Unintentional Insider Threat: Contributing Factors, Observables, and Mitigation Strategies

Frank L. Greitzer,
PsyberAnalytix
Frank@PsyberAnalytix.com

Jeremy Strozer, Sholom Cohen, John Bergey, Jennifer Cowley, Andrew Moore, and David Mundie
Software Engineering Institute, Carnegie Mellon University
jrstrozer@sei.cmu.edu, sgc@sei.cmu.edu, jkb@sei.cmu.edu,
jcowley@cert.org, apm@cert.org, dmundie@cert.org

Abstract

Organizations often suffer harm from individuals who bear them no malice but whose actions unintentionally expose the organizations to risk in some way. This paper examines initial findings from research on such cases, referred to as unintentional insider threat (UIT). The goal of this paper is to inform government and industry stakeholders about the problem and its possible causes and mitigation strategies. As an initial approach to addressing the problem, we developed an operational definition for UIT, reviewed research relevant to possible causes and contributing factors, and provided examples of UIT cases and their frequencies across several categories. We conclude the paper by discussing initial recommendations on mitigation strategies and countermeasures.

1. Introduction

A significant proportion of computer and organizational security professionals believe insider threat is the greatest risk to their enterprise, and more than 40% report that their greatest security concern is employees accidentally jeopardizing security through data leaks or similar errors [1]. This paper examines the unintentional insider threat (UIT) problem by developing an operational definition, reviewing relevant research to gain a better understanding of its causes and contributing factors, providing examples of UIT cases and the frequencies of UIT occurrences across several categories, and discussing initial recommendations on potential mitigation strategies and countermeasures. Because this research topic has largely been unrecognized, a major goal of this study is to inform government and industry stakeholders about the problem and its potential causes and to guide research and development (R&D) investments toward the highest priority R&D requirements for countering UIT.

The CERT® Insider Threat team, part of Carnegie Mellon University's Software Engineering Institute, conducted an initial research project [2] by examining relevant research papers and collecting UIT cases from public sources, in addition to cases that are in the CERT insider threat database. The present paper reports results obtained in the initial research and includes a simple template for sharing information about such threats and extracting data about them for inclusion in the CERT insider threat database, a feature model that categorizes recognizable characteristics of threats, and implications for possible mitigation strategies.

2. Definition of UIT

We use the following working definition of UIT:

> *An unintentional insider threat is (1) a current or former employee, contractor, or business partner (2) who has or had authorized access to an organization's network, system, or data and who, (3) through action or inaction without malicious intent, (4) unwittingly causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's resources or assets, including information, information systems, or financial systems.*

Malicious intent requires the intention to cause harm. Harm can also be caused by those who have no malicious intent (i.e., are nonmalicious), either by action or inaction, even if they knowingly break a rule (e.g., the guard who fails to check all badges does not mean to allow a malicious actor into the

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

978-1-4799-2504-9/14 $31.00 © 2014 IEEE
DOI 10.1109/HICSS.2014.256

building, but he lets someone in who sets the building on fire). An organization's resources or assets include people, organizational information including protected personal information and intellectual property, financial data, and information systems.

A *UIT incident* typically results from actions (or lack of action) by a nonmalicious insider (although not all such cases are characterized as completely nonmalicious, and individuals involved may not always be identified). We use the term UIT *threat vectors*[1] to identify different types of UIT incidents:

- DISC, or accidental disclosure (e.g., via the internet)—sensitive information posted publicly on a website, mishandled, or sent to the wrong party via email, fax, or mail
- UIT-HACK, or malicious code (UIT-HACKing, malware/spyware)—an outsider's electronic entry acquired through social engineering (e.g., phishing email attack, planted or unauthorized USB drive) that enables an attack carried out via software, such as malware and spyware
- PHYS, or improper/accidental disposal of physical records—lost, discarded, or stolen non-electronic records, such as paper documents
- PORT, or portable equipment no longer in possession—lost, discarded, or stolen data storage device, such as a laptop, PDA, smart phone, portable memory device, CD, hard drive, or data tape

2. Research literature review on contributing factors

We reviewed relevant research to identify possible contributing factors and begin to define mitigation strategies. A useful way to organize existing research is to map out possible causes and factors (contributing factors), which span a continuum between the culminating action by the UIT and the series of conditions, incidents, and failures that led to this failure. Table 1 summarizes research relevant to these factors (first column). In addition, the table describes means of observing or measuring the factors (second column) and possible mitigation strategies (third column, discussed in Section 5).

[1] We use term *threat vector* instead of *attack vector* because the word *attack* connotes malicious intent, which is absent in in the present context of unintentional acts by insiders.

2.1. Organizational factors

A major part of the UIT definition is the failure in human performance. While human errors can never be eliminated completely, they can be dramatically reduced through human error mitigation techniques. Such techniques should focus on system conditions that contributed to, or even made inevitable, the resulting errors and adverse outcomes. At the organizational level, these factors may be grouped into the following broad categories [3]: *data flow*—inadequate procedures or directions and poor communication; *work setting*—insufficient resources, poor management systems, and inadequate security practices; *work planning and control*—job pressure, time factors, task difficulty, change in routine, poor task planning and management practice, and lack of knowledge, skills, and ability; *employee readiness*—inattention, stress and anxiety, fatigue and boredom, illness and injury, drug and hormone side effects, values and attitudes, and cognitive factors.

Problems associated with organizational factors, such as work setting, management systems, and work planning, impact employee performance. For example, job stress [4] and time pressure [5] negatively affect performance; heavy and prolonged workload can cause fatigue, which adversely affects performance [6]; and in the presence of high email loads, users are more likely to respond to phishing email [7]. Organizational systems (particularly security systems) are often difficult and confusing [8]; systems that are difficult to use are less likely to be used [9]. Defensive measures may not detect well-implemented and sophisticated threats (such as malicious websites) [10]. Organizations are challenged to keep defensive measures and employee training up to date with changing strategies used by malicious adversaries; at least with respect to phishing threats, organizations can impact phishing susceptibility through antiphishing education [11].

2.2. Human factors

Despite organizations' efforts to apply best practices, the systemic, more distal organizational contributing factors may lead to more immediate proximal precursors to UIT incidents. Organizational factors that increase stress may in turn lead to cognitive impacts such as narrowing of attention (attending to fewer cues) [12], [13] and reduced working memory capacity [14]–[16]. Cognitive factors associated with UIT susceptibility include attention deficits and poor situation awareness [17], [18], lack of knowledge and memory failures [19],

[20], [10], and high workload or stress that impairs performance or judgment [21], [6].

Individual differences in risk-taking behavior should also be considered. The National Institute of Standards and Technology defines risk as the net negative impact of the exercise of vulnerability, considering both the probability and the impact of occurrence [22]. Risky decision-making behavior depends primarily on risk propensity and risk perception [23]. Cognitive biases or limitations may lead to a variety of decision-making errors [24], including inappropriate evaluation or prediction of risk (errors in estimating probability or impact) and incorrect over-weighting of spectacular incidents. Risk-tolerant individuals may take big risks despite cybersecurity training, while risk-averse individuals are less likely to knowingly take risky actions.

Physical states may affect performance and judgment and therefore increase the likelihood of UIT incidents. Fatigue or sleepiness increases the likelihood of human error [25]. Drugs may impact cognitive ability through negative effects on attention, memory, calculation, abstraction, ability to follow complex commands, and visuospatial skills [26]. Abuse of drugs and alcohol may impair productivity [27]. Dopamine levels influence the amount of risk that people take [28].

2.3. Psychosocial and demographic factors

External as well as organizational factors may affect an individual's emotional states, both normal and abnormal, which in turn can affect the human error rate and lead to UIT occurrences. Personality traits may be associated with UIT risk: for example, research by Parrish [29] indicates possible associations between social engineering susceptibility and various personality traits: high extraversion and increased susceptibility, high openness and decreased susceptibility, and high agreeableness and increased susceptibility.

Possible influences of demographic factors such as age, gender, and aspects of culture and subculture have not been conclusively demonstrated. Some studies report that females have lower perceived risk thresholds compared to males [30] and that females are more susceptible to phishing than males [11].

Various published results report phishing response rates between 3% and 11%, suggesting little, if any, cultural differences in phishing susceptibility [19], [31]–[33]. More research is needed to determine whether demographic factors such as age, gender, and culture are relevant and useful in developing more tailored mitigation strategies such as training and education topics.

3. Feature model and cases collected

Both intentional and unintentional insider threats play out in a broader sociological context of trust, workplace behaviors, and fallibility. To define the scope of the UIT project, we created a general taxonomy of negative impacts that discriminates among seven ways that projects fail, including intentional and unintentional actions on the part of both insiders and outsiders. This taxonomy of negative impacts is an extension of the one in Castelfranchi and Falcone's trust model [34], and UIT incidents are a subset of the entire taxonomy.

We developed a comprehensive feature model of negative impacts that includes UIT incidents. A feature model is the collection of features that characterize instances of a concept. The model represents relevant characteristics of an incident in the form of a hierarchical diagram that decomposes the concept into features and subfeatures, definitions of each feature, rules for combining features (such as features requisite for other features), and rationale for choice of features. The model categorizes four mandatory features for each incident: (1) the roles of the individuals in a UIT incident, (2) the underlying causes, (3) the system and format of the disclosed data, and (4) the industry sector or government agency where the incident occurred. The feature model describes UIT incidents in terms of these mandatory features and subordinate features. Figure 1 shows a schematic representation of the model.

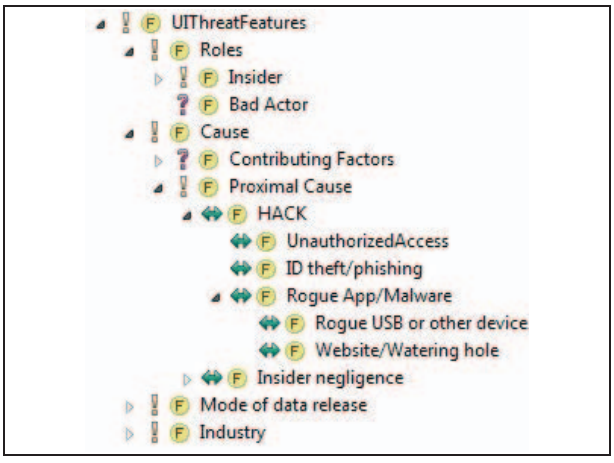

Figure 1. Extract of feature model

We use the feature model to analyze each case study that met the terms of the stated UIT definition. The analysis first considered the occurrence frequency of types of incidents under each top-level feature and its immediate subordinate features. The

feature model also helped characterize threat vectors and basic patterns of activity for each incident category, allowing our researchers to use features to search for specific types of incidents.

Because only 35 incidents with sufficient information to analyze were available, the results presented in this paper are preliminary. We found that 49% of the cases were associated with the DISC UIT threat vector, 6% with PHYS, 28% with PORT, and 17% with HACK. With nearly half of the incidents falling in the DISC category, the study determined that release through the internet and through email accounted for 23% and 20%, respectively, of the UIT cases. The combined incidence rates of PHYS and PORT (related to loss of electronic devices or non-electronic records) accounted for roughly one-third of the incidents, which points to the urgent need for a requirement for improved handling practices.

Figure 2 shows a class model for a UIT social engineering attack. The Attack Participant class includes the attacker and a number of UIT victims. The attacker may direct emails to a large number of potential UITs, or potential UITs may visit phishing websites. The Victim subclass includes only those who take the bait. The Attack Media class highlights the means used to obtain information, either through research in the early phases of the attack or via UIT responses, malware, or other electronic means. The attack comprises a variety of objects in the Attack Artifacts class (email, malware, or web pages).

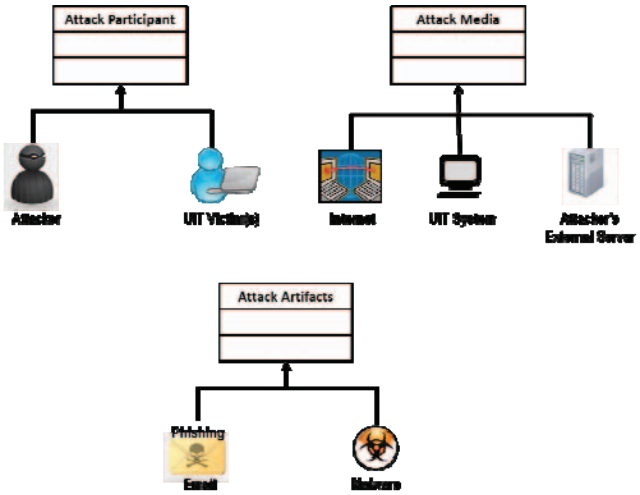

Figure 2. Class model for a UIT phishing exploit

4. Legal and ethical challenges

As indicated in Table 1, various methods can help recognize or infer potential indicators of concern. Some are surveillance methods (such as monitored electronic communications), while others require more intrusive testing and/or accessing of personnel records (including medical records in some cases). Clearly, these methods were identified without regard to possible legal constraints or boundaries, which must be considered. Legal and ethical issues constitute a major topic that deserves more attention; here we highlight a few of the most pertinent issues.

Potential indicators that are measured using some type of psychological testing (e.g., tests assessing risk tolerance, personality traits) may be deemed mental health testing, which would be limited by the Americans with Disabilities Act (ADA) or the Rehabilitation Act (for government employers). Monitoring electronic communications may implicate the Electronic Communication Privacy Act's protections, requiring an employer to obtain consent or fall within one of the law's exceptions. Differential treatment based on gender, age, culture, or subculture may be limited by Title VII of the Civil Rights Act of 1964 [35] or the Age Discrimination in Employment Act of 1967 [36]. Similarly, workplace drug testing is subject to both federal and state legal restrictions, such as the Mandatory Guidelines for Federal Workplace Testing Programs or the ADA (except for illegal drugs); most states also have drug testing laws.

Approaches to mitigation of insider threats (malicious as well as UIT) must also take privacy and ethical issues into account [37], [38]. Privacy rights advocates seek to ensure that employees will not suffer unwanted intrusions and that potentially harmful information will not be acquired about them. On the other hand, to the employer, the cost and damage of one incident may warrant data monitoring, collection, and analysis. To alleviate adverse effects of monitoring, employers should communicate the reasons for electronic monitoring and find a balance between such monitoring and employee privacy [37]. Disclosure of monitoring policies also may remove the expectation of privacy, from a legal perspective. If the process is disclosed, explained, and managed equitably across employees, it may not be considered unfair by employees, and the mutual trust relationship required for a healthy organization may remain intact [38].

Beyond legal and moral boundaries, organizations will be less likely to use indicators that are only weakly correlated to increased risk or that are expensive to implement and deploy.

Table 1. Summary of research identifying UIT contributing factors and possible mitigations

Factors	Effects	Measurement/Observation Methods	Mitigations Suggested by Research
General Organizational Factors			
Business processes and environment (work planning and control, data flow, work setting)	• Job stress negatively affects employee performance [4]. • Security measures are often difficult and confusing for an average computer user, and resultant errors can yield serious consequences [8]. • Systems that are difficult to understand or to use are negatively perceived by users and are less likely to be used [9]. • Exposure to antiphishing education may have a large impact on phishing susceptibility [11]. • Current antiphishing tools may not detect malicious websites that are well implemented [10]. • More likely to respond to phishing emails in the presence of large email loads [7]. • Time pressure negatively affects performance of even well-trained individuals [5]. • Heavy and prolonged workload can cause fatigue, which adversely affects performance [6]. • Stressors negatively impact human performance and increase errors, brought about through cognitive effects such as narrowing of attention (attending to fewer cues) [12], [13] and reduced working memory capacity [14]–[16].	• Business process requirements that are public should be observable. • Conduct detailed examination of business processes and environment to identify harmful effects on human performance or risk behavior • Conduct short worker surveys to assess business processes and environment • Human factors and management systems evaluations may be conducted to improve productivity and enhance business processes	• Assess business practice and management policies periodically to determine if business practices are arduous or have unintended effects on employee morale, performance, or risk behavior • Apply risk management, measurement and analysis approaches to critical business processes with incident-driven reviews • System dynamics modeling to characterize and communicate relationships between various contributing factors and unintended effects on employee morale, performance, or risk behavior
Human Factors			
Lack of attention, knowledge	• Poor situation awareness increases potential for human error (e.g., opening a phishing email) [17], [18] • Users may not notice or read the security warnings or indicators, or fail to notice the absence of security indicators (e.g., a padlock icon in the status bar) when they should be present [10]. • Users lack knowledge of design inconsistencies that distinguish real and fake error messages [20]. • Users may lack key knowledge elements such as knowledge about security features and understanding of URL/domain name syntax [19].	• Deficits in human attention and memory may be induced by human factors/organizational systems design issues and/or poor interface design. Various human factors based mitigations are relevant.	• Keep employees abreast of latest attack vectors and other threat-related news • More effective design of user-system interfaces to increase situation awareness and lower risk of errors
Workload	• Individuals experiencing the stress of high subjective mental workload are more likely to lower the threshold of acceptable performance and to shed some security process steps or tasks, even critical ones [7] • Heavy and prolonged workload can cause fatigue, which adversely affects performance [6].	• While there are experimental methods for measuring workload (such as subjective mental workload), workload issues are caused by factors such as poor interface design, human factors/organizational systems design issues, inefficient work practices, etc., for which various human factors based mitigations are relevant.	• Assist in prioritizing critical tasks • Automated tools to circumvent poor user decisions • Maintain an optimal level of arousal and stress for low error rates

Factors	Effects	Measurement/Observation Methods	Mitigations Suggested by Research
Risk tolerance	• Findings on risky decision making—how people perceive risk and react to risky situations—are situation specific and depend on organizational and individual characteristics • Risky decision-making behavior depends primarily on risk propensity and risk perception [23] • The magnitude component of risk may be more important in shaping risk perception than the probability component of risk [39] • Negatively framed risks tend to induce more risky decisions; positively framed risks may lead to less risky choices [40]	• Risk tolerance: Balloon Analogue Risk Task (BART) is a computerized and laboratory-based measure that correlates with a wide variety of risk-taking behaviors [30], [42] • Risk taking behavior is correlated with use of particular categories of words [43] as measured by the Linguistic Inquiry Word Count (LIWC) [44]; however, the applicability of this result to an individual's risk tolerance level has yet to be determined	• If high-risk takers are identified using BART or LIWC assessments, training/awareness workshops might be used to raise awareness of risk tolerance/risky decision making behaviors and their possible impacts on UIT/security. Benefits of the word use assessment method include simplicity, speed, expected low cost of electronics communication monitoring for word count; and since it doesn't involve psychological testing, it is not intrusive • Education about historical accidents and risk estimations • Training should employ personal/relevant descriptions of risk and reminders not to discount the probability of a particular (non-spectacular) concern
Cognitive limitations, biases, or faulty reasoning	• Cognitive biases or limitations may lead to a variety of decision making errors [24], including inappropriate evaluation/prediction of risk (errors in estimating probability and/or impact) and incorrect over-weighting of spectacular incidents • Mind wandering limits attentional resources and may lower performance [41], including ability to detect a risk • Annoyance with popup messages may lead users to click on fake popups [20]. • Users may think that they do not need redundant security features to slow down their job and that security risks in the internet are over-hyped [10].	• Cognitive biases are factors that contribute to human error, poor judgment, and flawed risk assessments that potentially increase the likelihood of UIT incidents. As such, it is most important to determine mitigation strategies or design principles to decrease the impact of cognitive biases or limitations rather than to develop or apply methods to measure such limitations.	• Training/awareness of cognitive biases such as prediction biases • Review systems designed to minimize security risks, including the CERT CRM and SRE methods • Automated tools to circumvent poor user decisions • Increase expertise leading to more balanced decisions • Provide info about costs of using technology • Appropriate framing may generate more risk-averse attitudes • Security/risk-related decisions framed positively to support less risky choice
Influence of physical states, drugs or hormone imbalances	• Fatigue or sleepiness increases the likelihood of human error [25] • Drugs may have negative effect on cognitive ability; may cause incorrect evaluation or prediction of risk • Two-thirds of patients in a 14-day substance abuse unit showed impaired neurocognitive performance, particularly in attention and memory, calculation, abstraction, ability to follow complex commands, and visuospatial skills [26]. • Abuse of drugs and alcohol may be associated with loss of productivity [27]. • Dopamine plays a role in the amount of risks that people take [28].	• Drug use might be observed using medical drug testing, for instance, urine sample tests, blood tests, hair sample tests, and breathalyzer tests. • Some hormones might be observed by medical testing and medical records.	• Provide Employment Assistance Program (EAP) and adequate health insurance benefits for mental health care • Ensure access to appropriate treatment for drug use/abuse; drug testing (within restrictions) • Automated tools to circumvent poor user decisions • Improve management practices to foster a productive work environment (e.g., decreasing stress and increasing self-care)

Factors	Effects	Measurement/Observation Methods	Mitigations Suggested by Research
Psychosocial, Sociocultural, and Other Factors			
Personality predispositions	• Individuals with various personality predispositions perceive risks as higher or lower than others without the predispositions • Extraversion may lead to increased phishing vulnerability [29]. • People who score high on openness may be less susceptible to social engineering attacks [29]. • Agreeableness—associated with greater trust, altruism, and compliance—may be the personality factor most highly associated with social engineering susceptibility [29].	• Personality tests for aspects of personality • Inferring personality traits through linguistic analysis of word counts in relevant word use categories [44]	• For high risk takers: apply strategies more often and with a greater degree of tailoring • Improved management practices • More effective security practices and processes • Effective design of user-system interfaces • Employ emotion- and logic-based influencers
Concerning behaviors	• Concerning behaviors (e.g., those discussed in [45]) such as anger, disgruntlement, stress, etc. may provide indications of more deep-seated psychological/psychosocial issues that could negatively impact the employee's perception of risk, risk tolerance, and decision making performance • Some moods affect perceptions of risk and the decision to act; an individual may take risks to improve his or her overall mood. However, research results are inconsistent regarding the effects of positive and negative moods on risk taking	• Concerning behaviors might be observed by colleagues and managers. • Factors relating to mood of an individual (anger, frustration, anxiety) might be observed by colleagues visually noticing body language or through conversation, writing, psychological tests, or automated linguistic analysis of electronic communications.	• Provide workplace environment programs that enhance respectful and calm environments • Ensure that employees have affordable access to mental health services, including drug treatment • Provide appropriate time off for employees to find a balance between work and home life • Promote team building activities and social interactions to enhance mood • Provide Employment Assistance Program (EAP) to help employees reduce outside stresses, which may cause mind wandering
Demographic factors (e.g., age, gender, cultural)	• Possible influences of demographic factors such as age, gender, and culture/subculture aspects have not been conclusively demonstrated, but the following results are suggestive regarding influences on risk tolerance/behavior: • On average, females have lower perceived risk thresholds and males have higher perceived risk thresholds [30] • People aged 18–25 found to be more susceptible to phishing [11]. • No significant differences found in phishing susceptibility between students, faculty, and staff in a university setting [19]. • Females more susceptible to phishing than males [11]. • Various published results report phishing response rates between 3% and 11%, suggesting little, if any, cultural differences in phishing susceptibility [19], [31]–[33].	• Demographic data may be obtained from personnel records. • Cultures and subcultures (national, cross-national, and organizational) might be observed in a variety of ways. Citizenship records and records of places lived (past and present) might be maintained by national law enforcement or from national security databases. • Information about languages spoken and social networks might be observed from online activity (possibly only available to law enforcement or national security personnel, but other data revealing this information might be publicly available, such as on a public Facebook page). • Analysis of social networks could reveal information about probable culture and subculture affiliations. Linguistic analysis might reveal culture or subculture affiliations.	• Recurring training of potential threats and their significance via systems security mailing lists, websites, and news organizations • Incident driven reviews of policies, practices, processes and training materials • Provide opportunities for training and fair advancement • Utilize effective learning tools based on learning styles and existing knowledge base • Evaluate organizational culture of work environment • Outline/develop ideal cultural workplace norms • Thorough orientation and continued training • Utilize ethnographic methods and maintain understanding of differing cultural norms • Employ emotion- and logic-based influencers

5. Mitigation strategies

We have described UIT contributing factors (or potential factors), ranging from broad organizational factors to human factors with a cognitive or psychosocial context. Research is required to yield more definitive and actionable strategies, but we can speculate on mitigation strategies and approaches. Table 2 summarizes a preliminary set of mitigation strategies and countermeasures.

A proactive approach that seeks to create productive and healthy work environments represents a first line of defense in helping to reduce UIT incidents. The focus of proactive mitigation strategies tends to be on improvements in work processes (relieving time and workload pressure), management practices to avoid overtaxing staff, training to increase awareness and motivation, and usability of security tools to help overcome user errors and negligence, the most common underlying factors for UIT [46].

Policies and countermeasures to guard against the impacts of UIT incidents provide another line of defense against failures that occur despite prevention efforts. Milligan and Hutcheson [47] discuss applications, associated security threats, and suggested countermeasures. For example, one strategy might be to address malware attacks in email by adopting specific countermeasures and policies that encourage or enforce more stringent process discipline; other strategies include developing automated defense tools to better recognize email threats and applying data loss prevention software to recognize possible harmful sites.

6. Conclusion

Our preliminary study of the UIT problem has identified a number of possible contributing factors and mitigation strategies The malicious insider threat and UIT share many contributing factors that relate to broad areas such as security practice, organizational processes, management practices, and security culture, but there are also significant differences. Human error plays a major role in UIT, so UIT countermeasures and mitigations should include strategies for improving and maintaining productive work environments, healthy security cultures, and human factors that increase usability and security of systems and decrease the likelihood of human errors. Differentiating risk-tolerant individuals from risk-averse individuals might enable an organization to increase or maintain productivity. For example, training and awareness programs should focus on enhancing recognition among staff of the UIT problem and help individuals identify possible cognitive biases and limitations that might put them at a higher risk of committing such errors or judgment lapses. However, training and awareness programs have their limits, and human factors or organizational systems cannot completely eliminate human errors associated with risk tolerance and other cognitive and decision processes. A comprehensive mitigation strategy should include more effective automated safeguards that seek to provide fail-safe measures against these failures.

Future research should include:

- Continue to collect incident data to accumulate cases for the UIT database. This will enable statistical analysis and further investigation of best and worst practices.
- Continue research to increase our understanding of UIT contributing factors and to help R&D stakeholders prioritize investments in new technology development, research, or practices that address the most important threat vectors.

Table 2. Summary of UIT mitigation strategies and countermeasures

Human Factors and Training	High-Level Organizational Best Practices	Automated Defense
• Enhance awareness of insider threat and UIT. • Heighten motivation to be wary of UIT risks. • Train employees to recognize phishing and other social media threat vectors. • Engender process discipline to encourage following of policies and guidelines. • Train continuously to maintain proper level of knowledge, skills, and ability. • Conduct training on and improve awareness of risk perception and cognitive biases that affect decision making. • Improve usability of security tools. • Improve usability of software to reduce likelihood of system-induced human error.	• Review and improve management practices to align resources with tasks. • Improve data flow by enhancing communication and maintaining accurate procedures. • Maintain productive work setting by minimizing distractions. • Provide effective security practices (e.g., two-factor authentication for access). • Implement effective work planning and control to reduce job pressure and manage time. • Maintain employee readiness. • Maintain staff values and attitudes that align with organizational mission and ethics. • Implement security best practices throughout the organization.	• Deploy better software to recognize bogus emails. • Deploy data loss prevention software to recognize potentially harmful sites and email practices. • Use firewalls. • Use virus and malware protection software. • Enable remote memory wipe for lost equipment.

- Identify best practices for organizations to follow after suffering a UIT incident, possibly including reporting of incidents to a central clearinghouse to facilitate analysis of incident statistics and better inform our understanding of contributing factors and the effectiveness of countermeasures.

7. Acknowledgments

We wish to acknowledge and thank CMU intern Arley Schenker for contributions to this research.

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of Department of Homeland Security or the United States Department of Defense.

This material has been approved for public release and unlimited distribution.

CERT® is a registered mark of Carnegie Mellon University.

DM-0000592

8. References

[1] AlgoSec, "The State of Network Security 2013: Attitudes and Opinions," AlgoSec, Inc., 2013.

[2] CERT Insider Threat Team, Unintentional Insider Threats: A Foundational Study (CMU/SEI-2013-TN-022), Software Engineering Institute, Carnegie Mellon University, May 2013.

[3] D. J. Pond and K.R. Leifheit, "End of an Error," Security Management, 47(5), 2003, pp. 113-117.

[4] S. Leka, A. Griffiths, and T. Cox, "Work Organization and Stress: Systematic Problem Approaches for Employers, Managers, and Trade Union Representatives," Protecting Workers Health Series, No. 3, World Health Organization, Geneva, Switzerland, 2004. http://www.who.int/occupational_health/publications/pwh3rev.pdf

[5] P. Lehner, M. Seyed-Solorforough, M.F. O'Connor, S. Sak, and T. Mullin, "Cognitive Biases and Time Stress in Team Decision Making," IEEE Transactions on Systems, Man, and Cybernetics Part A: Systems & Humans, 27, 1997, pp. 698-703.

[6] E. Soetens, J. Hueting, and F. Wauters, "Traces of Fatigue in an Attention Task," Bulletin of the Psychonomic Society, 30, 1992, pp. 97-100.

[7] A. Vishwanath, T. Herath, R. Chen, J. Wang, and H. Rao, "Why Do People Get Phished? Testing Individual Differences in Phishing Vulnerability within an Integrated, Information Processing Model," Decision Support Systems, 51(3), 2011, pp. 576-586.

[8] A. Whitten, and J.D. Tygar, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0," Proceedings of the 8th USENIX Security Symposium, Washington, D.C., 1999.

[9] V. Venkatesh, M. Morris, G.B. Davis, and F.D. Davis, "User Acceptance of Information Technology: Toward a Unified View," MIS Quarterly, 27(3), 2003, pp. 425-478.

[10] J. Erkkila, "Why We Fall for Phishing," Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI) Vancouver, BC, Canada, May 7-12, 2011, ACM, 2011.

[11] S. Sheng, M. Holbrook, P. Kumaraguru, L. Cranor, and J. Downs, "Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions," 28th ACM Conference on Human Factors in Computing Systems, Atlanta, GA, April 10-15, 2010, ACM 2010.

[12] B.K. Houston, "Noise, Task Difficulty, and Stroop Color-Word Performance," Journal of Experimental Psychology 82, 2, 1969, pp. 403-404.

[13] A. Stokes, and K. Kite, Flight Stress, Ashgate, 1994.

[14] D.R. Davies, and R. Parasuraman, The Psychology of Vigilance, Academic Press, 1982.

[15] G.R.J. Hockey, "Changes in Operator Efficiency as a Function of Environmental Stress, Fatigue, and Circadian Rhythms," in K.R. Boff, L. Kaufman, and J.P. Thomas, (Eds.), Handbook of Perception and Human Performance (vol. 2), Wiley, 1986.

[16] P.L. Wachtel, "Anxiety, Attention and Coping with Threat," Journal of Abnormal Psychology 73, 2, April 1968, pp. 137-143.

[17] M.R. Endsley, "Toward a Theory of Situation Awareness in Dynamic Systems," Human Factors, 37, 32-64, 1995.

[18] M.D. Rodgers, R.H. Mogfor, and B. Strauch, "Post Hoc Assessment of Situation Awareness in Air Traffic Control Incidents and Major Aircraft Accidents," in M.R. Endsley and D.J. Garland (Eds)., Situation Awareness Analysis and Measurement, Lawrence Erlbaum Associates, Mahway, NJ, 2000.

[19] R. Dhamija, J.D. Tygar, and M. Hearst, "Why Phishing Works," Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '06), New York, NY, 2006, ACM, pp. 581-590. http://dl.acm.org/citation.cfm?id=1124861

[20] D. Sharek, C. Swofford, and M. Wogalter, "Failure to Recognize Fake Internet Popup Warning Messages," Proceedings of the Human Factors and Ergonomics Society 52nd Annual Meeting, 2008, pp. 557-560.

[21] S.G. Hart, and C.D. Wickens, Workload Assessment and Prediction," in H.R. Booher (Ed.), MANPRINT: An Approach to Systems Integration, Van Nostrand Reinhold, New York, 1990, pp. 257-296.

[22] National Institute of Standards and Technology (NIST), Risk Management Guide for Information Technology Systems (Special Publication 800-30), U.S. Department of Commerce, 2002.

[23] S.B. Sitkin, and L.R. Pablo, "Reconceptualizing the Determinants of Risk Behaviour," Academy of Management Review 17(1), 1992, pp. 9-38.

[24] D. Kahneman, and A. Tversky, "Prospect Theory: An Analysis of Decisions Under Risk," Econometrica, 47(2), 1979, pp. 263-291.

[25] P.H. Gander, M. van den Berg, and L. Signal, "Sleep and Sleepiness of Fisherman on Rotating Shifts," Chronobiology International, 25(2&3), 2008, pp. 38-398.

[26] P.S. Meek, H.W. Clark, and V.L. Solana, "Neurocognitive Impairment: The Unrecognized Component of Dual Diagnosis in Substance Abuse Treatment," Journal of Psychoactive Drugs, Apr-Jun, 21(2), 1989, pp. 153-60.

[27] HealthyPeople.gov, Substance Abuse, 2013. http://healthypeople.gov/2020/LHI/substanceAbuse.aspx

[28] A. Park, "Why We Take Risks—It's the Dopamine," time.com, December 30, 2008. http://www.time.com/time/health/article/0,8599,1869106,00.html

[29] J.L. Parrish, Jr., J.L. Bailey, and J.F. Courtney, "A Personality Based Model for Determining Susceptibility to Phishing Attacks," Decision Sciences Institute, 2009, pp. 285-296.

[30] M.K. Hunt, D.R. Hopko, R. Bare, C.W. Lejuez, and E.V. Robinson, "Construct Validity of the Balloon Analog Risk Task (BART) Associations With Psychopathy and Impulsivity," Assessment, 12(4), 2005, pp. 416-428.

[31] M. Jakobsson, and J. Ratkiewicz, "Designing Ethical Phishing Experiments: A Study of (ROT13) Ronl Query Features," Proceedings of the 15th International Conference on World Wide Web, Edinburgh, Scotland, 2006, ACM, 2006, pp. 513-522.

[32] W. Knight, "Goin' Phishing?" Infosecurity Today (1:4), 2004, pp. 36-38. http://www.sciencedirect.com/science/article/pii/S1742684704000898

[33] J.G. Mohebzada, A. El Zarka, A.H. Bhojani, A. Darwish, "Phishing in a University Community," International Conference on Innovations in Information Technology (IIT), 2012, pp. 249-254.

[34] C. Castelfranchi, and R. Falcone, Trust Theory: A Socio-Cognitive and Computational Model (Wiley Series in Agent Technology), John Wiley and Sons, Chichester, UK, 2010.

[35] United States Code, Volume 42—The Public Health and Welfare, Section 2000e-16, 1964.

[36] United States Code, Title 29 – Labor, Chapter 14 – Age Discrimination in Employment, Sec. 621.

[37] A.I.T. Kiser, T. Porter, and D. Vequist, "Employee Monitoring and Ethics: Can They Co-Exist?" International Journal of Digital Literacy and Digital Competence, 1(3), 2010, pp. 30-45.

[38] F.L. Greitzer, D.A. Frincke, and M. Zabriskie, "Social/Ethical Issues in Predicitve Insider Threat Monitoring," in M.J. Dark (Ed.), Information Assurance and Security Ethics in Complex Systems: Interdisciplinary Perspectives. Information Science Reference, Hershey, PA, 2010, pp. 132-161.

[39] M. Keil, L. Wallace, D. Turk, G. Dixon-Randall, and U. Nulden, "An Investigation of Risk Perception and Risk Propensity on the Decision to Continue a Software Development Project," The Journal of Systems and Software 53(2), 2000, pp. 145-157.

[40] C. Gonzalez, J. Dana, H. Koshino, and M. Just, "The Framing Effect and Risky Decisions: Examining Cognitive Functions with fMRI," Journal of Economic Psychology 26(1), 2005, pp. 1-20.

[41] E. Klinger, "Modes of Normal Conscious Thought," in K.S. Pope and J.L. Singer (Eds.), The Stream of Consciousness: Scientific Investigations into the Flow of Human Experience, Plenum, New York, 1978, pp. 225-258.

[42] C.W. Lejuez, J.P. Read, C.W. Kahler, J.B. Richards, S.E. Ramsey, G.L. Stuart, D.R. Strong, and R.A. Brown, "Evaluation of a Behavioral Measure of Risk Taking: The Balloon Analogue Risk Task (BART)," Journal of Experimental Psychology Applied, 8(2), 2002, pp. 75-84.

[43] W.G. Moons, J.R. Spoor, A.E. Kalomiris, and M.K. Rizk, "Certainty Broadcasts Risk Preferences: Verbal and Nonverbal Cues to Risk-Taking," Journal of Nonverbal Behavior, 37(2), 2013, pp. 79-89.

[44] Y.R. Tausczik, and J.W. Pennebaker, "The Psychological Meaning of Words: LIWC and Computerized Text Analysis Methods," Journal of Language and Social Psychology 29(1), 2010, pp. 24-54.

[45] F.L. Greitzer, L.J. Kangas, C.F. Noonan, A.C. Dalton, and R.E. Hohimer, "Identifying At-Risk Employees: A Behavioral Model for Predicting Potential Insider Threats," 45th Hawaii International Conference on System Sciences (HICSS-45), Wailea, Maui, Hawaii, 2012, pp. 2392-2401.

[46] A. Yayla, "Controlling Insider Threats with Information Security Policies (Paper 242)," ECIS 2011 Proceedings, Helsinki, Finland, June 9-11, 2011. http://aisel.aisnet.org/ecis2011/242 (2011).

[47] P.M. Milligan, and D. Hutcheson, "Business Risks and Security Assessment for Mobile Devices," Proceedings of the 8th WSEAS Int. Conference on Mathematics and Computers in Business and Economics, Vancouver, Canada, June 19-21, 2007, ACM, 2007, pp. 189-193.