 billion in earnings, and \$2.6 billion in federal/state/local tax revenue *annually* (White House, 2010). And the primary threat enabling the theft of proprietary information is the deliberate actions of current and former employees (ASIS, 2007, p. 3). The insider threats exist for all organizations as a trusted employee may betray their

obligations and allegiances to their employer to conduct acts of sabotage and espionage for personal gain or revenge (Noonan & Archuleta, 2008, p. 4).

While the actions of insider threat actors are certainly criminal in nature, the exploitation of the insider threat is part of a broader international effort to acquire illegally U.S. intellectual property to gain a competitive advantage in the global marketplace. Recent court records demonstrate that countries that are economic competitors to the United States have undertaken efforts to obtain illegally western technology. American industries, beyond the traditional military and high-tech targets, risk having valuable secrets exposed by their own employees (Drew, 2010). On June 8, 2010, a former DuPont chemist pleaded guilty to trade secret theft. The chemist tried to send detailed information regarding proprietary chemical formulas and processes to China. On July 22, 2010, a former General Motors employee and her husband were arrested of providing hybrid vehicle technology to a Chinese competitor. The value of the technology was placed at \$40 million (Office of the United States Intellectual Property Enforcement Coordinator, 2010, p. 4). On February 8, 2011, a former Corning employee was sentenced to 30 months in prison for conspiracy to commit theft of trade secrets regarding Corning's thin film transistor and liquid crystal display glass production process on behalf of a Taiwanese competitor (Department of Justice, 2011a). On February 17, 2011, a former technical operations associate at the Bristol-Myers Squibb pleaded guilty to stealing trade secrets to help start up a company in India (Federal Bureau of Investigation, 2011a). On April 12, 2011, a former Ford employee was sentenced to 70 months in federal prison after pleading guilty in federal court to two counts of theft of trade secrets relating to the theft of automobile designs from Ford and providing them to a Chinese competitor (Department of Justice, 2011b).

While the court cases listed above demonstrate the very real threat of the insider to the security of proprietary information, less obvious are the methods used by hostile actors to identify and exploit a company's employees to acquire the same information. Using a technique known as social engineering,<sup>1</sup> a hostile outsider gathers inside

---

<sup>1</sup> Social engineering is defined as using influence and persuasion to deceive people and take advantage of their misplaced trust in order to obtain insider information (Mitnick, 2002).

information, some of it seemingly innocuous, but all with the purpose of making a hostile actor seeking classified or proprietary secrets seem a friendly follow insider. Traditional social engineering techniques, such as combing through the trash of a target company, making a series of deceitful phone calls, and otherwise “connecting” to the unwitting employees, are used to obtain the names of senior executives, IT persons and processes, and company lingo; all to enable the elicitation of sensitive information and/or obtaining access to the otherwise secure company IT network (Graves, 2010). Social engineering exploits the laziness, good manners, or enthusiasm of a company’s staff to obtain illegally a company’s money, intellectual property, or IT security information (Microsoft TechNet, 2006). Mitnick describes how effective social engineer renders moot expensive IT and security programs and technologies by stating, “A company may have purchased the best security technologies that money can buy...(and still be) totally vulnerable” (Mitnick, 2002). According to the *2011 Data Breach Investigations Report*, for data breach avenues that used social engineering methods, criminals are increasingly relying on direct contact with a company insider, with 78 percent of cases involving a solicitation to obtain confidential insider information having in-person contact (Baker, Hutton, Hylander, Pamula, Porter, & Spitler, 2011). The report notes, “Even in our high-tech business world, many deals won’t get done without an in-person meet-and-greet” (Baker et al., 2011).

Although social engineering has been a threat to protecting intellectual and classified information for many years, the explosion of the popularity of an entirely new communications medium acts as a catalyst for the threat. Social networking sites,<sup>2</sup> unheard of 10 years ago, have come to be a major force in internet usage today. By itself, the social networking site *Facebook* accounted for an extraordinary 12.3 percent of the time spent online in the United States in 2010 (comScore, Inc., 2011). A marketing report examining internet use indicates that **51 percent** of all Americans aged 12 and older have profiles on *Facebook* (Aritron, Inc. & Edison Research, 2011). These sites

---

<sup>2</sup> Social networking sites are defined as web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system (Boyd & Ellison, 2007).

encourage users to display publically a wealth of personal and private information as a means of providing updates and maintaining communications with friends and associates. Businesses and government agencies use social networking sites to help users find their products and services. Like with any new technology, social networking media has the potential to be used by criminals and other hostile threats for illegal purposes, including the attempt to gain access to protected, sensitive information.

While the use of social networking sites to enable social engineering attacks is not clearly documented in real-world attacks, a *Washington Post* article noted the existence of a “powerful computer tool to ‘scrape’ *Facebook* and other social-media sites for personal information” in order to use it for nefarious purposes (Eggen, 2011). With the explosion of popularity of these sites, an organization’s employees and contractors, many with access to critical information valued by foreign governments or business competitors, can be expected to have active social networking media profiles. A USA Today article described how “Elite cybercriminals are tapping into search engines and social networks to help them target specific employees for social-engineering trickery at a wide range of companies, professional firms and government agencies” (Acohido, 2011). Rather than through phone calls and dumpster diving, a hostile social engineer can now leverage these new sources of detailed information (personal and professional) found in social networking sites to make more efficient the potential exploitation or recruitment of an insider (Hadnagy, Aharoni, & O’Gorman, 2011). The existing threat to sensitive information essentially is able to employ a new intelligence-collection mechanism (social networking media) to make better use of existing techniques (social engineering).

A difficult challenge to counter this new attack avenue for social engineering efforts is the lack of boundaries between work and personal life in social media management. With social networking sites being such a new and immature industry, there are very few examples to model proper and vulnerable behavior to employees (Hadnagy et al., 2011). This thesis will explore how social networking media can be used to gain access at the exact point with gravest consequences to a target organization; and determine potential mitigation strategies to limit the vulnerability introduced by social networking media.



### **C. RESEARCH QUESTION(S)**

1. Does the use of social networking media by an organization's employees introduce new vulnerabilities to the loss of intellectual property? If so, how?
2. Are there any documented cases of hostile actors using social networking sites to gain access to an organization's sensitive (proprietary or classified) information?
3. What are examples of current policy or research to guide organizations in the mitigation of social engineering and the insider threat?
4. What are examples of current policy or research to guide organizations on employee use of social networking sites?
5. What are current or emerging methodologies that mitigate the vulnerability of social networking sites in enabling the insider threat?

### **D. HYPOTHESIS AND TENTATIVE SOLUTIONS**

This hypothesis claims social networking media increases the ability of hostile actors to use social engineering techniques to gain access to cause severe economic damage to an organization. By doing so, the use of social networking media by an organization's employees increases the Vulnerability in the Risk = Threat x Vulnerability x Consequences equation. Therefore, social networking media has the capacity to increase total risk. Tentative solutions to be explored include technical and operational security methods to decrease both vulnerabilities and consequences created by nefarious use of social networking media.

### **E. SIGNIFICANCE OF RESEARCH**

This thesis will examine how social networking media introduces new vulnerabilities that can be leveraged by the threat of hostile actors in acquiring an organization's sensitive information. In addition, the thesis will introduce strategies to potentially mitigate or neutralize those effects. This thesis is designed to be a starting point in which any future use of the proposed strategies can be tried to gauge their effectiveness.

## **F. RESEARCH METHOD**

This thesis will survey reports and other literature and will use the interview method to ascertain the potential or actual use of social networking media to enable the loss of intellectual property via the insider threat. In addition, the thesis will identify current mitigation strategies and attempt to identify new strategies that can reduce the vulnerability created by social networking media.

## **G. INTERVIEW RESPONDENTS**

The interview respondents consisted of: 1) Chief Security Officers or Executive/Senior Vice Presidents of Security or Operations drawn from companies in the security consultancy and defense contractor sectors; and 2) analysts expert in understanding the use of social engineering techniques and social networking media in business intelligence. All of the respondents have significant experience in the security, law enforcement, and/or intelligence communities. The mix of expertise in the respondents helped define the impact of the social networking media on the insider threat and create realistic mitigation strategies. I identified the respondents through two avenues. First, I was allowed to provide a short presentation at a meeting of the Federal Bureau of Investigation's (FBI) National Business Alliance in which I explained the nature of my research and requested volunteers to interview. Second, I leveraged contacts within the FBI's Social Media Working Group to gain access to a community of analysts inside and outside of government that used or examined the use of social networking media in intelligence collection. Using respondents identified through these two forums, I conducted interviews of seven subject matter experts in support of this thesis.

## **H. INTERVIEW QUESTIONS**

The interviews were comprised of nine open-ended questions designed to solicit information regarding professional background and familiarity with social networking media; any actual or perceived vulnerabilities introduced by social networking media;

current security postures and proposed solutions to mitigate the vulnerabilities created by social networking media; and an understanding of measures to gauge the effectiveness of any mitigation strategies.

**1. General Background**

- What is your professional background?
- What is your personal familiarity with social networking media? Which sites, if any, do you or your family use?
- Does your organization use social networking media? If so, how?

**2. Social Networking Media Vulnerabilities**

- Do social networking media introduce a new or different set of vulnerabilities to the protection of intellectual property? If so, describe those vulnerabilities and the way social networking media can enable them.
- Are you aware of any incidents that involved the use of information found on social networking media to negatively impact an organization? If so, describe the incident(s) and the impact(s).
- Are you aware of the use of social networking media to obtain relevant professional and personal information when gathering competitive business intelligence? If so, describe the methods used and gauge the impact of the use of social networking media on the resulting consequence to the target organization.

**3. Social Engineering and the Insider Threat**

- Are you aware of social engineering techniques being used to gather an organization's sensitive information? Do social networking media make the use of social engineering techniques more effective? If so, how.
- Does your organization have a program to identify and/or mitigate the insider threat? If so, describe that program, and how its effectiveness is gauged.

**4. Policies or Programs Regarding the Vulnerability Mitigation of Social Networking Media**

- What programs, methodologies, or technologies could be used to mitigate any risk introduced by the new vulnerabilities of the use of social networking media by an organization's employees?

The widespread use and acceptance of social networking media as a new communications medium has created whole new aggregations of data that can be used to exploit an organization and its employees. It has greatly increased the attack surface<sup>3</sup> for a hostile actor to gain access to protected information. The huge loss to the U.S. economy caused by the theft of intellectual property and trade secrets requires us to better understand this new vulnerability to more effectively ensure U.S. competitiveness in the global economy.

---

<sup>3</sup> Attack surface is defined as an organization's exposure, the reachable and exploitable vulnerabilities that are present to potential hostile actors (Northcutt, 2011).

## II. LITERATURE REVIEW

This literature review is designed to ascertain the existing base of knowledge that:

1. Identifies the perceived insider threat and the use of social engineering to acquire an organization's sensitive information ; while further examining if the literature addresses the use of social networking media to enable that threat; and
2. Identifies security methodologies that mitigate or neutralize the insider threat—while examining if the literature addresses the mitigation of the vulnerability of social networking media.

A summary of the literature demonstrates that documented cases that acknowledge the use of social networking media to illegally acquire an organization's sensitive information are rare. The cases that are described focus on the cyber threat of using social networking media to enable more realistic phishing attacks.<sup>4</sup> Professional and security industry literature, however, shows the perception of the vulnerability created by social networking media to business is quite prevalent. In addition, while there is literature that explains the necessity to protect proprietary information and describes methodologies to counter the insider threat, there is no peer-reviewed literature that specifically addresses strategies to define and mitigate the vulnerability introduced by social networking media.

Of note is the fact that private industry has a legal and fiduciary responsibility to protect intangible assets, such as intellectual property and trade secrets. An American Bar Association (ABA) article highlights the Sarbanes-Oxley Act (SOX) legislation bringing a focus to the protection of intangible assets (e.g., trade secrets) as it relates to valuation of all of a company's assets. SOX requires management to document, test, and certify the effectiveness of internal controls over financial reporting. This would include procedures that provide reasonable assurances regarding prevention or timely detection of unauthorized acquisition, use, or disposition of the issuer's assets that could have a

---

<sup>4</sup> Phishing—In a phishing attack, the adversary sends an e-mail to a target group soliciting them to perform some action that will reveal sensitive information. Spear phishing refers to attacks that are targeted at particular individuals or companies, instead of the broader, generic phishing attacks. Whaling is a special case of spear phishing aimed at company executives and other important targets (Bishop, Engle, Peisert, Whalen, & Gates, 2009).

material effect on the financial statement. All corporations owe a fiduciary duty to their shareholders to protect valuable trade secrets; however, in spite of the SOX requirements, companies often do not comprehend the totality of the obligation necessary to protect from the insider threat. The article identifies this obligation and recommends remedies that focus on vulnerability reduction (e.g., identify and track access to critical intellectual property, have an active IT security program) (Allen, 2007).

An Institute of Internal Auditors article describes the Security and Exchange Commission (SEC) recommendations that company management “include consideration of the vulnerability of the entity to fraudulent activity (for example, fraudulent financial reporting, misappropriation of assets, and corruption), and whether any such exposure could result in a material misstatement of the financial statements” (Institute of Internal Auditors, 2008). This requirement has spawned a new auditing industry with a focus on a company’s internal controls on tangible and intangible assets alike, including processes to mitigate the theft of trade secrets.

The SOX and SEC requirements give context for the need to examine social networking media as a new vulnerability to fraudulent activity. Due diligence would seem to require companies understand the social networking media vulnerability and have in place policies and programs to account for it.

#### **A. LITERATURE THAT IDENTIFIES THE INSIDER THREAT AND THE USE OF SOCIAL NETWORKING MEDIA**

*PCWorld* outlined a long-term attack (over four years) in which Chinese hackers targeted oil, gas, and petrochemical companies with technical attacks on their public-facing Web-sites. The hackers also used persuasive social-engineering techniques to get key executives in Kazakhstan, Taiwan, Greece, and the United States to divulge information (Kirk, 2011).

A Public Broadcasting System article highlights two separate incidents in which a fake online persona was created by an unknown individual who was able to “friend” a community of analysts, contractors, and defense officials—all with security clearances. In both cases, the fake profile involved an attractive, young woman with apparent inside

knowledge of the verbiage and inner workings of those communities. Department of Defense and U.S. Intelligence Community officials are unclear on whether any actual security breach occurred. They are also unsure on how to best regulate and mitigate this threat (Frost, 2011).

In one of the aforementioned cases, Thomas Ryan conducted the Robin Sage experiment by creating a fictitious cyber security analyst with a false identity and profile on several social networking Websites. Ryan used this vehicle to research people's decision to share sensitive information with "Robin Sage." Contacts included executives at government agencies and Fortune 500 companies. The experiment showed how social networking media and social engineering are well posed to enable the insider threat (Ryan, 2010).



Figure 1. The Infamous "Robin Sage" (From Waterman, 2010)

A Federal Bureau of Investigation Business Alliance study highlighted the results of a project in which a summer intern was tasked to use open source and social media to acquire an technical data on a sensitive device being built by a cleared contractor (Federal Bureau of Investigation, 2010). The intern used news articles, press releases, and the product Website to find specific technical details (including encryption type and standards), project development team information, and field support personnel biographical data. The report highlighted the use of *Facebook* and *LinkedIn* social media

in identifying additional project personnel and conducted a behavioral analysis for potential employee recruitment for insider information (Federal Bureau of Investigation, 2010).

A report summarized the *Social-Engineer.org* sponsored “DefCon 18 Social Engineering CTF:How Strong Is Your Schmooze” contest to acquire sensitive company information using social engineering techniques (Hadnagy et al., 2011). This event directed 15 participants to target unwitting companies in order to acquire protected information through the use of social engineering. Some of the targeted information included acquisition of the operating system used by the company’s computers, the version of the e-mail client, the version(s) of any anti-virus software, etc. The purpose of this exercise was to demonstrate the risk posed by social engineering to organizations, evaluate what approaches were effective, and demonstrate or recommend effective protections. The results highlighted the fact that “*Facebook*...was used extensively as the number of public accounts make it quite useful” for social engineers to discover and exploit the employee associations within a company (Hadnagy et al., 2011). The report recommended that companies clearly define appropriate social networking media behavior for employees and model how such behavior would appear (Hadnagy et al., 2011).

The *Symantec Internet Security Threat Report 2010* highlighted internet security trends that included a increase of targeted **attacks that find** the easiest vulnerability to exploit is the trust of friends and colleagues (Symantec, Inc., 2011). For example, Stuxnet could not have breached its target (the Iranian nuclear processing facilities) without someone having trusted access. Other attacks would not have been successful without convincing users that the links and attachments they received in an e-mail were from a trusted source. It does not matter whether the attacker is targeting a CEO or a member of the staff, social networking media is huge source of information for a majority of employees of any organization.

The Internet and social networks provide rich research for tailoring an attack. By sneaking in among friends, hackers can learn interests, gain trust, and convincingly masquerade as friends. The information gained by the use of social networking media renders obsolete the telltale signs of a



phishing attack of strange e-mail addresses, bad grammar and obviously malicious links. Social media has made a well-executed social engineering attack almost impossible to spot. (Symantec, Inc., 2011)

An article from an IT security and hacking Website discusses the specific social engineering threats enabled by social networking media.

Traditionally discovery is the first phase of a social engineering attack. It always aids an attacker to know details about their victim. Publicly available information regarding the victim's employer, organizational structure or coworkers is invaluable in creating an atmosphere of trust. Often times an attacker will research the names of higher level executives or people in departments normally accorded trust (for instance, the names of people in an organizations IT department).

Although an attacker might easily be able to glean names and titles of people in an organization, understanding a victim's trust network is much more difficult. Rather, this has traditionally been difficult. New online social and business networking applications make it increasingly easy for an attacker to explore the trust relationships of a victim by scrutinizing the data that the victim voluntarily, but perhaps unwittingly, provides. For instance, scanning through business networking sites like *LinkedIn*, or social networking sites like *Facebook*, *My Space*, or *Friendster*, can yield a very complete picture of a person's trust network. By examining the people the victim has linked to via these networking sites the attacker can build a clear picture of the victims trust network.

Once armed with a topology of the victim's trust network the attacker can much more effectively exploit the victim. By identifying trusted third parties and manufacturing or mimicking relationships with these third parties, the attacker can leverage the trust accorded them. (MadIrish.net, 2008)

An abstract titled *Towards Automated Social Engineering Using Social Networking Sites* describes how a cleverly written Automated Social Engineering bot<sup>5</sup> can “learn” a victim’s friendship circle and send message automatically in a manner that quite often can pass the Turing test.<sup>6</sup> Into these messages are written malicious code to be loaded into the victim’s computer or network. This technique has the advantage of being targeted and automated. The test cited in the abstract showed mixed results in

---

<sup>5</sup> Bot: Software that can run applications over the Internet (Levy, 2011).

<sup>6</sup> Turing test: The ability of an artificial process to produce dialogue that passes as produced by an actual person (Levy, 2011).

convincing the subjects that the virtual chat was with a real person but concluded that the success rate was good enough to make this approach a cheap and attractive method for a social engineering attack (Huber, Kowalski, Nohlberg, & Tjoa, 2009).

A Comsec Consulting report extensively describes the social networking corporate threat (Zalalichin, Efrati, & Cohen, 2010). The attack vectors that create a security risk are available mainly due to the ease of social networking media use and the manner in which one can quickly establish trust between an organization's employees and the attacker. In the past, access to valuable company data required the use of bribes, social engineering, and physical entry into a target organization's space. Social networking media allows an attacker, with minimal technical knowledge, the ability to obtain an employee's full name, position, and role within the company, area of specialty, e-mail, and phone numbers, known circle of friends, education, etc. An aggregation of this information allows for a more complete understanding of the target organization, its products, its people, and the critical "inner trust circle"—defined as the core decision-making group within the organization (Zalalichin, Efrati, & Cohen, 2010). Armed with this intelligence, a hostile actor can mount sophisticated social engineering attacks via the internet or other avenues to gain access to the most critical persons and sensitive information with the organization (Zalalichin, Efrati, & Cohen, 2010).

## **1. Summary of Social Engineering and Social Networking Media Threat Literature**

The literature demonstrates that a threat to organizations exists when hostile actors use social networking media to enable social engineering attacks—either virtually or via actual contact with company employees. Interestingly, most of the literature provides a descriptive or hypothetical understanding of the vulnerabilities introduced by social networking media. While there are examples of the potential of social networking media being used in an effort to acquire proprietary or sensitive information (e.g., the DefCon 18 and FBI studies), there is very little empirical evidence of its use in a documented attack outside of targeted spear phishing attacks. In spite of the lack of empirical evidence, the literature highlights that the vulnerability of social networking media is potentially a very real problem. This review acknowledges a significant number

of articles that were generated by security firms with a profit-making interest in hyping any hostile threat, including the very relevant DefCon summary. For this reason, the FBI study and the already documented use of social networking media in phishing attacks are critical to give credence to the security industry articles.

**B. IDENTIFY SECURITY METHODOLOGIES THAT MITIGATE THE INSIDER THREAT AND THE VULNERABILITY OF SOCIAL NETWORKING MEDIA**

The article “Microsoft Technet: How to Protect Insiders from Social Engineering” offers an in-depth understanding of social engineering and describes a thorough framework to design defense strategy to counter the social engineering threat (Microsoft Corporation, 2009). Some recommendations include specific policies and process to govern interaction on the phone or e-mail, awareness training, physical security, and data and IT security (Microsoft Corporation, 2009).

The Federal Bureau of Investigation highlights its Business Alliance as a specific Counterintelligence Strategic Partnership program (Federal Bureau of Investigation, 2010). This program builds relationships with cleared defense contractors to enhance the delivery of counterintelligence education. The stated purpose of the program is to assist business partners to identify counterintelligence vulnerabilities thereby resulting in the modification of internal security processes to decrease the susceptibility to theft of intellectual property (Federal Bureau of Investigation, 2010). The program explicitly notes that “The protection of our Business Alliance partners’ intellectual property results in the tangible benefits to our national security.” (Federal Bureau of Investigation, 2010).

The United States Secret Service (USSS), in conjunction with Carnegie Mellon Institute, produced two reports that examined and outlined the implications of the insider threat to: 1) the banking and financial sector; and 2) the critical infrastructure sector (utilities, energy, transportation, etc.) respectively (Randazzo, Keeney, Kowalski, Cappelli, & Moore, 2004). The findings included the following commonalities:

- Most incidents required little technical sophistication;
- The actions were planned;

- Financial gain or revenge from a negative work-place issue were the primary motivators;
- Perpetrators did not share a common profile;
- A range of methods caused detection but the most common detection method was through non-automated means by personnel not directly affiliated in the company's security program (Randazzo et al., 2004).

The report recommended better IT monitoring and a robust training and reporting mechanism regarding suspicious IT behavior for company employees, vendors, and customers (Randazzo et al., 2004). All recommendations were reactive in nature although the need was noted for “organizations to look beyond their information technology and security to their overall business practices” (Randazzo et al., 2004).

The Department of Homeland Security's (DHS) Cyber Security Research and Development Website describes an Insider Threat Detection and Mitigation program (Department of Homeland Security, 2010a). This program analyzes the structure of actions through the normal IT processes and detects small deviations from those patterns. This methodology is completely technically focused as it attempts to detect unauthorized usage of an IT system (Department of Homeland Security, 2010a).

*Utility Week*, an industry trade journal, examined a Spanish utility company that implemented an IT enterprise security monitoring system in order to correlate the millions of potential security events that occur daily on a large corporate network (Newton, 2005). The specific technical solution became the focus of the insider threat awareness and mitigation program that showed some promise to mitigate that threat (Newton, 2005).

The ABA provides a risk mitigation template for an industrial security program. At a minimum, it recommends that every company should consider internal controls to mitigate the theft of trade secrets via the insider threat (Newman, 2007). The list is primarily focused on IT controls and monitoring, physical access control for visitors, and a robust confidentiality agreement program, starting in the hiring process and maintained through training. The ABA discussed the phrase “trade secret audit” that should be conducted on an annual basis to assess the status of trade secret programs and

protections, mandating that resources be devoted to this issue proactively, rather than after an employee misappropriates core trade secret data (Newman, 2007).

Magkarlas and Furnell wrote *A Preliminary Model of End User Sophistication for Insider Threat Prediction in IT Systems* in which they offer a model for insider threat prediction in IT systems based on the analysis of the IT sophistication of the end-user (2002). The model acknowledges its limitations based on the sample selected to determine user proficiency but argued it might prove useful as a metric for insider threat prediction (Magkarlas & Furnell, 2002).

After listing many of the statistics for the cost of the rogue insider, a business article in *Information Week* outlined the start of a human intelligence/IT security program (Greenemeier, 2006). The article recommended an active synergy between human resources and IT security by ensuring adverse workplace issues are made known to corporate security which then would monitor the relevant IT activities to find potential insider threat anomalies (Greenemeier, 2006). The article states that “Simply getting to know employees will create loyalty and may even tip off potential problems. ‘If a guy on your staff needs an extra \$20,000 to pay for his kid’s tuition, he might try to sell (proprietary information)’.” Social networking media may provide some information that would alert an organization to potential issues that could indicate a higher risk for insider threat (Greenemeier, 2006).

In a *CyberPsychology & Behavior* article, Gudaitis outlined the fact that the disciplines to assess, evaluate, and solve human-based problems have not been integrated into the mitigation of the insider threat problem (1998). She called for the integration of behavioral experts (profilers) and IT security experts and recommended a multidimensional approach be developed and used to specifically assess those who would commit computer crimes (Gudaitis, 1998).

A Defense Personnel Security Research Center report noted a clear relationship between personnel stress, as well as, adverse social climates and the level of risk for system abuse (Shaw & Fischer, 2005). It warns against the reliance on software solutions or technical deterrents as opposed to knowing what is happening in employee’s lives (be

it possible loss of employment, marital stress, substance abuse, financial problems, etc.) (Shaw & Fischer, 2005). The report further recommended a robust program for monitoring workplace and employee issues, especially as it relates to IT network access and administration (Shaw & Fischer, 2005).

In a *Digital Investigation* article, Shaw framed the integration of human behavioral assessment and IT vulnerabilities (2006). He discussed how a behavioral consultant can assist investigators in several aspects of insider cyber investigations and case management decision-making, from providing insights into the perpetrator(s) of anonymous attacks to advice on specific investigation strategies and tactics (Shaw 2006). In the private sector where most cases are resolved without the direct involvement of law enforcement or the intelligence community, the behavioral consultant's assistance may be particularly important to designing plans to evaluate the subject, and if necessary, remove him or her from the organization while minimizing the risk of the subsequent attacks. Finally, when insider cases go to trial, behavioral consultants can provide support similar to other cases. This may involve assistance preparing witness examination strategies and tactics, addressing jury issues and advice regarding effective communications with legal decision-makers (Shaw 2006).

A *Computers & Security* article developed a framework to define relevant types of insider attack-related behaviors and symptoms—indicators that include deliberate markers, meaningful errors, preparatory behaviors, correlated usage patterns, verbal behavior, and personality traits (Schulz, 2002). Using these indicators, both IT and behavioral based, a predictive model is applied to possibly thwart an insider attack. The presence of numerous inputs necessitates the use of quantitative methods but it includes off-net inputs based on real-world observations of employee actions. The article suggests that behavioral observations be translated into empirical data to be used as part of an overall predictive model (Schulz, 2002).

RAND produced the proceedings of a workshop that developed a process to understand and evaluate insider threat detection programs using past espionage cases as the validating test data (Brackney & Anderson, 2004). While it leveraged IT system markers and actions as the basis of the program, the report defined an “Observables

Taxonomy” of the insider threat (Brackney & Anderson, 2004). Listed under observables were the following items: polygraph, security violations (physical, cyber), missing reporting (financial, travel, etc.), physical access (logs, badges), cyber actions, foreign travel, private finances, vices, materials transfer to handlers, counterintelligence, social activity (internal, external), and communications (Brackney & Anderson, 2004). This represented the totality of observable inputs into the detection model. The report continued by further defining the cyber actions and developing detection and mitigation strategies (Brackney & Anderson, 2004). Noted was the report’s focus on the insider threat to U.S. government agencies and not private industry (Brackney & Anderson, 2004).

In an Air Force Institute of Technology thesis, Puelo directly addressed the methodology of including observable human actions in a process for mitigating insider threat using human behavior influence models (2006). The thesis treats the insider threat as a people problem and describes a process that begins by identifying the nature of relationships between personnel in the organization. Only by understanding these relationships can one identify the potential vulnerabilities of an individual being a critical node of access. An extensive battery of evaluations of life stressors is used to translate that individual’s life environment into a numerical score. The observable stressors are reduced into a formula that includes influences, events, responses, and stimuli between the individual and his/her environment. This model is a dynamic model over time, so the trend or slope of the empirical output is plotted to determine a complete insider threat risk. The thesis details a robust process that attempts to use human behavior to identify insider threat risk (Puleo, 2006).

A Center for Homeland Defense and Security thesis describes a redesign of corporate work processes in order to severely limit the amount of time an individual would be left alone or allowed unfettered access to critical work processes (Catrantzos, 2009). The redesigned procedures would make for a more extensive probation period to better evaluate employees while promoting transparency and accessibility to all team members. The end result is that potential insider threat personnel will become part of an extended team environment and opportunities for clandestine access will be severely

constrained. The author noted the tendency of organizations to apply technology to the insider threat problem, equating it to the use a laser when a broader, flashlight would provide a better picture of the threat environment (Catrantzos, 2009).

A *Competitive Intelligence Review* article describes a Counter Competitive Intelligence strategy that identifies what is absolutely critical for the firm's survival or competitiveness—the “corporate jewels”—and then takes action to limit their vulnerability to competitor intelligence collection (Mark, 1997). The author makes use of the military's five-step operations security approach for assessing risk and establishing countermeasures to limit a firm's risk to competitive intelligence (Mark, 1997). It adds that counterintelligence should move away from the government-clandestine model to an approach based on seeking to learn the routine intelligence activities that competitors are directing at a company. The firm could then apply mitigation strategies and analyze any damage (Mark, 1997).

The FBI's Security Division has issued a draft document to govern the use of social networking media by its employees. “Social Network Sites and the FBI Employee Guidance” provides background and trend analysis for social networking sites and outlines some general precautions to take while using social networking media (Federal Bureau of Investigation, 2011b). This includes prohibiting “accessing publicly accessible social networking sites for non-FBI business purposes from FBI Information Systems” and limiting the amount of personal information that is posted while being alert to social engineering elicitation (Federal Bureau of Investigation, 2011b). In 2011, the FBI added awareness training of social engineering and the threat of nefarious use of social networking media to its annual security training. This was the first time the topics were part of the mandatory training on information security (M. Levett, personal communication, June 13, 2011).



## **1. Summary of Current Literature to Identify Security Methodologies that Mitigate the Insider Threat Especially Threats Enabled by the Use of Social Networking Media**

A summary of the literature concerning security methodologies designed to counter the insider threat showed a common emphasis placed on reducing vulnerability to the company; primarily through the application or modification of IT security methods to mitigate loss of intellectual property. Much literature exists that defines the use of technologies to counter the insider threat in the cyber realm. The second theme of the review recommended the integration of human behavior observables into the aforementioned IT monitoring to counter the insider threat. Of the findings, the implications of the non-automated, non-security personnel detections are most critical. While social networking media were not noted in any of the insider threat detection literature, the information found on social networking media would seem to be of great utility in supplying more background in the behavioral assessment models of insider threat detection; all of which require a vehicle to observe and input specific human behaviors and relationships.

The FBI, USSS, and DHS describe specific policies and operational actions that can be employed to mitigate the risk of insider threat and loss of intellectual property. In addition, there exists some initial awareness training and nascent policy to govern and manage the use of social networking media by employees. None of the literature recommends barring the use of social networking media by employees.

## **C. CONCLUSION**

This literature review found that a majority of the insider threat mitigation methodologies were specific to the application of IT monitoring technology to detect anomalies. There was extensive literature for existing physical and IT security programs and ample government guidance for program administration within a classified environment. While a number of business articles described methodologies for the reduction of the threat enabled by social networking media, this review could find no peer-reviewed literature that defined the insider threat vulnerability introduced by social

networking media. The existing peer-reviewed literature primarily focused on the privacy issues related to the widespread use of social networking sites.

A sizable portion of the review showed research that pertained to the integration of human behavioral disciplines into insider threat detection. Most of that literature attempted to find a repeatable model in which human behaviors could be converted into empirical data and inserted into a proposed formula that could identify personnel with a higher risk as an insider threat. The two Shaw articles did discuss specific methods to use to integrate behavioral analysis and IT security (2009; 2010). The RAND study was extremely specific in defining the observable taxonomy that could indicate an insider threat (2004). The combination of the RAND report and Shaw studies better defined what behaviors would be relevant in an integrated security program but neither addressed social networking media

The most telling study was the FBI's presentation of the real-world use of open source and social media by a relative novice in the cyber security profession to identify critical technical data and key personnel for exploitation (Federal Bureau of Investigation, 2010). While the FBI study and DefCon synopsis demonstrated actual, if somewhat controlled, use of social networking media for information collection, there seems to be no peer-reviewed literature that examined the use of open source and social networking media from an information or intelligence collection perspective. This thesis will examine of the use of social networking media as an initial framework in which to identify vulnerabilities and behavioral markers within an organization and propose potential strategies to mitigate this new vulnerability.

### **III. RESEARCH METHODOLOGY**

This thesis's hypothesis posits that social networking media increases the ability of hostile actors to use social engineering techniques to gain insider access to cause severe economic damage to an organization. If true, social networking media becomes, in essence, another method to collect sensitive intelligence. In the context of defining a framework to describe how social networking media is used to gather information, it stands to reason that lessons can be adapted from industries that specialize in gathering intelligence and countering the same. This thesis will draw upon the existing disciplines of counterintelligence, corporate security, and intelligence collection and analysis. It follows that subject matter experts from such disciplines, who themselves have significant experience in the collection or protection of information, also possess insights useful for advancing an understanding of the vulnerabilities introduced by social networking media.

This thesis adopts the qualitative approach of separate, individual interviews of a diverse group of experts to derive insights and judgments to affect the research. I interviewed seven subject matter experts who possess significant experience within the counterintelligence, security, and business intelligence communities; including an understanding of social engineering attack methodology. The subject matter experts possess professional backgrounds in identifying, investigating, countering, or exploiting the insider threat and offer useful insights in which to understand and mitigate the negative impact of social networking media. The interview's open-ended questions were designed to determine if social networking media is perceived as a vulnerability; examine its impact on existing attack vectors such as social engineering and phishing; and elicit expert opinion on the best methods in which to mitigate or neutralize this new vulnerability.

I presented a short briefing on the topic of this thesis and its intended research goals at two forums: the FBI's Business Alliance and the FBI's Social Media Working Group. I identified the respondents through the larger population of corporate security experts and competitive intelligence analysts at these forums. During these presentations, I solicited volunteers for a more formal interview process to examine thoroughly the effects of social networking media on the insider threat. In the end, four corporate security and operations executives and three competitive intelligence analysts responded and agreed to be interviewed for this thesis.

Table 1 describes the expertise of the respondents. Many of the individuals have overlapping skill sets but, as a whole, the respondents coalesced into two categories: 1) senior corporate executives having a responsibility for protection of the intellectual property and mitigation of the insider threat; and 2) intelligence analysts having experience in understanding how to exploit social networking media for information collection. The ages of the respondents corresponded to their professional groupings. The executives ranged from 50–62 years old (four respondents), while the analysts fell between 28–35 years old (three respondents).

Table 1. Relevant Biographical and Professional Information of the Subject Matter Experts

Expert 1	Chief psychologist for a federal law enforcement agency for over 15 years. Extensive review of the Guantanamo Bay detainees. Senior consultant with several public industry and government clients. Ph.D. in psychology.
Expert 2	Intelligence Analyst for a federal law enforcement agency. Over five years of experience, lead agency expert in the field of exploiting social networking media for intelligence collection. M.S. in strategic intelligence.
Expert 3	Competitive intelligence analyst for a security intelligence firm. Over five years of experience in human intelligence collection and counterintelligence for the U.S. military. Clients include private industry and government. M.A. in forensic psychology.
Expert 4	Chief Security Officer for a large classified contractor. Over 25 years of federal law enforcement, counterintelligence, and security experience, including as a certified intelligence officer. Possesses a J.D.
Expert 5	Senior security executive for government and private industry clients. Over 25 years of experience in federal law enforcement, security, and physical and personal protection expertise.
Expert 6	Senior operations executive for a security consulting firm for government and private industry clients. Over 25 years of experience in the intelligence community, specializing in counterintelligence and counterterrorism. Possesses a J.D.
Expert 7	Competitive intelligence analyst for a security intelligence firm. Over 10 years of experience in human intelligence collection and strategic and tactical vulnerability targeting within the intelligence community and private industry. Clients include private industry and government. M.A. in International Relations/ Economics.

Table 2. Cumulative Summary of the Expertise These Interviewees Possess

<b>Professional Expertise</b>	<b>Interviewees Possessing Expertise</b>
Protection responsibilities for proprietary or classified material	7
Understanding of corporate/government security practices	5
Focus on threats hostile to own organization	4
Understanding or use of counterintelligence techniques	4
Specific experience with or use of social engineering	4
Use of social networking media to gather intelligence	3

All respondents agreed to participate in the study under the standard confidentiality protections with no classified or proprietary information being considered for the study. The interviews were scheduled at the place and time of the respondents' convenience. On each occasion, the setting was private with only the interviewer and respondent present. The questions were e-mailed approximately one week in advance. Of the seven respondents who agreed to participate in the interviews, 100 percent saw the process through to completion.

The respondents were encouraged to review their own experiences to identify actual use of social networking media that enabled follow-on information collection. Examining social networking media from the offensive (threat or collector) optic and the defensive (security or protection) optic allowed an opportunity to juxtapose the respondents' expert opinions on the same topic from opposite sides. The analysis captured points of expert convergence and divergence. The next chapter will analyze these points of convergence and divergence and synthesize a new and actionable methodology to understand and mitigate the vulnerability of social networking media.

## IV. RESULTS

The results of the interviews of the respondents show very real vulnerabilities created by the pervasive use of social networking media. While hard evidence of an actual event that exposed these vulnerabilities is lacking, the intuitive perception that these vulnerabilities exist is very strong among *all* respondents. Respondents described how the “treasure trove” of data loaded into social networking media has the potential to become the foundation of a process to target and exploit critical individuals within an organization. Social networking media is tailor-made to enable intelligence collectors to use more refined social engineering techniques. The respondents proposed the mitigation strategies of a social networking media awareness campaign for an organization’s employees; and a social networking media monitoring process that tracks information found on social networking media from a threat perspective to allow for a better of an organization’s attack surface.

### A. GENERAL BACKGROUND

#### 1. What is Your Professional Background?

The professional background of the respondents was summarized in Tables 1 and 2 of the previous chapter.

#### 2. What is Your Personal Familiarity with Social Networking Media? Which Sites, If Any, do You or Your Family Use?

All respondents used social networking media, with *LinkedIn* (six of seven) and *Facebook* (five of seven) being the most common sites. All respondents indicated their families use social networking sites, with *Facebook* (seven of seven) being most common among family use. As noted in the methodology chapter, the ages of the respondents were grouped between 50–62 years old (four respondents) and 28–35 years old (three respondents). This fact seemed correlated to some of the divergence regarding social networking media use. The older (or perhaps “more experienced”) respondent group described social networking media usage as important, but not essential, in their day-to-day lives. The younger group described social networking media usage as critical for

their professional activities and essential to their personal lives. All respondents were deliberate on limiting the amount of personal information posted to the social networking sites and counseled immediate family members to use caution. “Common sense” seemed the standard to gauge the appropriateness of information posting with that exact phrase used by five of seven respondents.

### **3. Does Your Organization Use Social Networking Media? If So, How?**

The seven respondents represented six different organizations; and five of the represented organizations used social networking media, primarily for advertising for hiring purposes. One organization used social networking media to solicit crime tips from the *Facebook*-using public. Three organizations used social networking media during the hiring process to help screen perspective employees.<sup>7</sup> The respondents of the other organizations did not know if social networking media was used in the hiring process (or chose not to answer). None of the respondents had responsibility for their organizations’ use of social networking media.

As a whole, the respondents were aware of the use of social networking media by their respective organizations but its organizational use had no direct or tangible impact on their jobs. The analysts were quite specific in delineating their respective organization’s use of social networking media (noted above) from their own specific use. That divergence will be addressed in the results to later questions.

## **B. SOCIAL NETWORKING MEDIA VULNERABILITIES**

### **1. Do Social Networking Media Introduce a New or Different Set of Vulnerabilities to the Protection Of Intellectual Property? If so, Describe Those Vulnerabilities and the Way Social Networking Media Can Enable Them**

All respondents were adamant that social networking media introduced a new set of vulnerabilities to their organizations or clients. The initial comments by the

---

<sup>7</sup> A *New York Times* article described a firm that scrapes the Internet for everything prospective employees have posted online in the past seven years finding examples of professional/academic honors and charity work, along with negative evidence of racist remarks, drug use, offensive photos/videos, and violent activity. Data is retrieved from social networking media such as *Facebook*, *Twitter*, and *MySpace* and comments on blogs, *Yahoo* user groups, e-commerce sites, and *Craigslist* (Preston, 2011).



respondents for this question included: “absolutely,” “definitely,” and “a whole new can of worms.” Table 3 summarizes the types of potential vulnerabilities cited by the respondents that are created by certain features of social networking media.

Table 3. Summary of Types of Potential Vulnerabilities Created by Certain Features of Social Networking Media

<b>Features of Social Networking Media that Potentially Create Vulnerability</b>	<b>Cited by <i>n</i> Respondents</b>
Huge aggregation of data (personal and professional)	7
Quicker and more efficient communication or information sharing	5
Requirement for virtual self-validation (i.e., the desire to have a large number of “friends” on a site)	3
Blurring of boundaries between private/public information	3
Change of communication methods from other less vulnerable avenues (e.g., phone or e-mail)	3
Constant pressure to post more information or update social networking media	2

Four of the respondents used Wikileaks as an example of the capacity of social networking media to transmit rapidly large amounts of data almost instantly. Three of the respondents noted the vulnerability contained in the data unintentionally uploaded onto the social networking sites, such as physical location information embedded within digital photos taken by mobile devices with a Global Positioning System.<sup>8</sup>

**2. Are You Aware of Any Incidents That Involved the Use of Information Found on Social Networking Media to Negatively Impact an Organization? If So, Describe the Incident(s) and the Impact**

Five of seven of the respondents were not aware of an actual incident in which information gathered from social networking media was used to negatively impact an organization. One of the respondents indicated there were examples of negative impact but security measures prevented the disclosure of any detailed information. Another respondent had heard of an incident in which social networking media was used to communicate inappropriately, even unethically, in a competitive bid situation causing the loss of the company’s participation in the bid. The respondent had no specific details on

---

<sup>8</sup> This technique is known as geographical tagging or *geotagging* (Shankland, 2007).

this incident. Of note is the divergence of results between the analysts (two of three) and the executives (zero of four) when discussing examples of social networking media being used in an attack.

The respondents' inability to cite empirical evidence of an attack being enabled by social networking media mirrors the literature review's lack of evidence of such attacks (outside of phishing malware attacks). The lack of actual examples of social networking media use stands in contrast to the respondents' perception of the great vulnerability of social networking media noted in the analysis of the responses to question 4.

**3. Are You Aware of the Use of Social Networking Media to Obtain Relevant Professional and Personal Information When Gathering Competitive Business Intelligence? If So, Describe the Methods Used and Gauge the Impact of the Use of Social Networking Media on the Resulting Consequence to the Target Organization.**

The group of executive-level respondents did not have any knowledge of the use of social networking media to obtain information in business intelligence. This fact could be the result of the nature of this group's positions within their respective organizations—positions that focus on protection and security and not business intelligence collection. Two of the four respondents in this group volunteered that their organizations could be using social networking media in this manner.

The respondent group of analysts all indicated a use of social networking media to collect business intelligence. Two of the respondents in this group described a rather aggressive and robust use of social networking media in this matter, with the third respondent having “no comment” due to security and classification issues.

This technique of leveraging information harvested from social networking media allows for identification of connections not seen in a company's organization chart. The analysis of this collected information more clearly delineates the informal lines of communication and provides insight into the decision-makers in an organization, the “shakers-and-movers,” or the critical IT persons that control network access and security.


All of which can become targets for follow-on actions for solicitation, for information, or access either via social engineering or via focused internet malware attacks. The informal connections are overlain on a targeted company's organization chart to discover "spheres of influence." In this manner, a more coordinated and focused effort can ensure a tailored message is delivered to specific recipients in the sphere of influence. In turn, the actual target might hear (or see) some version of the message from multiple nodes within the sphere of influence, making the target far more likely to give merit to that message.

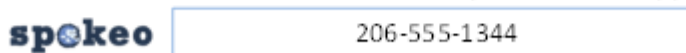
Social networking media adds a new and massive data source to be searched for information regarding a client's competition or persons of interest. There is always a question of validity of the information culled from social networking media, as with any other internet source that relies on the user to post information on self (Toma, Hancock, & Ellison, 2008). The potential for social networking media to house inaccurate information makes it advisable to confirm the veracity of the data through multiple sources. On balance, however, the possible inaccuracies of the data (e.g., biographical and physical descriptions) are outweighed by the usefulness of the relationships observed by the communications themselves (e.g., personal relationships, activities, interests). Ironically, the understanding "trust networks" is based on identifying the lines of communication/influence and not necessary the veracity of the content of the communication itself.

The following steps shown in Figure 2 take about 10 minutes for an analyst to execute to gather information using social networking media.

Figure 2. Steps to Exploit Social Networking Media of Information-Gathering

**Social Networking Media Information-Gathering Methodology**

1. Conduct “Google-hack” searches to find public profile of targeted individual  


The image shows the Google logo on the left. To its right are two search input boxes. The first box contains the text "site: facebook.com "John Public"". The second box contains the text "site: linkedin.com "jpublic1984@gmail.com"".
2. Setup phony account in social networking sites to obtain full profile
3. Use member status to identify selector information to aid to further searches (e.g. other work and personal emails, personalized user names, phone numbers)
4. Use selector information to search in “deep web” search applications  


The image shows the Spokeo logo on the left. To its right is a search input box containing the text "206-555-1344".

This social networking media and “deep Web” search<sup>9</sup> information is then combined with information from other data sources (trade journals, business records, interviews) to build a more complete picture of the person or organization of interest. A good analyst can convert the information found on social networking media into target intelligence that a social engineer can employ in an attack.

A hypothetical example has a client in support of a merger and acquisition targeting the CEO of the acquiring firm to influence the terms of the agreement in a manner more favorable to the client. The business intelligence analyst would leverage social networking media to discover that the CEO and junior manager having a strong

<sup>9</sup> Deep web search engines access the contents of searchable databases (e.g., a library catalog or statistical databases); pages excluded by common search engines (e.g., blogs, discussions threads, public-record databases); and pages deliberately restricted so web search engines avoid the page (University of California at Berkeley, 2010).

informal relationship based on each having children on the same travel sports team. A message to influence a business decision would be tailored for the junior manager who, in turn, might pass part of it on to the CEO in support of the desired position. This technique, repeated through multiple avenues of the “sphere of influence,” allows for greater attack surface into the targeted person.

## **C. SOCIAL ENGINEERING AND THE INSIDER THREAT**

### **1. Are You Aware of Social Engineering Techniques Being Used to Gather an Organization’s Sensitive Information? Do Social Networking Media Make the Use of Social Engineering Techniques More Effective? If So, How?**

All of the respondents were aware of the use of social engineering techniques for the collection of sensitive information; however, none of the respondents shared information regarding any specific attack on an organization. One respondent produced a copy of an e-mail that had been sent to all employees of an organization highlighting the DefCon event designed to use social engineering to collect sensitive company information. The e-mail defined social engineering, explained its threat, and described reporting procedures. Although the e-mail itself was confidential to that organization, I was allowed to share the following paragraph that defined social engineering to demonstrate better an effort at raising employee awareness to the social engineering threat.

Social engineering refers to attempts to elicit sensitive information from employees by obscuring the true motivation behind a request. It is often done by indirect contact using telephone, e-mail, instant message, or through social networking sites. Examples might be someone posing as a representative of our (IT) team who claims to need an employee’s user name and password to perform some authorized task. Another example might be someone posing as a potential customer or representative of a current vendor, subcontractor, or prime, who inquires for an apparently legitimate reason into a company capabilities and activities. (SME3, 2010)

Of note is the specific mention of social networking sites as a method of contact. All respondents indicated that social networking media is an ideal source of information to enable a more effective social engineering attack. Many of the respondents gave

examples of how information commonly found on social networking media that could be used in a social engineering attack. One such example is outlined in Table 4 in which Mary Doe is an important employee in the executive office of an organization.

Table 4. Hypothetical Conversation Between a Social Engineer and the Target Individual

<b>Hypothetical Information on Mary Doe’s Facebook page</b>	<b>Tailored Social Engineering Approach from a Hostile Actor Targeting Mary Doe on the Business Development Team</b>
I need a vacation because my boss is a jerk and is always mean to me.	“Mary, this is Jim from the IT Help desk. Can I get you to help me? I would ask your boss but he is really hard to deal with. I was hoping to get a friendly face.”
Went down to the Cape with some friends and had a great time. Went to Maquire’s and heard some awesome music.	“I’m not liking work today because I just got back from the Cape—some beers, some Irish music, some beach-time. It was great.”

The scenario above plausibly demonstrates that a couple of “lines” to build rapport with the target can greatly increase the chance that a social engineering approach would be successful. While the information gleaned from the hypothetical *Facebook* page seemed relatively innocuous, a hostile collector, armed with an accurate company roster and/or organization chart, can leverage social networking media to great effect. While one respondent was very specific in outlining the hypothetical example, all respondents acknowledged the potential of social networking media as a basis for follow-on actions for solicitation for information or access, either via social engineering or targeted internet malware attacks.

**2. Does Your Organization Have a Program to Identify and/or Mitigate the Insider Threat? If So, Describe That Program and How its Effectiveness is Gauged.**

All respondents indicated their organizations had a program to identify and mitigate the insider threat. The respondents working in business intelligence were not aware of the specifics of the program outside of some awareness training. The four

respondents working at the executive level with responsibility for security and/or operations provided a more in-depth understanding protecting against insider threat. The input from that subgroup is summarized in Table 5.

Table 5. The Respondents’ Organization’s Insider Threat Mitigation Programs

<b>Insider Threat Mitigation Program Technique</b>	<b>Number of Respondents Acknowledging the Use of Technique</b>
Awareness training (e.g., unusual behavior, atypical IT usage, personal or professional difficulties, reporting avenues)	4 of 4
IT processes to monitor and detect anomalous behaviors to trigger follow-on investigation	3 of 4
Integrated information flow across departments to assist in insider threat prevention (e.g., human resources, IT, security)	2 of 4

Insider threat awareness training was common to all seven respondents. Of the four respondents in the executive subgroup, three described a rather robust IT security effort to guard against hacking attacks while detecting unusual IT patterns. Two respondents highlighted a more holistic approach in preventing the insider threat problem. Both admitted the prime driver in the prevention effort was the prevention of workplace violence but emphasized the program methodology of monitoring for triggering employee behavior patterns and intra-department coordination is effective when trying to identify potential employees with potential to execute an insider attack.

**D. POLICES OR PROGRAMS REGARDING THE VULNERABILITY MITIGATION OF SOCIAL NETWORKING MEDIA**

**1. What Programs, Methodologies, or Technologies Could Be Used to Mitigate any Risk Introduced by the New Vulnerabilities of the Use of Social Networking Media by an Organization’s Employees?**

All of the respondents described methodologies very similar to the programs currently existing to counter the insider threat. Fundamentally, this would include awareness training to increase the understanding of the vulnerability of social networking media and its ability to enable social engineering attacks tailored to a specific target. Three of the respondents emphasized the need to make the training more “personal”

when demonstrating how social networking media can be used in a nefarious manner. The respondent that provided the hypothetical scenario in the write-up to question 7 offered it as a good example for inclusion in awareness training. Another respondent described the need to demonstrate how social networking media itself may be the vehicle to initiate a social engineering attack and mentioned the Robin Sage incident as an example to increase awareness.

All respondents agreed that banning the use of social networking media by employees, even among a smaller subset of critical employees, was not a realistic or practical mitigation strategy. To that end, one respondent showed a confidential report that stated the changing demographics of the workforce means more and more employees have been “raised on the Internet and socially networked...via *Facebook* and *Twitter*...(and) have developed an expectation for constant and immediate access to information” (SME2, 2011).

One respondent recommended scenario-based training that could be administered online. The training would demonstrate how threat actors could use information found on social networking media to target the employee. Emphasis would be given on all threats enabled by social networking media, including criminal (e.g., burglary while on vacation and crimes by child predators.) The awareness and mitigation strategies are equally effective for all threats enabled by social networking media and, therefore, more cost-effective from a security perspective.

Three respondents were aware of social networking media monitoring services but all mentioned they were expensive and, as such, were not feasible for widespread use for a large organization’s employees. Two of the respondents, with firms that conduct deep Web searches and social networking media searches for use as part of the screening process for hiring employees, indicated a limited and focused use of monitoring resources on critical personnel and programs would be very effective in understanding an organization’s attack surface. This is notwithstanding the complicating impact on employees of legal/privacy issues and the “big brother” perception of such a security program.



## **E. SUMMARY**

The results of the interviews demonstrated the potential vulnerabilities created by the features of social networking media but no evidence of actual attacks enabled by social networking media. The availability of the wealth of personal data in social networking media is the foundation of a process to target and exploit critical individuals within an organization. Information from social networking media enables social engineers to employ more refined techniques for intelligence collection. The respondents' proposed mitigation strategies include an awareness campaign for an organization's employees and a social networking media search process that identifies relevant information found on social networking media from a threat perspective to allow for a better understanding of an organization's or employee's attack surface. The thesis will examine the results offered by the experts and apply it through a framework of a human behavioral taxonomy suggested in the literature with the intention of identifying a potential mitigation strategy.

THIS PAGE INTENTIONALLY LEFT BLANK

## V. CONCLUSIONS

As the preceding chapters demonstrate, there is an accepted notion among the respondents and within relevant business literature that social networking media has become a very real and potent vulnerability when attempting to protect an organization's intellectual property and other sensitive information. All respondents were adamant in the view that the vulnerability was a critical one requiring a more thorough examination. Social networking media increase this vulnerability by expanding the attack surface into an organization and its members. Hostile actors can exploit the new, larger attack surface using existing techniques (e.g., spearphishing and social engineering) in a more focused and tailored manner when targeting individuals to gain access to high value information.

Outside of identity theft and phishing attacks, the research has uncovered a lack of evidence in both literature and among the respondents that describes a documented case where social networking media enabled an insider attack. This finding contrasts sharply with the seemingly widespread, almost intuitive understanding of the vulnerability introduced by social networking media. Of interest, however, is the fact that two of the respondents and some of the business literature (i.e., the DefCon summary and the FBI study) provided controlled or hypothetical examples of how social networking media could be exploited to enable a more effective social engineering attack. The relatively straightforward use of social networking media in these hypothetical examples is noteworthy for it begs the question of the cause of the lack of evidence of nefarious use of this information-gathering tool. Maybe there are better or more efficient ways to compromise an insider that do not require the use of social networking media.

Perhaps a case that involved the use of social networking media has not progressed through the process for litigation or prosecution. In other words, the offense might be way out in front of the defense for social networking media so there is no evidence available. The research for this thesis did not seek to provide an explanation for this lack of hard causal evidence.

While examples of the vulnerability of social networking media and the insider are not common, there is extensive research and understanding among the respondents regarding the use of social engineering and the insider threat. Most social engineering mitigation strategies have a foundation in raising awareness in employees through training and establishing good habits through policy to authenticate contacts via e-mail, phone, or face-to-face requests of sensitive information. Additionally, the literature and respondents emphasize an active IT monitoring process to detect anomalous employee IT-usage for further investigation by the security and IT teams.

Some of the literature and respondents went a step further in recommending a blending of inputs from across disciplines (e.g., human behavior, IT usage, personal stressors) to identify individuals with a higher risk for insider threat activity. The Greenmeier article described a process by which adverse workplace issues are made known to corporate security and the RAND study delineated an extensive taxonomy of insider threat predictive inputs. All of these mitigation strategies are rooted in a more holistic understanding of an organization's employees. An examination of the social networking media of critical employees can make the use of these blended security methodologies more feasible for it allows for a larger viewing window into the employee's life. Since social networking media could be used by employees to broadcast vulnerabilities and increase their attack surface to the hostile threat; it follows that the same insight can be gained by a proactive security methodology to attain awareness of the attack surface a potential threat might see. With this awareness comes the foundation for a mitigation strategy to decrease the vulnerability to social networking media for each critical employee.

The literature and research reveal an evolving environment of policies to regulate the use of social networking media by employees. Business literature and examples of policy provided by some of the respondents have commonalities that include training to make employees more aware of the hostile use of social networking media and directing employees to:

- Ensure the privacy settings on social networking sites are configured to limit posted information to confirmed ‘friends;’
- Avoid posting issues and information regarding the workplace; and
- Use common sense when posting sensitive, personal information online.

Outside of the social networking media policy framework described above, this thesis could not identify an active mitigation methodology to limit the attack surface introduced by social networking media. Of note are the existing services and technologies that comb social networking media and other internet applications for interesting or derogatory information on individuals to use the hiring process for organizations; including by some of the respondents’ organizations. These social networking media information ‘scraping’ programs are also used for nefarious means to tarnish political opponents or enable malware attacks. This thesis opines the technologies used by hostile actors to find the attack surface of key individuals should be used by organizations to understand the exactly what the threat “sees” via social networking media in order to limit or eliminate that vulnerability through personal vulnerability assessments.

This thesis will conclude by attempting to demonstrate a possible methodology that the threat actor would use to enable an insider attack, while specifically highlighting the use of social networking media in this effort. This thesis will then offer a mitigation strategy based on an analysis of an organization’s critical assets, a technical program to identify social networking media attack surfaces, and a tailored personal vulnerability assessment. Establishing the framework of a realistic attack strategy from the threat perspective allows the thesis to propose potential solutions to help lessen the vulnerability and decrease an organization’s attack surface within the world of social networking media.

#### **A. HOSTILE ACTOR METHODOLOGY FOR INFORMATION COLLECTION, TARGETING, AND SOCIAL ENGINEERING TO ENABLE THE INSIDER THREAT**

At its foundation, the threat actor’s goal is to acquire information that can translate into value for a potential client. At a briefing to the American Society of

Industrial Security, a representative from the FBI's Economic Espionage Unit described how every aspect of corporate intellectual property is "fair game, from aerospace to biological and agricultural secrets, and the thieves can be competitors or foreign nations" (Lengel, 2011).

Whether the threat actor is a foreign intelligence service or a cybercriminal, the essential starting point for a hostile attacker is having a good understanding of the nodes of value in the targeted organization. Therefore, under the assumption that an organization cannot protect everyone and everything all of the time, the initial step in establishing the threat methodology is to understand the target organization's vulnerabilities and possible consequences of a malicious attempt to gain insider access. This organizational vulnerability assessment would be then coupled with an evaluation of the consequences to an organization of a targeted attack. The nodes (e.g., people, data, or intellectual property) that would affect the greatest consequence are the nodes of highest value requiring the highest level of protection. A threat actor would implement an information-gathering operation to acquire the intelligence necessary to identify those high-value nodes and explore potential avenues of access into the same.

	Technology	Suppliers	Manufacturing	Financials	Personnel	Publishing
Vulnerabilities	<ul style="list-style-type: none"> <li>•Software</li> <li>•Hardware</li> <li>•R&amp;D</li> <li>•Patents</li> </ul>	<ul style="list-style-type: none"> <li>•Distribution network</li> <li>•Component providers</li> </ul>	<ul style="list-style-type: none"> <li>•Methods</li> <li>•Supply Chain</li> </ul>	<ul style="list-style-type: none"> <li>•Strategies</li> <li>•Contracts</li> <li>•Mergers &amp; Acquisitions</li> </ul>	<ul style="list-style-type: none"> <li>•Executive Leadership</li> <li>•IT</li> <li>•Human Resources</li> <li>•IP Creators</li> </ul>	<ul style="list-style-type: none"> <li>•Records</li> <li>•Databases</li> <li>•Internet</li> <li>•Social Media</li> </ul>
Consequences	<ul style="list-style-type: none"> <li>•Market leadership</li> <li>•Litigation</li> <li>•Loss from counterfeit</li> </ul>	<ul style="list-style-type: none"> <li>•Loss of distribution network</li> <li>•Loss of component providers</li> </ul>	<ul style="list-style-type: none"> <li>•Counterfeit and manufacturing loss</li> <li>•Supplier disruptions</li> </ul>	<ul style="list-style-type: none"> <li>•Brand reputation</li> <li>•Lost customers</li> <li>•Increased M&amp;A costs</li> </ul>	<ul style="list-style-type: none"> <li>•Employee loss to competitors</li> <li>•IT vulnerabilities</li> <li>•IP leakage</li> </ul>	<ul style="list-style-type: none"> <li>•Exposure of strategies, contract details, personnel information</li> </ul>

Figure 3. The Vulnerabilities and Consequences of Certain Industries or Segments of an Organization (From Tailored Solutions & Consulting, 2010)

The threat actor would seek to acquire a broad understanding of the entirety of an organization and start honing in on the specific nodes of highest value. Open source material (e.g., company websites, industry trade journals, industry conferences, tax records, and required financial filings) can provide a wealth of general information on an organization’s leadership, strategy, and relative financial health. In addition, business competitive intelligence firms are often leveraged to drill down to acquire more detailed information regarding organization charts, current and former employees, patents, etc.

Armed with this general targeting information, a social engineer would initiate efforts to acquire sensitive company information using many of the techniques outlined in previous chapters in this thesis; such as making deceitful phone calls or e-mails and otherwise “connecting” to the unwitting employees using the acquired names of senior executives, IT persons and processes, and inside company verbiage. In summary, Figure 4 shows this traditional methodology to acquire access and insider information is a two-step process: 1) acquisition of target organization information, and; 2) execution of social engineering attacks to gain access to sensitive information.



Figure 4. Existing Threat Process to Acquire an Organization’s Insider Information

The advent of the widespread use of social networking media allows for the addition of entire step between the two existing processes that makes a social engineering attack more likely to succeed; the use of social networking media for the acquisition of the personal information of critical employees (Figure 5).



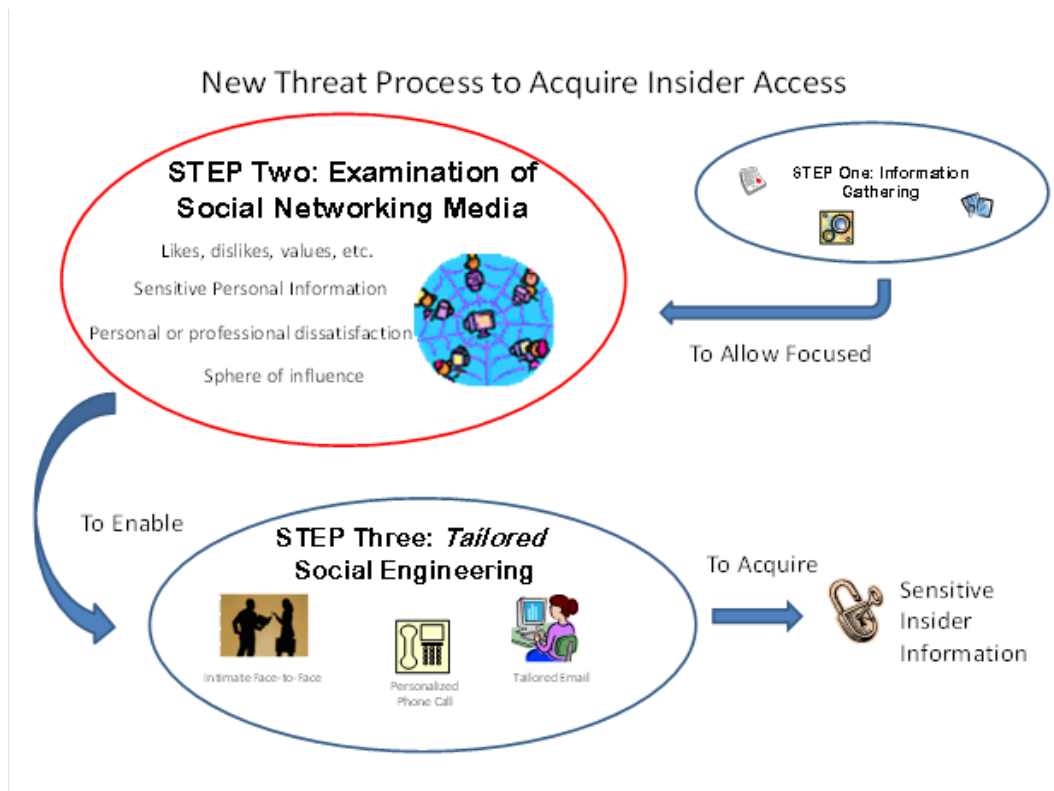


Figure 5. New Threat Process to Acquire an Organization’s Insider Information Using Information from Social Networking Media

Literature such as the ComSec report, the FBI study, and the DefCon summary, reviewed in a previous chapter, clearly delineated the capacity of social networking media to identify the sphere of influence or inner trust circle of a targeted individual and its importance to enable exploitation by social engineering techniques. All respondents agreed that social networking media would make social engineering attacks far more likely to succeed. Their responses for this increase of effectiveness mirror that of the literature; social networking media allows for a better understanding of the target’s personal relationships; a more complete awareness of the target’s value set; and detailed personal information on the goings-on in the target’s life.

The FBI study and interview data provide hypothetical or controlled examples of the manner in which data can be harvested from social networking media sites. This thesis has concluded that social networking media clearly can make the use of social

engineering methodologies more effective in acquiring sensitive inside information. The thesis will propose some mitigation strategies based on existing literature and the data from the respondents.

## **B. POTENTIAL PROGRAMS, POLICIES, AND TECHNOLOGY TO HELP LESSEN THE VULNERABILITY TO SOCIAL NETWORKING MEDIA**

The need for training and awareness to lessen the vulnerability of social networking media and social engineering among an organization's employees was echoed in both the literature and by all respondents interviewed for this thesis. The training should inform an employee on how to limit the attack surface presented on social networking media. The techniques to limit information should be rooted in policy specific to employee use of social networking media. In addition, training should make employees aware of social networking media's capacity to provide a wealth of personal data that enables social engineers to target insider information and common criminals to find an easy mark. The training could be scenario-based and personalized to give its impact more weight. By limiting the amount of information available on social networking media, the training reduces the total vulnerability by creating a barrier to exploitable personal information (Figure 6).



Figure 6. Training Creates a Barrier to the Volume and Type of Information Found on Social Networking Media

The training should include simple steps such as not accepting the usually less secure default settings for viewing your social media page; limiting the posting of identifying information (e.g., SSN, address, usernames) and excessive personal and professional information; and ignoring “friend” requests from unknown parties.

By having the training include an awareness of social engineering techniques, the vulnerability of the exploitation of information gathered on social networking media would be reduced. The training decreases vulnerability from steps two to three of the threat methodology slide by emphasizing the need to establish the bona fides of a contact who asks for sensitive company or customer information and be wary of a new contact with many similarities shown in Figure 7. This is an application of already existing social engineering awareness training.

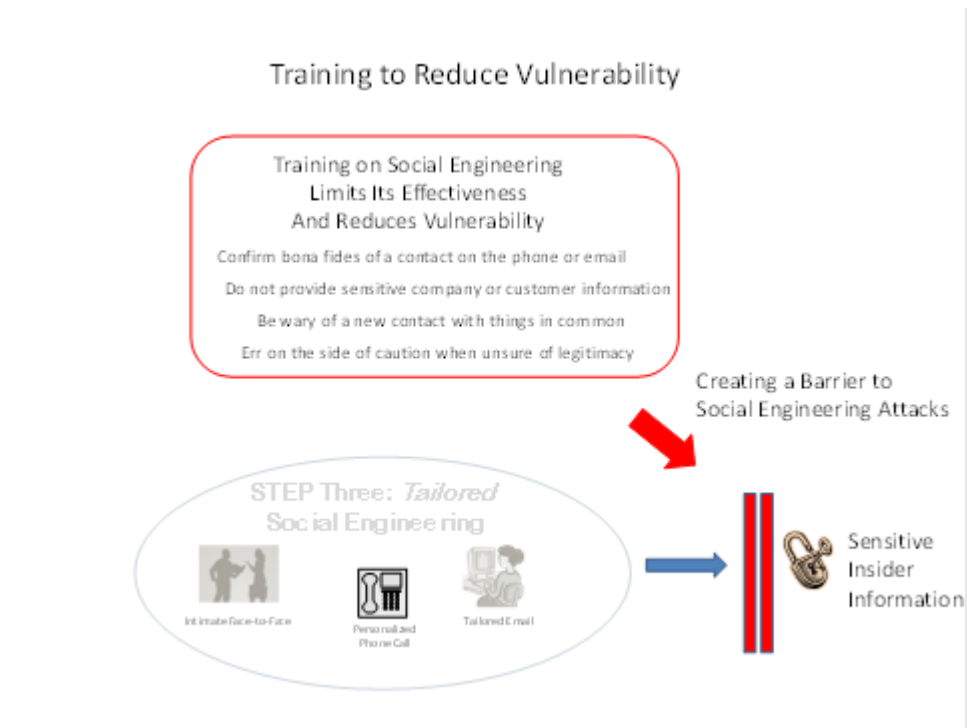


Figure 7. Training Limits the Effectiveness of Social Engineering Techniques

In addition to a training and awareness program, this thesis proposes an active assessment program for identified critical employees to gauge social networking media exposure. Fundamental to this program is an understanding of the organization’s nodes of high consequence. Some examples of critical employees might be lead engineers on next-generation technology development teams, merger and acquisition analysts and negotiators, senior executives, or experienced IT security and operations personnel. For each of these critical persons, a survey of open source and social networking information could be gathered for that individual and their inner trust circle. Acquiescence to being subject to such a survey would be a condition of employment for being in one of these critical positions.

### C. Technical Applications

Three of seven respondents highlighted the need to make the mitigation strategy more personal to the employees. The literature and respondents made mention of technologies that monitor the internet and social networking sites to acquire information

on target individuals or companies. This thesis advocates the use of these technologies to survey employees identified as critical nodes of value for their open source and social networking media footprint. This collected data, coupled with some rudimentary analysis of the employee's friends and family, would most certainly make the vulnerability awareness more personal. In addition, the survey would be used as the basis for a briefing on how a social engineering attack or criminal action could be tailored to that targeted individual. Finally, the briefing would recommend actions to be taken to reduce vulnerability and exposure to hostile actors.

Prior to its implementation, the organization would have to make the legal and privacy concerns clear to the employee by defining the nature of the program and its intended purpose, the extent to which the collected data would be used, and its policy for storage and protection. The vulnerability assessment and risk mitigation program could be included as a condition of employment in certain critical positions within the organization; much like U.S. government clearances requires candidates to waive certain privacy restrictions during the background checks. The program should specify that it would only search publically available information to determine an employee's vulnerability, although it should note that a criminal would not be under any such restriction.

A hypothetical *Vulnerability Assessment and Risk Mitigation Report* (shown in Appendix) would form the foundation of the security briefing to a critical employee. In this case, the report was created for an engineer on a team developing a critical piece of technology. The report is designed to alert the employee to the type of publically available personal and professional information on social networking media, a possible attack scenario to be used by a hostile actor, and steps to take to lessen the vulnerability and mitigate that risk.

### **C. LIMITATIONS AND OPPORTUNITIES FOR FURTHER RESEARCH**

The mitigation strategies of training and active survey of select employees await refinement and validation that would follow the introduction of this model in an organization with insider threat concerns. Ideally, the organization could then be

compared other similar organizations in size and industry to gauge the effectiveness of the proposed mitigation strategy. Results of this follow-on research could attempt to measure positive and negative impacts to security and productivity, relative costs, and relative expenditure of security resources and training time. Other limitations include the fact some of the respondents were familiar with the results of the FBI study that highlighted a controlled example of the use of social networking media to acquire an organization's sensitive information—perhaps causing a bias toward validating this hypothesis of this thesis (Federal Bureau of Investigation, 2010). Further research could draw upon a larger pool of respondents, perhaps from a wider range of industries or professions to mitigate these potential biases. In addition, follow-on research could explore the cause of the lack of hard evidence of the use of social networking media as an enabler for the insider threat when the research in this thesis points to social networking media's great potential to enable the same.

#### **D. SUMMARY**

This thesis suggests the impact of theft of intellectual property on the U.S. economy is very much a homeland security issue due to the size of the loss annually. Competitors and foreign adversaries are actively targeting U.S. industry to acquire trade secrets to undercut U.S. business in the marketplace. Of primary concern in this endeavor is an insider's betrayal of an organization, witting or unwitting, by providing sensitive information to a hostile outsider that negatively impact an organization.

A common existing technique to enable this breach of sensitive information is social engineering—the attempt to elicit sensitive information by obscuring the true motivation and/or identity behind the request. The research indicates that social engineering, when coupled with the new and widespread use of social networking media, can be made more effective through exploiting the wealth of information found on the social networking sites to more selectively target critical individuals with a tailor-made message to reduce suspicion. The business literature and interviews of industry experts give credence to this increased vulnerability.

Relevant to any mitigation application within private industry are the requirements mandated by SOX and the SEC to protect intangible assets demonstrably. The pressure from these regulations should be a catalyst for business to seek new and cost effective methods to identify threat and reduce vulnerability. The combination of relatively inexpensive open source and social media examinations and the SOX requirements could make this a readily applied model, if shown to be effective.

The pervasiveness of social networking media cannot be ignored when developing a security program to limit its impact on an organization's vulnerability to the insider threat. This thesis proposes a mitigation and prevention strategy that couples training and awareness with active surveys and monitoring of critical persons within an organization. This thesis does not claim, however, to provide a perfect solution to the insider threat enabled by a system as complex as social networking media; it is only the start of a long process of trial and error as business and government grapple with this new communications medium. "Let's make mistakes in a good direction," describes the trial and error approach as the ideal technique for arriving at a solution to a difficult problem in a challenging, complex environment (Harford, 2011). This thesis has strived to be a "mistake in a good direction" in understanding the vulnerability of social networking media and mitigating its impact on the insider threat.

## **E. EPILOGUE**

John was excited about taking the job as a materials engineer on the US Aerospace NexGenCF team. It paid well and the work seemed very cutting-edge. As part of the condition of employment, he signed a waiver for the security people to conduct an assessment of his Internet footprint. Now, as John sat in his confidential security briefing looking at the two-page assessment of his life—his jaw dropped. He could not believe how the report was able to construe an accurate profile of exactly what he was about. It really was shocking. John readily agreed to follow the mitigation strategy and was suddenly was less naïve and more aware of possible bad actors using social networking media.

A few years had passed, and John had settled into his job and the Seattle scene quite well. Money was a little tight, but he was having a great time. John had a faded memory of that security briefing provided by US Aerospace but he had tried to be careful and not post information about work. On the way back from the local coffee house one day, John was reflecting on the coincidence of meeting that girl Robin in the Bears jersey. She seemed great but there was something about her overt friendliness that he thought was a bit off. John considered it somewhat paranoid to give any credence to that US Aerospace security briefing, but this Robin person sure did fit the profile. On the other hand, she might just be really Midwestern-friendly and that spy stuff never really happens to normal people anyways. John ignored his suspicions and looked forward to possibly getting some Bears tickets.

Sometime after their meeting at the coffee house, John received an e-mail from Robin requesting sensitive company IT information in the form of an “anonymous” survey . His stomach tightened. John now knew Robin was the not the real deal and she was up to no good. John went straight to his boss and corporate security to discuss the series of interactions with Robin. The US Aerospace Director of Security, a former FBI Special Agent-in-Charge, briefed the senior executives and recommended an active partnership with the FBI to help permanently neutralize this threat. With the CEO’s approval, US Aerospace security called the FBI and assisted in developing an active economic espionage investigation. The investigation entailed the introduction of an undercover Special Agent as a fellow US Aerospace employee. John and the undercover agent laid the groundwork for meeting Robin.

Next weekend at the Roaster, John showed up with Rob, his “good friend” from work. They quickly spotted Robin. After sitting down, Rob and Robin seemed to hit it off straight away. It got to the point where John excused himself and left Rob and Robin sitting at the coffeehouse chatting about work and travel. John found a new coffeehouse to frequent about two blocks away—not a tall order in Seattle. He never talked to Robin again.

Two years later, the Department of Justice released a press statement in which four people were sentenced to six years in federal confinement for committing economic



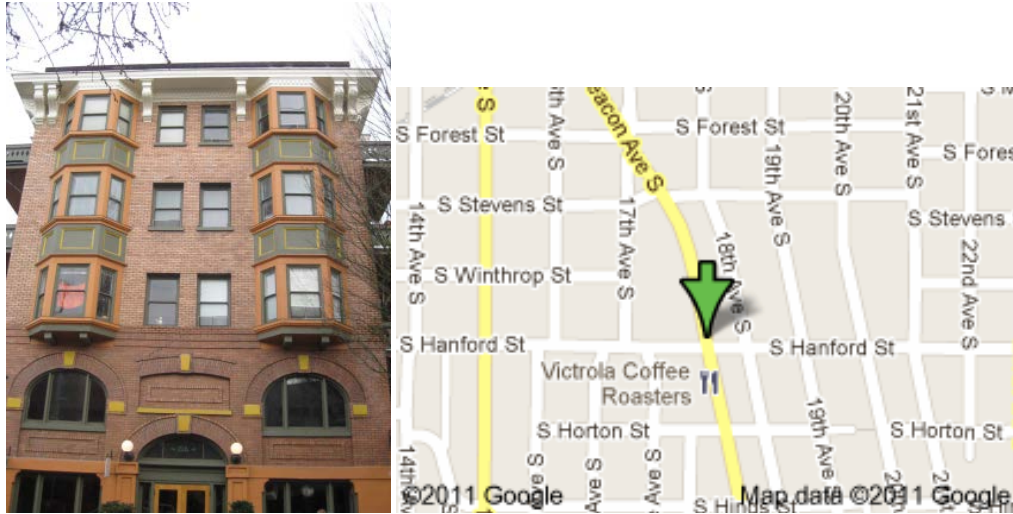
espionage in violation of Title 18 US Code Section 1831. The U.S. attorney hailed this case as a stellar example of cooperation between private industry and the U.S. government. Security experts noted the manner in which US Aerospace became aware of the hostile effort—through an effective and preventative insider threat program based, in part, on the understanding of the use of social networking media. John read the press release while sitting in one of his new fuel-efficient US Aerospace jets on a flight back to Chicago for a Bears’ playoff game. He smiled, logged-off *Facebook*, and closed his eyes.

THIS PAGE INTENTIONALLY LEFT BLANK

**APPENDIX. VULNERABILITY ASSESSMENT AND RISK MITIGATION REPORT FOR JOHN Q. PUBLIC, NEXGENCF TEAM, US AEROSPACE**

**General Background:** male, white, age: 27, dob: 6/10/84, pob: Illinois (Chicago area), parents: Robert and Mary Public (Naperville IL), sister: Sarah Public, age 21 (Champaign IL)

**Current Address:** 3174 Beacon Avenue South, Seattle, WA



**e-mail:** [jpublic1984@gmail.com](mailto:jpublic1984@gmail.com), [john.public@usaerospace.com](mailto:john.public@usaerospace.com), [jpillini@yahoo.com](mailto:jpillini@yahoo.com);  
**phone:** 206-555-1433(c), 206-321-1234(w)

**Professional Background:** 1996 B.S. mechanical engineering- Univ of Illinois 3.5 GPA, 1998 M.S. materials engineering-Univ of Illinois; employed three yrs U.S. aerospace as materials engineer—NexGenCF structural materials team

**Personal Background:** Avid Chicago sports fan—esp. Bears; “loves” traveling around Europe; golf; skiing; recently purchased a 2008 Porsche; active social life

**Contacts Based on Social Networking Posts:** 1) [twjohnson23@gamil.com](mailto:twjohnson23@gamil.com) , Tammi Johnson, Seattle WA, age 25, (25 posts in last 30 days); 2) [sarahp1990@gmail.com](mailto:sarahp1990@gmail.com), Sarah Public, Champaign IL, age 21, (15 posts in last 30 days); 3) [Irishgirlpower@gmail.com](mailto:Irishgirlpower@gmail.com), Kerry Rooney, age 28, (10 posts in last 30 days)

**Communications of note:** “I may have to pass on the ski trip. M/D talking about cutting my \$\$\$ off.” “Car needed a new thermostat. \$785. Wow!” “Whistler was out of control with Skid and the boyz. That’s what CCs are for!” “Another hangover morning at the Roaster.”

**Personal photos of note:**



### **Attack Avenue Analysis**

**Relevant US Aerospace Vulnerability from Open Source Research:** Patent applications and aerospace business journals indicate NexGenCF is US Aerospace’s advanced carbon fiber research to enable construction of lighter, stronger and more fuel-efficient aircraft. Reports indicate over \$250m of development since 2008. The material would “revolutionize” aircraft construction and is a key part of the US Aerospace long-term plan in the global marketplace.

**Critical Employee Vulnerability:** High probability that finances to support lifestyle are not sound. Enjoys higher-end travel (golf and skiing), expensive cars, drinking/partying.

**Possible Attack Profile:** Manufacture a bump (female preferred) at Victoria Coffee Roaster’s (3220 Beacon Ave S, Seattle WA) on a Sat or Sun morning wearing Chicago Bears apparel. Discuss football, Chicago, and skiing. Future offer to make money for work IT information re: what OS, A/V, etc.; possibly via a job interview or survey. Continue to solicit information while paying or offering free “comps.” Once ready, pass handling to a Business Consultant representing overseas clients.

### **Risk Mitigation Steps:**

1. Conduct personalized awareness briefing with agreement to modify social networking media profile with an emphasis on understanding the reporting procedures regarding any solicitation of information
2. Reexamine in 14 days social networking media to ensure elimination of financial references and specific work team involvement (e.g., Nex Gen CF)
3. Employee Assistance Program reference to financial counseling

4. Heighten alertness for the coincidence of social contacts with many personal commonalities that have a focused interest in work information (e.g., IT procedures, project, access to information)

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF REFERENCES

- Acohido, B. (2011, March 31). *Social media tools used to target corporate secrets*. Retrieved April 4, 2011, from <http://www.usatoday.com/tech/news/2011-03-31-hacking-attacks-on-corporations.htm?csp=obnetwork>
- Allen, P. (2007, January 1). Taking data security to heart: The NYSE Group adopts a “defense-in-depth” strategy to secure sensitive data and comply with Sarbanes-Oxley. *Wall Street & Technology*, p. 22.
- Aritron, Inc. & Edison Research. (2011, March 24). *Media Surveys*. Retrieved April 23, 2011, from [http://www.edisonresearch.com/home/archives/2011/03/facebook\\_achieves\\_majORITY.php](http://www.edisonresearch.com/home/archives/2011/03/facebook_achieves_majORITY.php)
- ASIS. (2007, August). *Trends in proprietary information loss*. Retrieved October 22, 2010, from <http://www.asisonline.org/newsroom/surveys/spi2.pdf>
- Baker, W., Hutton, A., Hylendar, C., Pamula, J., Porter, C., & Spitler, M. (2011). *2011 Data breach investigations report*. New York: Verizon Business.
- Bishop, M., Engle, S., Peisert, S., Whalen, S., & Gates, C. (2009). Case studies of an insider framework. *Proceedings of the 42nd Hawaii International Conference on System Sciences 2009*. Big Island, HI: University of Hawaii at Manoa.
- Brackney, R. & Anderson, R. (2004). Understanding the insider threat. *Proceedings of a March 2004 Workshop* (pp. 1–113). Rockville, MD: RAND National Security Division.
- Catrantzos, N. (2009). *No dark corners: Defending against insider threats to critical infrastructure*. M.S. thesis, Naval Postgraduate School, Monterey, CA.
- comScore, Inc. (2011). *The 2010 U.S. digital year in review*. Reston, VA: comScore, Inc.
- Department of Homeland Security. (2010a). *Insider threat detection and mitigation: CSRD: DHS*. Retrieved December 13, 2010, from [http://www.cyber.st.dhs.gov/insider\\_threat.html](http://www.cyber.st.dhs.gov/insider_threat.html)
- Department of Homeland Security. (2010b). *Quadrennial Homeland Security Review Report*. Washington, DC: Author.
- Department of Justice. (2011a, February 8). *Computer crime and intellectual property section*. Retrieved April 23, 2011, from <http://www.justice.gov/criminal/cybercrime/linSent2.pdf>

- Department of Justice. (2011b, April 11). *Cyber crime and intellectual property section*. Retrieved April 23, 2011, from <http://www.justice.gov/criminal/cybercrime/youSent2.pdf>
- Drew, C. (2010, October 17). New spy games: Firm's secrets sold overseas. *New York Times*. Retrieved October 21, 2010, from [http://www.nytimes.com/2010/10/18/business/global/18espionage.html?\\_r=1](http://www.nytimes.com/2010/10/18/business/global/18espionage.html?_r=1)
- Eggen, D. (2011, March 7). Dirty-tricks campaigns get boost from digital sleuths. *The Washington Post*, p. A3.
- Federal Bureau of Investigation. (2010, Summer). FBI Business Alliance Presentation - Social Media and Open Source Collection. *Open Source Research Project - PowerPoint Presentation*. Washington, DC: USA: Federal Bureau of Investigation.
- Federal Bureau of Investigation. (2011a, February 17). *FBI: Albany Division*. Retrieved July 12, 2011, from <http://www.fbi.gov/albany/press-releases/2011/former-bristol-myers-employee-sentenced>
- Federal Bureau of Investigation. (2011b). Social network sites and the FBI employee guidance. Washington, DC: Federal Bureau of Investigation, Security Division.
- Federal Bureau of Investigation. (2010). *Strategic partnerships: FBI*. Retrieved December 14, 2010, from <http://www.fbi.gov/about-us/investigative/counterintelligence/strategic-partnerships>
- Frost, J. (2011, April 26). *The tweeter who loved me*. Retrieved July 12, 2011, from <http://www.pbs.org/wnet/need-to-know/voices/the-tweeter-who-loved-me/8859/>
- Graves, K. (2010). *CEH: Certified ethical hacker*. Indianapolis, IN: Wiley Publishing, Inc.
- Greenemeier, L. (2006, December 11). Insider threats; To head them off, consider the psychology and technology behind the attacks. *InformationWeek*, 25.
- Gudaitis, T. (1998). The missing link in information security: Three dimensional profiling. *CyberPsychology & Behavior*, 1(4), 321–340.
- Hadnagy, C. J., Aharoni, M., & O’Gorman, J. (2011, March 23). *DefCon 18*. Retrieved April 23, 2011, from [http://www.social-engineer.org/resources/sectf/Social-Engineer\\_CTF\\_Report.pdf](http://www.social-engineer.org/resources/sectf/Social-Engineer_CTF_Report.pdf)
- Harford, T. (2011, July). *Trial, error and the God complex*. Retrieved July 26, 2011, from [http://www.ted.com/talks/tim\\_harford.html](http://www.ted.com/talks/tim_harford.html)



- Huber, M., Kowalski, S., Nohlberg, M., & Tjoa, S. (2009). *Towards automating social engineering using social networking sites*. Retrieved July 13, 2011, from <http://www.sba-research.org/wp-content/uploads/publications/2009 - Huber - Towards Automating Social Engineering Using Social Networking Sites.pdf>
- Institute of Internal Auditors. (2008, January). *Sarbanes-Oxley Section 404: IIA*. Retrieved December 13, 2010, from <http://www.theiia.org/download.cfm?file=31866>
- Kirk, J. (2011, February 11). *Night dragon attacks from China energy companies*. Retrieved July 12, 2011, from [http://www.pcworld.com/businesscenter/article/219251/night\\_dragon\\_attacks\\_from\\_china\\_strike\\_energy\\_companies.html](http://www.pcworld.com/businesscenter/article/219251/night_dragon_attacks_from_china_strike_energy_companies.html)
- Lengel, A. (2011, February 8). *FBI agent warns business sector of theft of trade secrets*. Retrieved July 18, 2011, from <http://www.ticklethewire.com/2011/02/08/fbi-agent-warns-business-sector-of-threat-of-theft-of-trade-secrets/>
- Levy, S. (2011, July 26). *Steven Levy on letting bots do our tweeting for us*. Retrieved August 29, 2011, from Wired Magazine: [http://www.wired.com/magazine/2011/07/pr\\_levy\\_socialbot/](http://www.wired.com/magazine/2011/07/pr_levy_socialbot/)
- MadIrish.net. (2008, March 20). *Hacking Penetration Testing*. Retrieved July 11, 2011, from <http://www.madirish.net/?article=188>
- Magkarlas, G. & Furnell, S. (2002). *A preliminary model of end user sophistication for insider threat prediction in IT systems*. Plymouth, UK: University of Plymouth.
- Mark, D. (1997, Fall). Competitive intelligence and the corporate jewels. *Competitive Intelligence Review*, 62–70.
- Microsoft TechNet. (2006). *How to protect insiders from social engineering threats*. Redmond, WA: Microsoft Corporation.
- Mitnick, K. D. (2002). *The act of deception: Controlling the human element of security*. Indianapolis, IN: Wiley Publishing, Inc.
- Newman, B. (2007, November/December). *Business law today: ABA*. Retrieved December 13, 2010, from <http://www.abanet.org/buslaw/blt/2007-11-12/newman.shtml>
- Newton, P. (2005, December 9). Questions of trust. *Utility Week*, 22.
- Noonan, T. & Archuleta, E. (2008). *The insider threat to critical infrastructure*. Washington, DC: National Infrastructure Advisory Council.

- Office of the United States Intellectual Property Enforcement Coordinator. (2010, August). *Intellectual Property Spotlight*. Retrieved October 22, 2010, from [http://www.whitehouse.gov/sites/default/files/omb/assets/intellectualproperty/IPEC\\_Spotlight\\_August2010.pdf](http://www.whitehouse.gov/sites/default/files/omb/assets/intellectualproperty/IPEC_Spotlight_August2010.pdf)
- Preston, J. (2011, July 20). Social media history becomes new job hurdle. *New York Times*. Retrieved July 26, 2011, from [http://www.nytimes.com/2011/07/21/technology/social-media-history-becomes-a-new-job-hurdle.html?\\_r=2&smid=tw-nytimes&seid=auto](http://www.nytimes.com/2011/07/21/technology/social-media-history-becomes-a-new-job-hurdle.html?_r=2&smid=tw-nytimes&seid=auto)
- Puleo, A. J. (2006). *Mitigating insider threat using human behavior influence models*. Wright-Patterson AFB, OH: Air Force Institute of Technology.
- Randazzo, M., Keeney, M., Kowalski, E., Cappelli, D., & Moore, A. (2004). *Insider threat study: Illicit cyber activity in the banking and finance sector*. Washington, DC: United States Secret Service.
- Ryan, T. (2010). *Getting in bed with Robin Sage*. Seattle, WA: Blackhat USA.
- Schulz, E. E. (2002). A framework for understanding and predicting insider attacks. *Computers & Security*, 526–531.
- Shaw, E. (2006). The role of behavioral research and profiling in malicious cyber insider investigations. *Digital Investigation*, 20–31.
- Shaw, E. & Fischer, L. (2005). *Ten tales of betrayal: The threat to corporate infrastructure by information technology insiders: Analysis and observations*. Monterey, CA: Defense Personnel Security Research Center.
- Shankland, S. (2007, September 4). *Geotagging links photos to locales*. Retrieved August 29, 2011, from Cnet News: [http://news.cnet.com/Geotagging-links-photos-to-locals/2100-1041\\_3-6205734.html](http://news.cnet.com/Geotagging-links-photos-to-locals/2100-1041_3-6205734.html)
- Symantec, Inc. (2011). *Symantec Internet threat report - volume 16*. Retrieved June 20, 2011, from Symantec.com: <http://www.symantec.com/business/threatreport/index.jsp>
- Tailored Solutions & Consulting. (2010, August 19). Taking a proactive approach to managing risk. *IP3 Solutions*. Silver Spring, MD, USA: Tailored Solutions & Consulting.
- Toma, C., Hancock, J., & Ellison, N. (2008, August). Separating fact from fiction: An examination of deceptive self-presentation in online dating profiles. *Personality and Social Psychology Bulletin*, pp. 1023–1036.

- U.S. Chamber of Commerce. (2010). *Homeland security and defense issues*. Retrieved October 21, 2010, from <http://www.uschamber.com/issues/defense>
- University of California at Berkeley. (2010, January 8). *Invisible or deep web: What it is, how to find it, and its inherent ambiguity*. Retrieved August 4, 2011, from <http://www.lib.berkeley.edu/TeachingLib/Guides/Internet/InvisibleWeb.html>
- Waterman, S. (2010, July 18). Fictitious femme fatale fooled cybersecurity. *Washington Times*. Retrieved July 25, 2011, from <http://www.washingtontimes.com/news/2010/jul/18/fictitious-femme-fatale-fooled-cybersecurity/>
- White House. (2010, June). *White House: Intellectual property*. Retrieved July 12, 2011, from [http://www.whitehouse.gov/sites/default/files/omb/assets/intellectualproperty/intellectualproperty\\_strategic\\_plan.pdf](http://www.whitehouse.gov/sites/default/files/omb/assets/intellectualproperty/intellectualproperty_strategic_plan.pdf)
- Zalalichin, S., Efrati, R., & Cohen, T. (2010). *The social networking corporate threat*. Retrieved July 13, 2011, from <http://www.comsecglobal.com/FrameWork/Upload/The Social Networking Corporate ThreatComsec.pdf>

THIS PAGE INTENTIONALLY LEFT BLANK

## **INITIAL DISTRIBUTION LIST**

1. Defense Technical Information Center  
Ft. Belvoir, Virginia
2. Dudley Knox Library  
Naval Postgraduate School  
Monterey, California