Software Engineering Institute

Unintentional Insider Threats: A Foundational Study

Produced for
Department of Homeland Security
Federal Infrastructure Protection Bureau

The CERT® Insider Threat Team

August 2013

TECHNICAL NOTE
CMU/SEI-2013-TN-022

CERT® Division

http://www.sei.cmu.edu

Carnegie Mellon

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.

DM-0000484

Table of Contents

Sponsor Information vii

Executive Summary ix

Abstract xv

1 Introduction 1

2 Defining and Characterizing Unintentional Insider Threat 2
- 2.1 Broad Context 2
  - 2.1.1 Definition of Unintentional Insider Threat 2

3 Related Work 6
- 3.1 Research on Intentional Insider Threat 6
- 3.2 Challenges and Approach to Identifying Relevant Research 6
- 3.3 Relevant Human Factors/Cognitive Science Research 7
  - 3.3.1 Human Error 7
  - 3.3.2 Fatigue or Sleepiness 8
  - 3.3.3 Subjective Mental Workload 8
  - 3.3.4 Situation Awareness 9
  - 3.3.5 Mind Wandering 10
- 3.4 Risk Tolerance and Decision Making 10
  - 3.4.1 Risk Perception and Risky Decision Making 10
  - 3.4.2 Human Limitations and Biases 12
- 3.5 Relevant Research on Psychosocial and Sociocultural Factors 14
  - 3.5.1 Risk Tolerance as a Psychological or Personality Trait 14
  - 3.5.2 Cultural Factors 15
  - 3.5.3 Gender 16
  - 3.5.4 Mood 17
  - 3.5.5 Age Effects and Variations Over Time 17
  - 3.5.6 Influence of Drugs and Hormones 17
- 3.6 Addressing Causal Factors at a Deeper Level 18
- 3.7 Summary of Causal Factors and Possible Mitigation Strategies 19

4 Comprehensive UIT Feature Model 22

5 Summary of Collected Cases 26
- 5.1 Description of Case Collection Requirements 26
- 5.2 Case Collection Examples 26
- 5.3 Sources of Collected Cases 27
- 5.4 How the Feature Model Supports Analysis of Case Studies 28
- 5.5 Breakdown of Case Collection Frequency by Features 28
  - 5.5.1 Roles Features 28
  - 5.5.2 Cause Features and Summary by Threat Vector 29
  - 5.5.3 Mode of Data Release Features 31
  - 5.5.4 Industry Features 32
  - 5.5.5 Patterns of Incidents 32
  - 5.5.6 Emerging Causes of Incidents 33

6 Unintentional Insider Contributing Factors and Observables 34

7 Mitigation Strategies for Unintentional Insiders 37

8 Conclusions **42**

9 Suggested Future Work **44**

Appendix A: Taxonomy of Negative Impacts **46**

Appendix B: UIT Incident Totals **49**

Appendix C: UIT Features Glossary **50**

Appendix D: UIT Incident Features **51**

Bibliography **54**

List of Figures

Figure 1: Descriptive Characterization of Risk Perception and Decision Processes 11

Figure 2: Comprehensive UIT Feature Model 24

Figure 3: Roles of Unintentional Insiders 28

Figure 4: Causes of UIT Incidents 31

Figure 5: Modes of Data Release 32

Figure 6: Industry in Which Release Occurred 32

Figure 7: Taxonomy of Negative Impacts (Note that only the cases labeled with “§” are in scope for this project.) 48

List of Tables

Table 1:	Summary of Research Identifying UIT Contributing Factors and Possible Mitigations	19
Table 2:	Model Feature Types	22
Table 3:	Some Potential Observation Methods per Factor	34
Table 4:	Mitigations and Countermeasures for Different UIT Threat Vectors	39

Sponsor Information

The Department of Homeland Security (DHS) Office of Federal Network Resilience (FNR) Cybersecurity Assurance Branch (CAB). The key contact is Project Lead Sean McAfee (Sean.Mcafee@hq.dhs.gov). Please forward any questions about this work to FNR/CAB via Sean Mcafee.

Executive Summary

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 report examines the problem of unintentional insider threat (UIT) by developing an operational definition of UIT, 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 presenting initial thinking on potential mitigation strategies and countermeasures. Because this research topic has not been specifically studied, 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, built this report from research reports on UIT cases we discovered in public sources and collected in the CERT insider threat database. The report provides a simple template for sharing information about such threats and extracting data about them for inclusion in the CERT insider threat database. It also proposes a feature model that categorizes recognizable characteristics of threats; lists roles, causes, systems affected, and government or industry setting; and shows relationships among these features.

Unintentional Insider Threat Definition

We recommend 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,[2] (4) causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems.*

We use the term *UIT threat vectors* to refer to four types of UIT incidents that account for virtually all of the incidents we have collected:

- 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

---

1 AlgoSec. *The State of Network Security 2013: Attitudes and Opinions.* AlgoSec, Inc., 2013. http://www.algosec.com/resources/files/Specials/Survey%20files/State%20of%20Network%20Security%202013_Final%20Report.pdf

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

2 Malicious intent includes 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 does not check badges does not mean to allow a malicious actor into the building, but he lets someone in who sets the building on fire).

- 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) and carried out via software, such as malware and spyware
- PHYS, or improper or 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

Research Literature Review

Though little research explicitly focuses on UIT, the research applicable to UIT is vast and may be organized in several different ways. Our purpose in studying relevant research is 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, which span a continuum between the culminating action by the UIT and the series of conditions and incidents that led to this failure.

A major part of the UIT definition is the failure in human performance. While human errors can never be eliminated completely, human error mitigation techniques can dramatically reduce errors induced by external influences. Such techniques should focus on system conditions that contributed to, or even made inevitable, the resulting errors and adverse outcomes. At the organizational level, we group these broad, external causal factors into four categories:

- data flow—inadequate procedures or directions, poor communication
- work setting—distractions, insufficient resources, poor management systems, inadequate security practices
- work planning and control—job pressure; time factors; task difficulty; change in routine; poor task planning and management practice; 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, cognitive factors

These systemic, distal contributing factors may lead to immediate proximal precursors to UIT incidents. These proximal precursors are human factors and performance indicators such as high subjective mental workload, lack of (or loss of) situation awareness, and mind wandering—each of which may increase the likelihood of human errors that lead to UIT incidents. Additionally, emotional states, both normal and abnormal, can affect the human error rate and UIT occurrences.

This report discusses other possible contributing factors, including psychological and psychosocial traits and predispositions, demographic (age and gender) effects, and cultural factors that may influence attitudes and risk perception. Risk perception and risky decision making are important components of a descriptive cognitive model, and they may be used to better understand how UIT behavior plays out in the mind of the insider as well as to identify possible mitigation strategies and countermeasures.

Feature Model and Cases Collected

This report develops and summarizes an initial construction of a comprehensive feature model of UIT. A feature model is the collection of features that characterize instances of a concept, in this case a UIT incident. The model represents relevant characteristics of any incident and comprises 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:

- roles of the individuals in a UIT incident
- underlying causes
- system and data format of the disclosed data
- industry sector or government agency where the incident occurred

We used the feature model to categorize cases collected and support analysis of how frequently cases in each category occur. Specifically, we used the feature model to support analysis of each case study that met the stated requirements. 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.

Though the results presented in this report are preliminary due to the limited amount of data collected to date, 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 all UIT cases. The combined incidence rate for PHYS and PORT (related to loss of electronic devices or non-electronic records) accounted for roughly one-third of the incidents, which points to an immediate need for improved handling practices. These findings are preliminary due to the small sample size of 35 incidents. We must collect more cases to generate enough data to support more definitive analyses and conclusions.

The collection of additional UIT cases and subsequent analyses of the data will improve our understanding of similarities and differences among UIT incidents based on the model's features. The accumulation and analysis of incident statistics will also ultimately help stakeholders prioritize different types of UIT threats and associated mitigation strategies, informing decisions about where and how to invest R&D money to derive the greatest gains.

Mitigation Strategies

We developed a preliminary set of mitigation strategies and countermeasures based on the findings of the study.

- high-level organizational best practices
  - Review and improve management practices to align resources with tasks.
  - Improve data flow by enhancing communication and maintaining accurate procedures.
  - Maintain a productive work setting by minimizing distractions.
  - Provide effective security practices (e.g., two-way authentication for access).

  - Implement effective work planning and control to reduce job pressure and manage time factors.
  - Maintain employee readiness.
  - Maintain staff values and attitudes that align with organizational mission and ethics.
  - Implement security best practices throughout the organization.
- human factors and training strategies
  - Enhance awareness of insider threat, including unintentional insider threat.
  - Heighten motivation to be wary of insider threat risks.
  - Train employees to recognize phishing and other social media threat vectors.
  - Engender process discipline to encourage adherence to 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 human factors and usability of security tools.
  - Improve usability of software to reduce likelihood of system-induced human error.
- strategies that deploy automated defense tools
  - Deploy better software to recognize bogus emails.
  - Deploy data loss prevention (DLP) software to recognize potentially harmful sites and email practices.
  - Use firewalls.
  - Use antivirus software.
  - Use anti-malware software.
  - Enable remote memory wipe for lost equipment.

Conclusions and Recommendations

Our preliminary study of the UIT problem has identified a number of 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.

Training and awareness programs should focus on enhancing staff's recognition 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 perception and other cognitive and decision processes. A comprehensive mitigation strategy should include new and more effective fail-safe automated safeguards against these failures.

We recommend future research on UITs, with particular focus on contributing factors underlying accidental or mindless acts versus technical problems that lead to UIT incidents, and on more

effective mitigation strategies for these types of cases. The following are suggestions for future research:

- Continue to collect incident data to build up a large set of cases for the UIT database. These could be used for more extensive statistical analysis or investigation of best and worst practices.
- Continue UIT research and data collection to inform R&D stakeholders where to invest in new technology development, research, or practices; such analyses can help prioritize development of tools and mitigation strategies based on the most frequent threat vectors.
- Expand the CERT Division's *Common Sense Guide to Mitigating Insider Threats* to address UIT.
- Study organizations' responses to UIT. What are best practices for organizations to follow after suffering a UIT incident? In addition to utilizing the best mitigation and organizational responses currently available, reporting of incident data to a central clearinghouse would greatly facilitate collection and analysis of incident statistics, which would lead to better understanding of contributing factors and the effectiveness of countermeasures.
- Conduct research on factors that contribute to UIT. We derived many of the risk-related research results cited in this report from experiments that did not directly address cybersecurity, much less relate to UIT research. To refine and validate the hypothesized application or extrapolation of our results to the UIT domain, future research should directly address the cybersecurity and UIT domains.

Abstract

This report examines the problem of unintentional insider threat (UIT) by developing an operational definition of UIT, 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 presenting initial thinking 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.

1 Introduction

Organizations often suffer harm from individuals who bear no malice against them but whose actions unintentionally expose the organizations to risk in some way. The *State of Network Security 2013*, a report produced by the security management company AlgoSec, found that a significant proportion of security professionals view insider threat as their greatest organizational risk, and more than 40% of respondents consider employees accidentally jeopardizing security through data leaks or similar errors to be their greatest concern [AlgoSec 2013].

This report, *Unintentional Insider Threats: A Foundational Study*, examines initial findings from research on such cases, referred to as unintentional insider threat (UIT). This report examines the problem of UIT by developing an operational definition of UIT, 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 presenting initial thinking 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 (SEI), built this report from research reports on UIT cases we discovered in public sources and collected in the CERT insider threat database. The report provides a simple template for sharing information about such threats and extracting data about them for inclusion in the CERT insider threat database. It also proposes a feature model that categorizes recognizable characteristics of threats; lists roles, causes, systems affected, and government or industry setting; and shows relationships among these features.

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

2 Defining and Characterizing Unintentional Insider Threat

2.1 Broad Context

Both intentional and unintentional insider threats play out in a broader sociological context of trust, workplace behaviors, and fallibility. In order 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 by insiders and outsiders. UIT is a subset of the broader taxonomy, as explained in Appendix A.

2.1.1 Definition of Unintentional Insider Threat

We recommend 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,[1] (4) causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems.*

This definition specifies some of the abstract features of the general model that are prescribed by the taxonomy of negative impacts (see Appendix A), namely:

1. *a current or former employee, contractor, or business partner*: the insider to whom the leader has delegated parts of the task
2. *has or had authorized access to an organization's network, system, or data*: giving authorized access to the insider as part of the delegation process
3. *their action/inaction without malicious intent*: the nonmalicious, poor performance of the insider
4. *negatively affects the confidentiality, integrity, or availability of the organization's information or information systems*: the failure of the task

This report focuses on the branches of the taxonomy and associated feature map, in which an insider is involved and for which the insider lacks malicious intent. By definition, all of the UIT cases feature an organizational insider who facilitates the actual or potential threat incident.[2] However, there is a distinction between the UIT cases that originate with actions performed by the internal, nonmalicious member of the organization and UIT incidents that originate with an outside malicious agent. There are several cases of interest (see Appendix B): (1) the unwitting insider and a malicious outside actor are involved, (2) the incident is solely a function of the

[1] Malicious intent includes 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 does not check badges does not mean to allow a malicious actor into the building, but he lets someone in who sets the building on fire).

[2] By *facilitation* we mean (1) actively participating in the incident, (2) failing to report the incident, or (3) committing an error that (a) violated policy and/or industry-standard practices and (b) started a causal chain that led to the incident.

insider's performance or negligence, and (3) an organizational, system, or human factors deficiency contributes to the insider's failure.

Some types of cases are outside the scope of the present study: intentional or malicious insider threats; accidents, which should not be confused with UITs; and deliberate, well-intentioned actions that cause negative effects, such as cyber friendly fire[3] [Andrews 2011].

We use the term *UIT threat vectors* to refer to types of UIT incidents.[4] There are four main types of UIT threat vectors that account for virtually all of the cases in the CERT insider threat database (these were derived from *The Privacy Rights Clearinghouse* [PRC] and have been modified to suit the purposes of this study):

- DISC, or accidental disclosure—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) and carried out via software, such as malware and spyware
- PHYS, or improper or 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

Note that the DISC, PHYS, and PORT threat vectors are generally associated with cases that originate with an action (or lack of appropriate action) of a nonmalicious insider. In contrast, the UIT-HACK threat vector originates with an outside agent—an external threat. To be included in the CERT insider threat database, UIT-HACK cases must feature facilitation by the unknowing action or inaction of an internal agent. This excludes incidents in which the outside agent directly obtains data, damages data, damages a system, or causes a denial of service.

The PRC is not the only organization or research team to have categorized unintentional insider threats. We chose the PRC's work to illustrate one perspective into this large problem area. Many studies and surveys have underscored the breadth of the unintentional insider threat problem. These studies may categorize the unintentional threat in different ways, making it difficult to reconcile the scope of the problem. Future work could include mapping these differing taxonomies to ensure a better understanding of this area of work. Studies and surveys in this area include the following:

- *Verizon 2013 Data Breach Investigations Report*—"While not common in our main dataset, unintentional actions can have the same effect. The broader collection of 47,000+ security incidents featured in this report offers ample evidence of this fact. These include 'low-tech' events, such as sending sensitive documents to the wrong recipients, as well as less-frequent

---

[3] Greitzer, F. L.; Carroll, T. E.; & Roberts, A. D. "Cyber Friendly Fire: Research Challenges for Security Informatics." *IEEE International Intelligence and Security Informatics Conference,* Seattle, WA, June 4-7, 2013.

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

mistakes by system administrators and programmers. For instance, one incident in our caseload involved an errantly configured application debug setting that caused sensitive financial data to be stored insecurely and exposed to unauthorized parties" [Verizon 2013].

- Burke and Christiansen, *Insider Risk Management: A Framework Approach to Internal Security (2009)*—"The majority of organizations (52%) characterized their incidents arising from insider threats as predominantly accidental. We found that only 19% believed insider threat incidents were primarily deliberate and 26% believed they were an equal combination" [Burke 2009].
- Cisco Systems, *Data Leakage Worldwide: Common Risks and Mistakes Employees Make (2008)*—The survey "examined the relationships between employee behavior and data loss, as well as IT perceptions of those factors. The survey found that employees around the world are engaging in behaviors that put corporate and personal data at risk, that IT professionals are often unaware of those behaviors, and that preventing data leakage is a business-wide challenge" [Cisco 2008a].
- Cisco Systems, *Data Leakage Worldwide: The Effectiveness of Security Policies (2008)*—This report offers insight into how security policy creation, communication, and compliance affect data leakage. The analysis shows that a lack of security policies and a lack of employee compliance with security policies are significant factors in data loss [Cisco 2008b].
- Kumaraguru et al., *Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System* (2007)—This report features Carnegie Mellon University's Lori Cranor, who has done much work in this area and contributed to a spin-out company that provides antiphishing training to organizations [Kumaraguru 2007].
- Parmar, *Employee Negligence: The Most Overlooked Vulnerability* (2013) [Parmar 2013]

Some studies have examined UITs to specific industries, for example, the Ponemon Institute's third annual benchmark study on patient privacy and data security [Ponemon 2012].

Another approach, based on data reported in Microsoft's 2011 threat intelligence report, is to estimate UIT occurrences from malware counts [Faulhaber 2011]. For example, Microsoft released counts for malware detected by its malicious software removal tool in the second half of 2011. The tool runs on more than 600 million machines around the world. According to Microsoft's threat intelligence report, in the last 6 months of 2011, there were about 780,000 computers infected by malware Family 1 and 400,000 computers infected by malware Family 2 (p. 11). Microsoft's estimation approach assumed that approximately 44% of the infections required some form of user interaction (pp. 13–14) in order to propagate. If we also assume that none of the users intended to install the malware onto their machines, that would equate to 519,200 instances where a UIT compromised a computer with malware from the first two families alone. In addition to these two malware families, Microsoft listed 25 popular families of malware that were detected more than 25,000 times—each—during the same 6 months. These numbers are not exact, and certain assumptions were needed; further, it may be very difficult to get a large enough sample of data to make determinations about the total population. But this analysis suggests that the size of the unintentional insider threat problem is large.

2.1.1.1 Terminology

One of the key difficulties we faced when conducting research on UIT is the number of terms used to describe the same phenomenon, including unintended insider threat, accidental insider threat, and inadvertent insider threat. Our research included all of these areas. Other terms for this phenomenon could exist. We will continue to search for these to include in future research papers.

3 Related Work

3.1 Research on Intentional Insider Threat

As described in numerous CERT publications, most recently *The CERT Guide to Insider Threats* [Silowash 2012], a common practice in examining and analyzing insider crimes is to develop characterizations of the most critical incidents and observables in the form of a general set of models (Management and Education of the Risk of Insider Threat, or MERIT, models) that identify common patterns, contributing factors and observables, and mitigation measures. CERT researchers have used this practice extensively, with a focus on several major types of malicious (intentional) insider crime, including fraud, intellectual property (IP) theft, sabotage, and espionage. In this research, CERT researchers identified key contributing factors and observables that characterize these different types of insider crime. For example, personal predispositions are a particularly important indicator for insider IT sabotage. Insider IP theft crimes did not show as consistent a pattern, but often the perpetrators could be characterized as "entitled independent" (with feelings about a sense of entitlement and often exhibiting feelings of dissatisfaction) or as an "ambitious leader" who expects to profit in some way by committing the theft. Cases of insider fraud are characterized even more strongly by financial gain.

To identify UIT patterns and contributing factors and observables, we might begin by considering which, if any, of these that are defined for malicious insider crime might apply to UIT cases. We could start with the characteristics of malicious insiders and ask if individuals involved in UIT cases tend to

- hold a particular level or position in the organization
- work in a particular discipline or job category (e.g., technical, nontechnical, managerial, system administrator, etc.)
- have financial problems
- exhibit serious personal or work-related stresses
- often work at odd hours
- exhibit other identifying characteristics

3.2 Challenges and Approach to Identifying Relevant Research

Unfortunately, mapping common patterns and contributing factors and observables from malicious insider cases to UIT cases is challenging. Many of the factors associated with malicious insider crime (particularly those relating to motivational factors) do not appear to play a role in UIT cases. Nevertheless, we can consult the literature in human factors, cognitive science, safety, and human error as well as other research domains to suggest possible contributing factors.

The research applicable to UIT is vast and may be organized in several different ways. Our purpose in studying relevant research is 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, which span a continuum between the UIT incident and the series of conditions and incidents that led to this failure. Reactions to failure tend to focus on the individual who was

closest to producing and to potentially avoiding it. A better understanding of failures comes from an examination of the larger system in which such individuals work [Dekker 2002]. As Dekker explains, a system can be divided into a *proximal* sharp end (including people who are in direct contact with critical processes) and a *distal* blunt end (the organization that shapes, drives, and supports activities at the sharp end). In addition to providing resources, the blunt end creates constraints and pressures, which may present opportunities for errors at the sharp end. With this context and approach in mind, we present a review of relevant research in areas of human factors, cognitive science, psychology, and sociocultural factors—some with more proximal and some with more distal influences—that are relevant in considering UIT causes and mitigation strategies.

3.3 Relevant Human Factors/Cognitive Science Research

3.3.1 Human Error

Human error is a major factor in UIT—indeed, it is part of our definition of UIT. Human error is often the effect or symptom of deeper trouble. Human error is systematically connected to features of people's tools, tasks, and operating environment [Dekker 2002], so we will consider contributing factors further back in the chain of causes. But for now we will discuss the more immediate (proximal) effects of human factors that contribute to human error.

Human error is an ill-defined concept in the academic literature in part because errors can occur in cognition as well as behaviors. For the purposes of this report, *human error* is defined as a failure. Human errors account for about 80 percent of accidents in contexts ranging from air transport operations to nuclear power plants. This proportion has been increasing steadily since the 1960s due to such factors as greater system complexity and improved error analysis methods that enhance our error detection capability [Hollnagle 1993]. Human error analysis techniques have long been a mainstay of effective safety programs, with each implementation being tailored for a particular context.

Researchers in human error have adapted human information processing models to illustrate how individuals process hazards and how errors may occur in different stages of processing. In the communication-human information processing (C-HIP) model by Conzola and Wogalter [Conzola 2001], stimuli from the environment enter channels in the human sensory system. A subset of that information is attended to, comprehended, and aligned (or misaligned) with that person's attitudes, beliefs, and motivations, after which decision-making processes produce behavioral responses. Errors and limitations in the cognitive processes of perception, attention, comprehension, and decision making may produce bottlenecks and decrease performance.

Implications: It is widely accepted and documented that many mishaps of various types are inadvertent or unintentional, and that human errors underlying these mishaps often form patterns of recurrence when examined over time [Pond 2003]. More importantly, comparatively few safety incidents or information breaches are caused by individuals who purposefully seek to harm themselves, cause damage, or undermine information security. Instead, the human errors that cause negative impacts are often nearly inevitable consequences of ineffective system conditions, process features, or individual employee characteristics, and are therefore known as *system-induced human errors* [Norman 1983]. If a job requires the use of a ladder, an error could result in an accident; if a job requires the handling of sensitive, proprietary, or classified information, an error could lead to an information breach or security incident. Fortunately, evidence suggests that

many precursors that have been identified as relevant to safety are also relevant to security-related errors [Pond 2003]. While human errors can never be eliminated completely, those that are induced by external influences can be reduced dramatically through human error mitigation techniques that focus on the system conditions that contributed to, or even made inevitable, the resulting errors and adverse outcomes. By failing to identify and control the underlying, contributing causes of erroneous employee actions or decisions, we risk causing them again and again.

Contributing factors to human error in the cognitive domain include fatigue, high subjective mental workload, lack of (or loss of) situation awareness, and mind wandering. Additionally, emotional states, both normal and abnormal, can affect the human error rate.

3.3.2 Fatigue or Sleepiness

The effects of fatigue on human performance have been studied in diverse domains. The FAA is particularly interested in fatigue's effects on pilot performance because fatigue has been cited as a causal factor in several airline incidents. For pilots especially, changing time zones can cause sleepiness and shifts in circadian rhythms and sleep/wake cycles [Kryger 1994, Rosekind 1994]. In addition, shift work can adversely impact fatigue levels [Akerstedt 1998, Gander 1998], especially evening shifts [Signal 2006]. General sleep debt from reduced sleep cycles per 24-hour period results in subjective experiences of fatigue [Reid 2005, Signal 2006]. Gander and colleagues reported higher human error rates with greater cumulative sleep loss during rotating shifts [Gander 2008]. Various studies have documented an inverse relationship between performance and subjective experiences of sleepiness in sleep-deprived rail engineers [Gander 2002], F-117A pilots who were forced to remain awake for 37 hours [Caldwell 2003a], and commercial airline pilots [Co 1999].

The level of fatigue experienced affects the type of resulting performance decrements. A study of airline pilots found that as fatigue increases, the accuracy and timing of their trained behaviors wanes, their willingness to accept a lower standard of performance increases, their ability to integrate information from several instruments to generate a perception of reality is reduced, and their attention narrows such that they are less likely to attend to peripheral-vision information needed for safe flight [Caldwell 2003b]. Also, the frequency of social engagement between pilots and copilots is reduced [Caldwell 2012]. In addition, performance becomes less and less consistent as fatigue increases [Dinges 1990], and pilots often lapse into sleep, which causes them to miss task-relevant details often required for problem solving [Caldwell 2012].

Implications: The relationship between fatigue and performance has been well established, and this research clearly has implications for cybersecurity performance and UIT. If employees within a computing environment are sleepy, whether from jet lag, shifts in circadian rhythm, low points in circadian rhythm, shift work (static or rotating), or sleep debt, they may exhibit decreased attentiveness and increased inappropriate responses to critical network security information.

3.3.3 Subjective Mental Workload

For the purposes of this report, subjective mental workload is the personal feeling of being cognitively burdened by the work experience. The underpinnings of the relationship between subjective mental workload and human error come from the Yerkes-Dodson Law [Yerkes 1908],

which describes the relationship between arousal and performance as an inverse parabola. At the extreme low and high arousal levels, performance decrements occur. As arousal increases, performance increases until a maximum is reached and then begins to decline. Hence, an optimal level of arousal and stress are required for optimal performance with low error rates. The physiological stress response follows the same pattern [Lupien 2007]. It should be noted that not all people experience the same levels of subjective mental workload given a particular work load pressure [Crosby 1979, Damos 1978]; the experience of mental workload depends on the individual.

Subjective mental workload has also been described in terms of stress [Huey 1993, Ch. 2], and stress has been associated with human error in several ways. Stress narrows attention [Houston 1969, Stokes 1994] such that peripheral information is less likely to be attended to in high-stress situations [Weltman 1971]. Also, stress reduces working memory capacity such that less information can be held in memory at one point in time [Davies 1982, Hockey 1986, Wachtel 1968]. Finally, stress is correlated with higher incidents of perseveration [Zakay 1993]—the repeated execution of plans that have been used in the past regardless of their past effectiveness. In other words, a stressed person will continue to execute the same action in the same context but expect a different outcome [Shanteau 1993, pp. 293-308], which also adversely impacts effective decision making [Woods 1994]. When subjective mental workload is excessive, people may lower the threshold of acceptable performance such that performance degrades, find less demanding and more efficient ways to perform the same tasks, strategically not perform certain tasks (e.g., lower priority tasks), or not perform critical tasks [Hart 1990].

3.3.4 Situation Awareness

Endsley defines situation awareness (SA) as "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future" [Endsley 1995, p. 36]. SA has three levels:

- Level 1: attention or awareness of the elements in an environment
- Level 2: comprehension of the elements into a gestalt understanding of the system status
- Level 3: projection of future system states

SA is a *state* of knowledge about a given environment [Endsley 2000, Ch. 1]. A variety of factors can affect the process of building SA and, as a consequence, its accuracy. Generally, effective decision making to reduce error rates is predicated on having good SA [Rodgers 2000], though exceptions to this guideline exist [Endsley 2000, Ch. 1]. Human error correlates to poor SA rather than to poor decision making [Hartel 1989, Endsley 1995, Endsley 1999], though decision making requires SA. The appropriate amount of SA, rather than the maximum possible amount, is required for good decision making because operators can remember only a finite amount of information at any given time [Smith 1995]. To best utilize their finite memory and make critical, timely decisions in a dynamic environment, operators must perceive and attend to certain information and exclude irrelevant information [Prince 2000].

The relationship between SA and human error has traditionally been studied in aviation. In the study of operational errors made by air traffic controllers, 71% of the errors involved Level 1 SA (e.g., failure to perceive relevant information because of distracting tasks, memory burdens, and misperceptions), 21.4% involved Level 2 SA (e.g., inability to comprehend system status), and

28.6% involved Level 3 (e.g., over-projection of current trends that led to inaccurate future projections) [Endsley 1998]. Another study reviewed case studies of major airline accidents and found that in dynamic environments, information needed to improve SA was not being attended to even though checklists instructed pilots to review instrumentation panels to get information needed for good SA [Rodgers 2000].

Implications: In the computing world, incorrect or incomplete SA at any given time may result in human error that causes system failures, potentially increasing organizational risk. Employees must keep abreast of the latest attack vectors. Failure to perceive a phishing campaign (e.g., failure in Level 1 SA) may lead to failures to maintain network security.

3.3.5 Mind Wandering

Mind wandering has been defined as the process by which our attention is decoupled from the immediate task context, which makes us become absent-minded [Smallwood 2006]. William James [James 1892] suggests that mind wandering occurs when the individual experiences a meandering string of thoughts, some of which may not be influenced by the exogenous world of stimuli at a given moment. Thus, an individual can mind-wander through a series of thoughts that may or may not be related to incidents occurring in the task environment.

Cognitive processing and behavioral responses may be adversely affected by mind wandering. During subjective experiences of mind wandering, less attentional resources are available to dedicate to the task environment. Thus, attention to the exogenous world becomes decoupled from attention to conscious thought [Klinger 1978, Smallwood 2003a, Smallwood 2004, Smallwood 2007]. As a consequence of this decoupled state, the individual may develop a superficial representation of the environment [Smallwood 2006]. For example, mind wandering seems to reduce the encoding accuracy (i.e., the ability to create and store accurate human memories) of task-relevant information [Seibert 1991, Smallwood 2003, Smallwood 2007a, Smallwood 2008]. As a result, task-relevant memories are inaccurate [Smallwood 2003], which can compromise mental model building [Smallwood 2007a]. Similarly, off-task thinking has been related to response delays [Cheyne 2006, Smallwood 2007b], as well as higher rates of incorrect response execution [Smallwood 2007b]. Finally, the number of action slips—the execution of the wrong behavior when performing an automated task—increases during mind wandering [Broadbent 1982], as does the number of errors of commission, or the execution of the wrong behavior when the task requires controlled processing [Cheyne 2006, Helton 2009].

3.4 Risk Tolerance and Decision Making

3.4.1 Risk Perception and Risky Decision Making

In this report, we use the word *risk* to mean a measure of the probability and magnitude (severity) of adverse effects. This definition has been well established in the literature, including by Lowrance [Lowrance 1976] and the National Institute of Standards and Technology, which defines risk as the net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence [NIST 2002]. From a cognitive process point of view, risk tolerance and decision making under risk may be understood in terms of risk perception (a decision maker's assessment of the risk inherent in a situation), risk propensity (the general

tendency either to take or to avoid risk), and a decision process (determining how the individual will act in the face of a risky situation). Figure 1 illustrates relationships among these constructs.

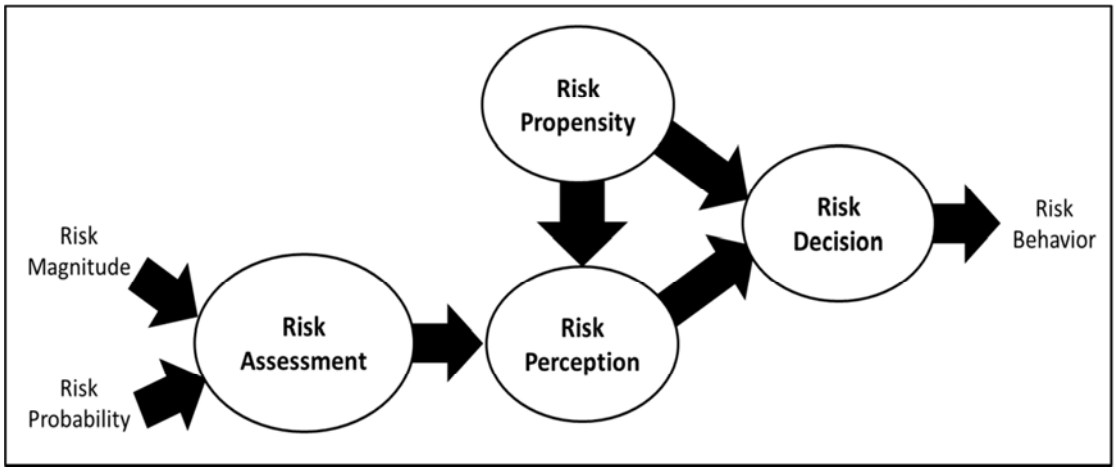

Figure 1: Descriptive Characterization of Risk Perception and Decision Processes

A risk assessment is based on perceived magnitude and probability of risk. Risk perception is a critical element of risk behavior and is influenced not only by the risk assessment process but also by individual differences in risk propensity (where an individual ranks in the continuum of risk aversion to risk seeking). An individual's ultimate decision under uncertainty (selection of a response among possible alternatives) may depend on perceived risk, the individual's risk propensity, and the decision process itself (which is subject to processing limitations, cognitive biases, and situational factors, as discussed above).

Psychological and cognitive science research may inform hypotheses about how constructs of risk tolerance and associated perception and decision processes influence UIT. Findings on risky decision making—how people perceive risk and react to risky situations—are situation specific and depend on organizational and individual characteristics as well as characteristics of the risk itself. Sitkin and Pablo reported that risky decision-making behavior depends primarily on risk propensity and risk perception [Sitkin 1992]. However, other studies concluded that the contribution of risk propensity to risky decision making may be insignificant [Keil 2000, Sitkin 1995]. Keil and colleagues reported that the magnitude component of risk is significantly more important in shaping risk perception than the probability component of risk [Keil 2000]. Further research is needed to build a more complete understanding of risk perception and risk tolerance in risky decision making, particularly in the context of UIT.

Risk tolerance and its components of risk perception and risk propensity are likely shaped by an individual's prior experiences, attitudes and beliefs, and other factors. Several disciplines outside of cybersecurity have conducted many studies of such individual differences in risk perception, and there is a significant body of research relating risk and cybersecurity (e.g., Alberts 2002, Pahnila 2007, Charette 1989, Charette 1990), including some studies addressing risk tolerance by unintentional insiders.

In the early 1990s, Robert Charette examined the subjective nature of risk and its effect on software systems [Charette 1989, Charette 1990]. The SEI leveraged Charette's work in the development of the Continuous Risk Management (CRM) and Software Risk Evaluation (SRE)

methods. These methods assume multiple perspectives of risk in software development organizations and attempt to consolidate those perspectives to arrive at an organizational consensus. The CERT Division of the SEI included this philosophy in the development of two early risk analysis methods: the Information Security Evaluation (ISE) and the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) [Alberts 2002]. The OCTAVE method brings together business, security, and IT staff to discuss risk from their perspectives and to create an organizational view of the current risk in relation to the organization's tolerance for risk.

We can speculate on how risk perception and risk decision making may relate to contributing factors and mitigation strategies for UIT. Some UIT cases studied for this report involved employees who were risk seeking (more likely to take risks than the average individual), and some involved those who were risk averse (less likely to take risks than average). These individuals may have perceived and formulated a network risk level during their decision-making process and subsequently made performance tradeoffs, for example, between work efficiency and taking additional precautionary measures. However, some individuals who committed UITs may not have been cognizant of network risk prior to committing the threat. For example, an employee experiencing high levels of stress and workload may commit user errors without any conscious thought of risk. This employee may rapidly move through tasks and accidentally infect a system by mistakenly clicking (i.e., committing an action slip) on a hyperlink involved in a phishing scam. Alternatively, an individual may be aware of the risk, but due to various factors (e.g., stress, time constraints, workload, illness) the individual consciously chooses to ignore the risk (for example, sharing a USB drive with an outside person even though this is against security policies).

Some individuals, despite their cybersecurity education, tolerate a high degree of risk. Security constraints are required to reduce their risk taking and keep systems more secure. In contrast, individuals who are risk averse may simply need education to prevent them from accidentally taking a particular risky action. Differentiating the risk-tolerant from the risk-averse individuals might enable an organization to increase or maintain productivity by appropriately targeting its security resources. Also, risk perceptions and risk-taking decision thresholds vary under different conditions, and an organization can act to influence those conditions and consequently minimize its associated risk.

3.4.2 Human Limitations and Biases

Limitations in humans' ability to predict the basic fundamentals of risk estimation—probability and magnitude—affect their perceptions of risk. Studies have shown that people are not very good at predicting the consequences, or impact, of an impending incident—in other words, at estimating risk. One probability prediction problem comes from lack of mathematical knowledge for probability calculation, which can vary from simple to complex. Other probability and impact prediction problems are influenced by human tendencies and cognitive biases that have been studied extensively by Kahneman and Tversky [Kahneman 1979]. Bruce Schneier writes extensively about various risks and how humans do not correctly assess their magnitude [Schneier 2008]. He lists five key ways in which people incorrectly assess the magnitude of risks: (1) exaggerating spectacular but rare risks but downplaying more common risks, (2) experiencing difficulties in determining risk for things outside of their normal situation, (3) underestimating

risks that they willingly take and tending to overestimate risks that are not in their control, (4) perceiving personified risks to be greater than anonymous risks, and (5) overestimating risks that are the object of public discussion [Schneier 2008]. The space shuttle Challenger accident of 1986 is a poignant example of how people can incorrectly assess the magnitude of risks. Following the accident, the Rogers Commission determined that the shuttle program's engineers and management had differing opinions regarding the risks of launching the shuttle; the engineers calculated a 1:100 probability of failure resulting in the loss of the shuttle and its crew, but the management calculated a 1:100,000 probability.

Kahneman and Tversky's [Kahneman 1979] prospect theory provides a widely accepted account of risky decision making. It is designed to account for how decision makers actually behave (considering their cognitive factors, limitations, and biases) in contrast to rational decision-making theories such as the expected utility theory. Prospect theory defines *value* in terms of gains and losses instead of utility; the value function for losses is steeper than the value function for gains (referred to as *loss aversion*). Prospect theory also considers problem framing: if a decision outcome is portrayed as a loss, then the value function will be convex and the decision maker tends to seek risk. However, if the outcome is portrayed as a gain, then the value function will be concave and the decision maker tends to be averse to risk. In one study of framing, participants chose the certain option more often when responding to positively framed problems and chose the risky option more often in response to negatively framed problems (those that offer a loss or deterioration of a situation) [Gonzalez 2005]. A study by Saner and Gonzalez showed that (1) providing decision makers additional information about the costs of using technology may more rapidly lead to better mental representations in technology-supported decision making, (2) positive framing is preferred to negative framing, and (3) increased expertise leads to more balanced decisions [Saner 2009].

As noted above, people are more likely to make risky decisions when problems are positively framed versus negatively framed. This is an example of a cognitive bias (framing). Numerous other cognitive biases have been studied and discussed (see for example, Kahneman 1979). *Confirmation bias* is particularly relevant. Confirmation bias is the tendency of people to favor information that confirms their beliefs [Nickerson 1998]. For example, Captain Larry Brudnicki (retired) was the commanding officer of the U.S. Coast Guard Cutter Tamaroa (WMEC-166) during the rescue operation depicted in the book and movie *The Perfect Storm*. During Captain Brudnicki's career, he conducted numerous accident investigations. He discovered that in almost every case, there had been enough risk information available to have avoided the accident. However, before embarking on a mission, captains would conduct a risk assessment for situation "A" and develop a plan "A" to deal with it. New risk information often presented itself in discrete, temporally separated segments. Captains would then find themselves in situation "B" but never deviate from plan "A." Brudnicki believes that the accidents were avoidable, but because the risk information was introduced slowly and in pieces, the victims did not re-evaluate the risk and so did not change their minds about what to do until it was too late.[5]

Implications: One implication is to frame insider threat decisions positively to encourage people to take fewer risks. Other suggestions are to make training more realistic, such as by including

[5] Captain Larry Brudnicki (retired), presentation to the National Reconnaissance Office, Chantilly, Va., 2008.

high-fidelity simulations and scenario-based problem solving, to encourage decision makers to be more responsible with their resources [Saner 2009]. Staff training should also include training and awareness of UIT risks and impacts. Cognitive biases such as flawed probability estimation and impact prediction may be addressed by discussing prediction biases and by using relevant and personal descriptions of risks, which will encourage more accurate risk perceptions that are aligned with organizational security objectives.

3.5 Relevant Research on Psychosocial and Sociocultural Factors

Individual differences in psychosocial, sociocultural, and cognitive characteristics may also affect the likelihood of an individual to cause a UIT incident. Risk tolerance, in particular, is likely shaped by an individual's prior experiences, attitudes, beliefs, and other factors. Several disciplines other than cybersecurity have conducted many studies of such individual differences in perception of risk, and there is a significant body of research relating risk and cybersecurity (e.g., Alberts 2002, Pahnila 2007, Charette 1989, Charette 1990), including some studies addressing the risk tolerance of unintentional insiders.

The following section discusses the possible effects of age, gender, culture, personality, and mood, especially within the context of risk tolerance and risky decision making.

3.5.1 Risk Tolerance as a Psychological or Personality Trait

An assessment of an employee's risk propensity (willingness to take risks) may prove useful to an organization's effort to identify and mitigate contributing factors to UIT. One way to measure risk propensity is to employ the Balloon Analogue Risk Task (BART), a computerized, laboratory-based instrument that involves risky behavior for which, as in real-world situations, risk is rewarded up to a point after which further risk results in poorer outcomes. Research shows that the results of the BART correlate with risk taking over a range of time [White 2008] and can be a predictor of risk-taking behaviors, including

- alcohol use, drug use, and cigarette smoking [Lejuez 2003]
- gambling, theft, aggression, psychopathy, unprotected sexual intercourse, sensation seeking, disinhibition, and impulsivity [Hunt 2005]

A different means of assessing risk propensity derives from demonstrated relationships between risk tolerance and personality predispositions. Nicholson and colleagues reported on personality correlates of risk-taking behavior [Nicholson 2005], relating risk-taking propensity with the Big Five personality traits: extraversion, openness, neuroticism, agreeableness, and conscientiousness [McCrae 2010]. Specifically, they found that overall risk-taking behavior correlates with high scores in extraversion and openness and with low scores in neuroticism, agreeableness, and conscientiousness. They conclude that personality profiles (in terms of the Big Five) are strong and distinctive and can be used to predict risk-taking behavior as follows: "high extraversion…and openness supply the motivational force for risk taking; low neuroticism and agreeableness supply the insulation against guilt or anxiety about negative consequences, and low conscientiousness makes it easier to cross the cognitive barriers of need for control, deliberation and conformity" [Nicholson 2005, p. 170]. Thus, measures of personality traits may shed light on individuals' propensity to take risks. Related research by Greitzer and colleagues examined

possible correlates of personality traits and individuals at risk of becoming insider threats [Greitzer 2012, Brown 2013].

3.5.2 Cultural Factors

Organizations can be placed and defined in a cultural context when they are viewed as a complex cultural system with their own reward system, social structure, language, economic and political systems, and religion [Jordan 2003]. Because risk perceptions are formed within the context of organizational culture, that culture should be considered an influencing factor on risk tolerance and decision making in the workplace. Culture in the broader sense informs decisions about risks and how to manage risks (see Boholm 2003; Douglas 1992; and Douglas 1982, p. 72).

Jordan describes organizational culture as a "web of interwoven and hierarchical cultural groups" [Jordan 1994, p. 5]. Organizational cultures and subcultures, as well as their national, regional, and industrial spheres of cultural interactions, can influence risk tolerance norms. According to Boholm, risk is "extremely contextual," and what is perceived as a risk is shaped by cultural beliefs, social relationships, power relationships, hierarchies, knowledge, experience, discourse, and practice [Boholm 2003, p. 175]. Thus, perceptions of risks are influenced by the cultural context in which they are formed. Ethnographic studies of public perceptions of risk have determined that individuals and communities develop and promulgate their own perceptions of risk [Reno 2011]. For example, in financial futures exchanges, stock exchange traders actively and voluntarily engage with risks, and they are rewarded socially and culturally [Zaloom 2004]. The propensity of Wall Street investment bankers to take risks in order to increase shareholder value has been directly linked to the investment banker culture [Ho 2009].

Organizational policies, practices, processes, and written values inform and shape organizational cultural knowledge, actions, and, ultimately, perceived risks. They also provide guidance on what behaviors are deemed appropriate, ideal, or inappropriate; they establish expectations and inform cultural knowledge. For example, most organizations have some type of enculturation process in the form of orientation or training, where new employees learn the stated and ideal values, ideal behaviors, and unwritten norms as well as the policies, practices, and processes that formalize the ideals.

Part of this enculturation may train employees on organizational policies and priorities for maintaining a secure environment. This would normally include learning the associated actions and behaviors. Armed with this cultural knowledge, the new employee observes and participates in the actual actions and behaviors, demonstrated values, and culture reinforced in practice and through storytelling. According to Feldman, storytelling, in the form of biographical accounts, myths, and legends, can communicate local and particularized notions of risk [Feldman 2001, p. 84]. Continuing with the security culture example, a new employee might observe that some employees and even managers do not practice the security measures put forth by the organization's formal enculturation. The employee must then determine his or her own risk tolerance. This scenario advances the case for examining the perceptions of risk in the context of the organizational culture in which it occurs. Most members of a cultural group or organization may agree to certain practices, but the more members that fall out of the cultural norm, as defined by the organization, the greater the exposed risk.

Implications: To mitigate cultural risks and to potentially influence perceived risk thresholds, organizations should gain a greater understanding of their own complex culture systems. The most common approach used by anthropologists is the ethnographic method [Geertz 1983], a qualitative approach that collects primarily observational and interview data and produces an ethnography [Clifford 1986]. Traditional ethnographic methods have been adapted for use in organizational settings and incorporate multiple data collection methods that allow observed behavior to be interpreted and placed in a culturally relevant and meaningful context [Fetterman 2009, Jordan 2003, Schwartzman 1993].

The heightened awareness of potential cybersecurity threats and their sources has influenced organizations to create and adapt their written and unwritten values, policies, processes, and other cultural artifacts to reduce the risk of a cybersecurity threat caused by an insider's action, whether intentional or unintentional [Silowash 2012]. Organizational culture should also be considered as an influencing force in the reduction of cybersecurity threat. Culturally informed strategies could be deployed to mitigate risks.

3.5.3 Gender

Previous research results have shown a correlation between gender and risk perceptions, as well as gender and risk taking. Byrnes, Miller, and Shafer reviewed more than 150 studies evaluating the risk-taking tendencies of female and male participants to find that men "are more likely to take risks than female participants" [Byrnes 1999]. A predominant number of studies have shown that men are less risk averse than women. According to Verbrugge, men from the ages of 17 to 44 sustain up to 60% more injuries than women do [Verbrugge 1985]. Courtenay states that males across all ages are more likely to engage in more than 30 behaviors that increase their risk of injury, disease, and death than do their female counterparts [Courtenay 2000]. A 1997 study reported that four times more men than women in the United States had reported that they had driven while drunk in the past month [Powell-Griner 1997]. Flynn, Slovic, and Mertz found that white males perceive risks at a much lower level than other groups [Flynn 1994], and Finucane and colleagues found that 30% of white males in the United States "judge risks to be extremely low" [Finucane 2000].[6] Differences in risk perception between the genders are not attributed to either education or rationality [Gardner 1989]. In addition, there is a difference in how men and women perceive risky situations [Figner 2011].

Some research has suggested that cultural conditions affect how people perceive risk and benefit [Weber 2008, Weller 2010]. According to studies, men are approximately 10% less likely to wear a seat belt than are women, and men were charged with driving under the influence approximately 500,000 more times than women in 2010 [esurance 2013]. For example, research indicates that teenage male drivers have a poorer perception of risk than females [Ivers 2009]. Women perceive a higher risk in recreational, ethical, and financial domains, while men perceive higher risk in social domains [Figner 2011]. BART testing has demonstrated that men tend to engage in riskier behavior than women [Hunt 2005]. Currently, there is limited research regarding the effects of gender on risk-taking behaviors within the field of cybersecurity and, in particular, in regards to taking unintentional risks specific to the workplace.

[6] According to the research of Finucane and colleagues, persons of color perceive risks to be higher than both men and women who are not of color [Finucane 2000]. They attribute this finding to sociopolitical factors.

3.5.4 Mood

An inconsistent body of research has sought to explain the influence of mood on making risky choices. Isen and Patrick developed a mood-maintenance hypothesis, which states that individuals in a negative mood tend to take greater risks than those who are in a neutral or positive mood, and that taking risks improves their overall mood [Isen 1988]. Other studies, such as by Bless and colleagues and Au, Chan, Wang, and Vertinsky argue the converse: individuals who are in a negative mood are actually more thorough in their processing and gathering of information than are those who are in a positive mood [Bless 1990, Au 2003]. Others have found that if people are in a positive mood versus a neutral one, they were more apt to be risk averse only when a possible loss was construed as salient or real [Isen 1988, Nygren 1996]. Further research is warranted in this area in order to better understand how to promote risk taking in the workplace when appropriate and how to decrease it when it is not.

3.5.5 Age Effects and Variations Over Time

Risk tolerance varies over time in individuals as well as in societies. Young drivers have a lower perception of risk than do older drivers [Ivers 2009]. Car insurance companies take this into account when determining insurance premiums for young male drivers [esurance 2013]. Risk perception threshold may increase in direct relation to the amount of time that one is exposed to a risk, in ways similar to the Stockholm Syndrome [Carver 2008, de Fabrique 2007], in which a captive begins to identify with the captor: a person in continuous contact with the same risk may adapt or become comfortable, to the point of no longer identifying the actual risk. For example, individuals living in areas with large-scale crime, terrorism, war, or natural disasters might come to accept or adapt to the surrounding risk and no longer perceive it the same way an outsider would. Another analog is the "Boiling Frog Syndrome" [Sedgwick 1888, p. 399]: if a frog is dropped into a bowl of boiling water, it will immediately jump out, but if the frog is placed into a bowl of room-temperature water very slowly raised to boiling, the frog will remain in the bowl until it dies. The evaluation of risk should be treated as a continuous process, and risks should be fully re-evaluated periodically to avoid the effects of lowered perceived risk threshold over time.

3.5.6 Influence of Drugs and Hormones

A drug may lower an individual's risk threshold by lowering inhibition or lowering risk perception sensitivity (e.g., might increase aggression and distract someone from perceiving a risk). There are many risks associated with overuse of drugs and alcohol, including loss of productivity, domestic violence, crime, family disruptions, financial problems, and failure in school [HealthyPeople.gov 2013]. The Healthy People study cited negative health problems or outcomes due to the overuse of substances such as drugs and alcohol, including HIV/AIDS or other sexually transmitted diseases, suicide, teenage pregnancies, and motor vehicle crashes. Likewise, risk-taking activities have a propensity to increase with substance use and abuse. There is a great deal of research on the impact of substance use and risk taking among adolescents. One study finds that "an estimated 6% of 16 to 17 year olds and nearly 17% of 18 to 20 year olds reported driving under the influence of alcohol in the past year" [Stagman 2011], possibly implying causation of a lower threshold for risk taking due to the influence of alcohol. According to another study on young adults, condom use was less likely among participants who had consumed five or more drinks on at least one occasion over the past year, increasing the probability of contracting a sexually transmitted disease [Graves 1995].

Hormones also play a role in the amount of risks that people take, particularly dopamine, the "feel-good chemical" in the brain [Park 2008]. Zald and colleagues found that dopamine is more pervasive in the brains of risk-takers, or that they have fewer dopamine-inhibiting receptors [Zald 2008]. They conclude that people with these higher levels of dopamine are more likely to take risks such as abusing drugs and other unsafe behaviors.

Implications: Drug education and policies (zero tolerance, along with rehabilitation programs available through employee assistance programs [EAPs]) should encourage a drug-free environment that reduces risk-taking behavior due to drug use.

3.6 Addressing Causal Factors at a Deeper Level

We have described many contributing factors to human error, risk tolerance, and decision making that are relevant to UIT. Most of the factors having to do with human performance, human error, risk behavior, and judgment may be considered proximal factors that, in turn, are also influenced by other more deeply seated organizational and human factors. As we have noted, human error is intimately related to UIT incidents, but a more complete understanding of UIT and its causal factors requires examination of deeper organizational or systemic factors that make errors and lapses more likely and perhaps exacerbate the effects of cognitive biases. UIT errors or lapses, like errors in general, may be classified as follows:

- unintentional acts ("I didn't mean to do that.")
- unintentional failures to act ("I forgot to do that.")
- intentional but incorrect acts ("I thought that's what I was supposed to do.")
- intentional but incorrect failures to act ("I didn't think I was supposed to do that.")

Arguably, a significant proportion of UIT incidents may result from deliberate but nonmalicious deviations from required policies and practices; these are typically referred to as *breaches*. Lack of good judgment or carelessness (i.e., negligence) is the characteristic feature of acts that increase the potential for a breach. The related fields of human factors and safety have a substantial body of evidence regarding the identifying factors of human error. The current view of human error compels us to examine not only proximal causal factors but also more deep-seated (distal) factors underlying human errors. Distal factors have been organized into a taxonomy comprising four categories of error or breach precursors [Pond 2003]:

- data flow—inadequate procedures/directions, poor communication
- work setting—distractions, insufficient resources, poor management systems, inadequate security practices
- work planning/control—job pressure, time factors, task difficulty, change in routine, poor task planning or management practice, lack of knowledge/skills/ability
- employee readiness—inattention, stress and anxiety, fatigue and boredom, illness and injury, drug and hormone side effects, values and attitudes, cognitive factors (misperception, memory, judgment)

Virtually all of the proximal factors described previously in this report fit easily into this taxonomy. For example, problems in data flow can negatively affect operator performance through deficits in SA or increased workload, both of which can contribute to errors. Similarly, problems in work setting and management systems, such as lack of available qualified staff or

inadequate or flawed policies, may lead to increased workload, increased stress, or other factors that affect information processing and decision making and lead to errors and failures. Problems with work planning and control, such as changes in routine, can affect performance through increased fatigue or stress. Deficiencies in employee readiness tends to negatively impact performance due to insufficient knowledge for correct task completion, as well as associated anxiety and stress that further affects judgment and decision making.

Implications: Identifying these contributing factors would enable organizations to conduct systems analyses and change any parts of their environments, systems, and procedures that foster these precursors. These analyses and associated changes to workflow, data flow, work setting, planning, and awareness of the impact of employee readiness on performance and job satisfaction might be largely coincident with organizational analyses that address malicious insider crimes.

3.7 Summary of Causal Factors and Possible Mitigation Strategies

As noted above, a comprehensive approach to addressing contributing factors to UIT incidents includes general and organizational best practices as well as specific strategies that may be tailored to identified human factors, cognitive limitations, psychosocial and sociocultural factors, and other factors. Table 1 summarizes the factors and their possible mitigation strategies reviewed in this section.

At the highest level, organizational improvements affecting the distal factors of human error and UIT incidents should focus on maintaining productive data flow, work setting, work planning and control, and employee readiness. As an example, implementing security best practices throughout the organization, as defined by widely tested and implemented security norms in the industry, should positively impact UIT mitigation goals. Best practices have been designed to help individuals and organizations perceive risks and mitigate normal human and organizational tendencies that can be problematic.

More specific mitigation strategies may be tailored to address particular human factors, cognitive limitations, and psychosocial and personality factors that may be associated with risk-taking behavior, and training might be tailored for the highest risk individuals.

Table 1: Summary of Research Identifying UIT Contributing Factors and Possible Mitigations

Factors	Effects	Possible Mitigations
Human Factors/Cognitive Factors		
Fatigue or sleepiness	• Increased likelihood of human error • May not evaluate risk properly and increase inappropriate responses to critical network security information	• Employ automated tools to circumvent poor user decisions • Improve management practices to foster a productive work environment (e.g., decreasing stress and increasing self-care)
High Subjective mental workload	• More likely to shed tasks related to risk mitigation without being aware of it	• Assist in prioritizing critical tasks • Employ automated tools to circumvent poor user decisions • Maintain an optimal level of arousal and stress for low error rates
Lack of Situation awareness (SA)	• Increased potential for human error (e.g., opening a phishing email)	• Keep employees abreast of latest attack vectors and other threat-related news • Improve design of user-system interfaces to lower risk of errors

Factors	Effects	Possible Mitigations
Mind wandering	• May lower ability to detect a risk	• Provide employee assistance programs (EAPs) to help employees reduce outside stresses, which may cause mind wandering • Provide adequate health insurance benefits for mental health care • Employ automated tools to circumvent poor user decisions
Framing	• Positively framed risks may lead to less risky choices	• Increase expertise leading to more balanced decisions • Provide info about costs of using technology • Use appropriate framing to generate more risk-averse attitudes • Positively frame security/risk-related decisions to support less risky choice
Other cognitive biases (probability and impact prediction, perceived incidents)	• Cognitive biases or limitations may lead to inappropriate evaluation/prediction of risk (errors in estimating probability and/or impact) • Incorrect evaluation/prediction of risk due to the inability to or refusal to calculate it correctly, sometimes because of incorrect over-weighting of spectacular incidents	• Provide training/awareness of cognitive biases such as prediction biases • Employ personal/relevant descriptions of risk • Remind employees *not* to discount the probability of a particular (nonspectacular) concern • Educate employees about math methods for probability calculation • Educate employees about historical accidents and their preceding risk estimations • Review systems designed to minimize security risks, including the CERT CRM and SRE methods
Psychosocial, Sociocultural, and Other Factors		
Personality predispositions	• Individuals with various personality predispositions perceive risks as higher or lower than others without the predispositions	• For high risk takers, apply strategies more often and with a greater degree of tailoring • Encourage awareness of individuals' biases and tendencies • Provide training and awareness • Improve management practices • Implement more effective security practices and processes • Improve design of user-system interfaces • Employ emotion- and logic-based influencers
Culture and subculture	• Different risk perceptions due to (organizational, national, other) cultural norms	• Evaluate organizational culture of work environment • Outline/develop ideal cultural workplace norms • Thoroughly orient new employees and provide continued training • Utilize ethnographic methods and maintain understanding of differing cultural norms • Employ emotion- and logic-based influencers
Gender	• On average, males have lower perceived risk thresholds and females have higher perceived risk thresholds	• Provide opportunities for training and fair advancement • Utilize effective learning tools based on learning styles and existing knowledge base
Mood	• 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	• Provide workplace environment programs that enhance respectful and calm environments • Ensure that employees have affordable access to mental health services, including drug treatment • Provide EAPs • 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

Factors	Effects	Possible Mitigations
Age effects and variations over time	• Previous decisions about risk levels reduce ability to perceive slowly rising levels of real risks; some age ranges correlate with lower perceived risk thresholds	• Provide recurring training of potential threats and their significance via systems security mailing lists, websites, and news organizations • Conduct incident-driven reviews of policies, practices, processes, and training materials • Periodically, fully re-evaluate risk to avoid the effects of lowered perceived risk threshold accumulated over time
Influence of drugs and hormones	• Drugs may have negative effect on cognitive ability • May cause incorrect evaluation or prediction of risk	• Ensure access to appropriate treatment for drug use or abuse; conduct drug testing (within restrictions)
General Organizational Factors		
Business process requirements (BPRs)	• BPRs that make changes too arduous discourage risk reduction changes	• Apply risk management and measurement and analysis concepts and approaches to critical business processes to ensure they are providing the intended results, with periodic and incident-driven review • Maintain records of reviews

4 Comprehensive UIT Feature Model

A feature model captures and models a collection of features to characterize instances of a concept. We have developed a UIT feature model that captures UIT incidents in the form of roles, causes, and other relevant information that are features of an incident. The model draws its feature types from the third chapter of this report, Related Work, which distinguishes between intentional and unintentional threats, the human factors that contribute to a UIT, and causal factors of an incident. The UIT feature model also draws on case studies, whose details help flesh out the model's roles, causes, and other features.

We developed the UIT model to represent relevant features of any incident. The model includes a hierarchical diagram (Figure 2) depicting the decomposition of the concept into parent features and child subfeatures. The diagram also categorizes features as mandatory (always part of a UIT incident), optional (may or may not be part of an incident), or alternate (one or more of a group of related features).

We followed three steps to build the model:

1. Identify the features. We examined case studies and reflected on the UIT Related Work research, taxonomy, and definition.
2. Characterize the features as mandatory, optional, or alternative. We again used the case studies to refine feature definitions.
3. Document the feature definitions and relationships. We annotated each feature and determined patterns of activity that lead to relationships among features.

We used the Pure Variants Eclipse plug-in (pure::variants GmbH 2012) to generate the model, which contains four types of features (mandatory, optional, and two types of alternate features; see Table 2).

Table 2: Model Feature Types

Feature Type	Description	Symbol
Mandatory	A mandatory element is implicitly selected if its parent element is selected.	!
Optional	Optional elements are selected independently.	?
Alternative	Alternative elements are organized in groups. Exactly one element must be selected from a group if the parent element is selected (though this can be changed using range expressions). pure::variants allows only one *Alternative* group for the same parent element.	
Or	Elements are organized in groups. At least one element must be selected from a group if the parent element is selected (though this can be changed using range expressions). pure::variants allows only one *Or* group for the same parent element.	

The feature model of the UIT concept is based on features of a UIT incident. The model categorizes four mandatory features for each incident: the roles of the individuals in a UIT incident, the underlying causes, the system and format of the disclosed data, and the industry sector or government agency where the incident occurred. The feature model describes UIT incidents in terms of these mandatory and subordinate features:

- *Role*—identity of individual(s) responsible for a UIT (mandatory)
  - *Insider* (mandatory)

  - *Bad Actor*—also called a "malicious outsider"; may play a role in a UIT-HACK incident (optional)
- *Cause*—includes immediate and contributing factors that led to the incident (mandatory)
  - Immediate (proximal) factors
    - *UIT-HACK* (alternative)
    - *DISC* (alternative)
    - *PORT* (alternative)
    - *PHYS* (alternative)
    - *Data destruction* (alternative)
    - *Data corruption* (alternative)
  - Contributing factors (mandatory)—error/breach precursors that led to the insider's action or inaction. The following subfeatures are broken down into various sub-subfeatures (see Section 3.6, Addressing Causal Factors at a Deeper Level, and Table 1).
    - *Data flow* (alternative)
    - *Work setting* (alternative)
    - *Work planning and control* (alternative)
    - *Employee readiness* (alternative)
- *Mode of data release*—data format and system of a disclosure (mandatory)
  - *Format* (mandatory)
    - *Electronic*
      - *Encrypted* (optional)
      - *Classified* (optional)
    - *Non-electronic*
      - *Classified* (optional)
  - *System*—for data loss through a UIT-HACK or DISC (optional)
    - *Internet*
    - *Intranet*
    - *Social media*
    - *Email*
    - *Cloud*
    - *Mobile/ubiquitous computing devices*
- *Industry*—sectors where the incident occurred, such as businesses (*Financial/Banking*, *Healthcare*, *Civilian* or *Military Government*, etc.). The sectors are alternative features.

The feature diagram in Figure 2 captures the top-level mandatory features and all subordinate features.

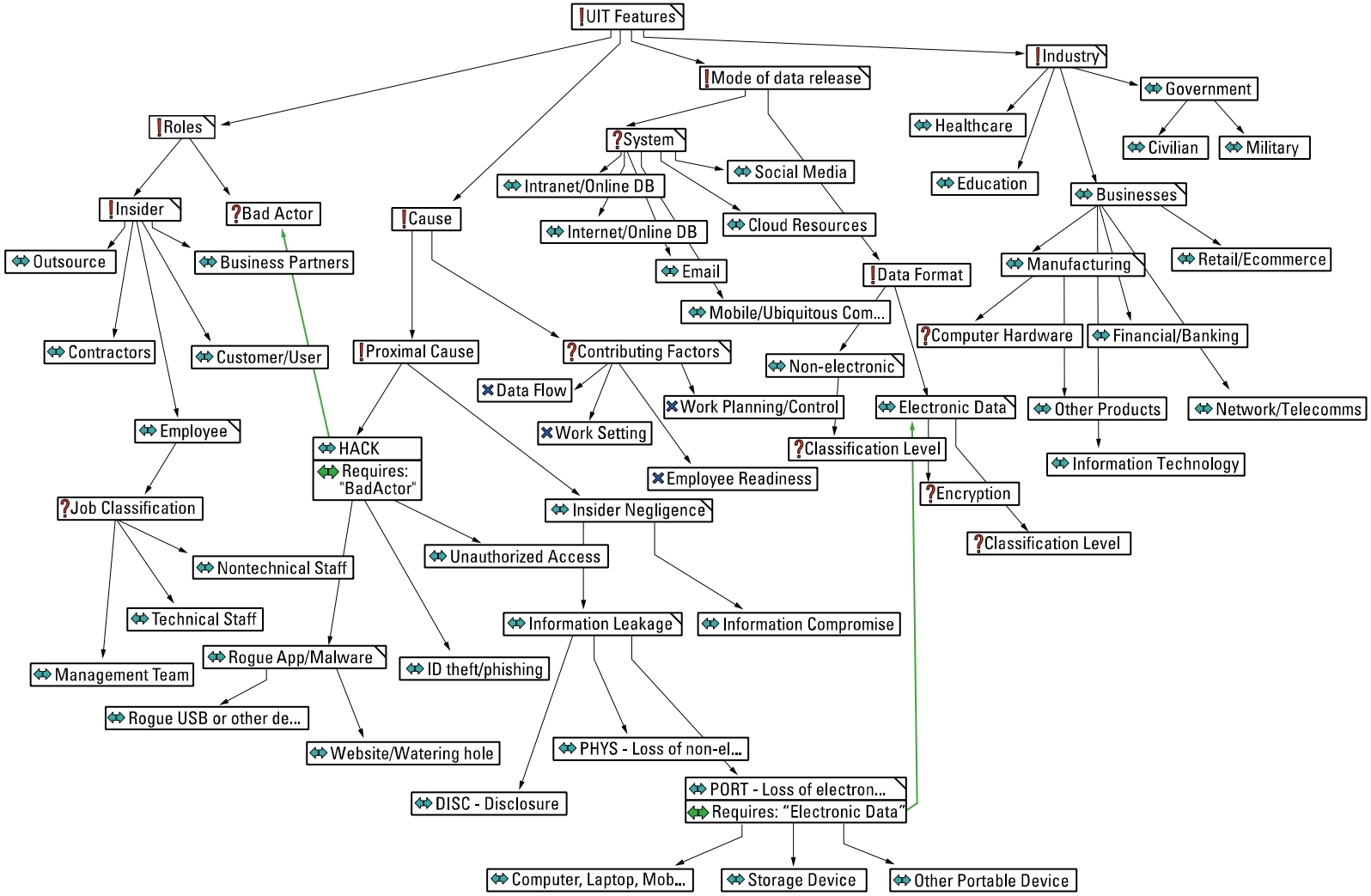

Figure 2: Comprehensive UIT Feature Model

Under each of the four top-level features are grouped subordinate features that qualify the top-level features. For example, the *Roles* feature must include an insider (mandatory) and may include a *Bad Actor* (optional). The *Bad Actor* is linked to a *UIT-HACK*, a subordinate feature to *Cause*, because a *UIT-HACK* incident requires a *Bad Actor*. Within the *Insider* feature are several different types specified by the subordinate alternative features under *Insider*. The other top-level features and their subordinates follow these same hierarchical rules.

The model also shows two relationships:

- A *UIT-HACK* requires a *Bad Actor* who obtains insider information (via unauthorized access, identity theft, or the introduction of a rogue app or other malware).
- A *PORT* always results in loss of electronic data.

Other relationships may be added or discovered as the model is refined through analysis of new incidents. We use the comprehensive feature model to characterize UIT cases we have collected, as described in the next section.

5 Summary of Collected Cases

5.1 Description of Case Collection Requirements

Cases collected for this study included either of the following situations:

- A nonmalicious insider makes a mistake or loses a device.
- A secondary actor influences a nonmalicious insider to take an action that provides the actor access to the assets or at least enables the actor to have a potential impact on them.

We adopted the DISC, PHYS, PORT, and UIT-HACK breach types from the PRC database, with the following caveat and modifications: we included only cases that may be attributable to unintentional incidents involving insiders. Assessing a DISC, PHYS, or PORT incident as a UIT breach was a relatively straightforward task; most of these incidents clearly involved the insider's unintentional release of equipment or material, except for situations where an outsider stole material or equipment without direct or indirect facilitation by an insider. Assessing UIT-HACK incidents required more scrutiny because many of these incidents were carried out by external actors. Collecting examples and statistics for UIT-HACK incidents required a manual review to determine if cases involved only an outside attack with no insider involvement, versus the exemplary case of an insider inadvertently enabling the potential or actual entry or access of malicious code.

Incidents can be succinctly summarized and expressed in a clear and consistent manner for informal review. The UIT incident template for these summary descriptions is as follows:

- **INCIDENT ID** <number from MERIT database or from public sources, with PRC entry date if available>
- **INDUSTRY** <classification of organization>
- **THREAT VECTOR** <UIT-HACK, DISC, PORT, PHYS>
- **INCIDENT** <condition that precipitated the incident>
- **BREACH** <type of loss or compromise>
- **OUTCOME** <nature and type of data potentially compromised>
- **RESPONSE** <specific action taken in response to the breach>
- **OTHER** <other incident information that supports the analysis>
- **IMPACT** <how the loss or compromise affected the organizations involved>
- **REFERENCE** <URL or reference to source of incident description>

5.2 Case Collection Examples

The following two examples illustrate the summary information for PORT and DISC UIT incident causes and follow the UIT incident template.

Incident ID 440

INCIDENT ID: MERIT ID 440, PRC (June 30, 2010)

INDUSTRY: Healthcare

THREAT VECTOR: PORT

INCIDENT: Contractor sent CDs containing billing information to parent company that outsourced the work.

BREACH: CDs were lost in transit.

OUTCOME: Data on CDs included Social Security numbers (SSNs), addresses, dates of birth, health plan numbers, driver's license numbers, and descriptions of medical procedures.

RESPONSE: CDs were never recovered, and disposition of data is unknown. Parent company had to disclose loss of data to its customers.

IMPACT: Shipping company suspects CDs were "swept up and destroyed" in the manufacturing plant.

REFERENCE: www.theregister.co.uk/2010/06/30/patient_data_exposed

Incident ID Web 05

INCIDENT ID: Web 05

INDUSTRY: Government—State

THREAT VECTOR: DISC

INCIDENT: A State health-assistance program informed 14,000 individuals that it had accidentally published their Social Security numbers.

BREACH: Accidentally published sensitive information that remained up on a government site for at least nine days before it was removed.

OUTCOME: Highly personal information, which also included names, care information, and home addresses. The leaked data affects medical providers in 25 of the State's counties.

RESPONSE: Unknown.

IMPACT: Similar breaches in the past exposed the personally identifiable information of more than 750,000 persons in multiple incidents within the same State.

OTHER:

REFERENCE: www.nbcnews.com/id/50186718/ns/technology_and_science-tech_and_gadgets/

The spreadsheet in Appendix B summarizes the entire collection of UIT case study incidents.

5.3 Sources of Collected Cases

This research effort collected more than 40 case studies altogether. Some did not meet the criteria and were rejected, leaving 35 cases for full analysis. The primary sources of case information were

- the Privacy Rights Clearinghouse.[9] The PRC provides summaries of incidents that are of interest to this study. The incident reports may include links to lengthier descriptions or follow-up information gathered since the initial report.

[9] www.privacyrights.org

- the CERT Division's MERIT database. This is the CERT Division's database of insider threat cases. It includes data on more than 800 insider threat cases, with information derived from court documents, investigator notes, news stories, and business and research partners.
- library sources. We searched online databases for information specific to UITs. The searches returned reports from the press and other publicly available information sources, as cited in each case study.

5.4 How the Feature Model Supports Analysis of Case Studies

The study used the feature model to support analysis of each qualifying case study. The analysis first considered the frequency of the types of incidents at the second level of the hierarchy (immediately under each top-level feature) and those second-level incidents' immediate subordinate features (third-level features). The feature model also helps characterize threat vectors and their basic patterns of activity. Finally, features can be used as a way to search for specific types of incidents, especially in emerging areas such as cloud, mobile, and ubiquitous computing (UbiComp) under the *System* feature.

5.5 Breakdown of Case Collection Frequency by Features

The following figures show the number of subordinate features under each of the four top-level features (*Roles*, *Cause*, *Mode of Data Release*, *Industry*). We use these numbers to make certain assertions about the case collection.

5.5.1 Roles Features

Though this report summarizes 35 cases of UIT, the feature total for *Roles* is greater than 35 because, in some of the cases, more than one role was assigned to a single case (e.g., *Bad Actor* and *Nontechnical Staff*).

Roles	41
Insider	34
Employee	18
Job Classification	
ManagementTeam	5
TechnicalStaff	0
NonTechnicalStaff	5
Customer/User	2
BusinessPartners	0
Contractors	1
Outsourcee	3
BadActor	7
Cause	34

Figure 3: Roles of Unintentional Insiders

Cases that did not explicitly specify the insider's role were assigned to the *Employee* feature. *Job Classification*, an optional feature, was used only when a specific position was mentioned in the report. The absence of the *Technical Staff* subfeature implies that these employees may be more alert to potential risks of causing an incident, due to better training or use of better tools.

Organizations should study their internal operations to see if more *Insider Negligence*, under the *Cause* features, can be attributed to nontechnical staff than to technical staff. If this preliminary analysis proves correct under further scrutiny, organizations may want to examine their internal policies to create a less incident-prone environment for that staff category.

5.5.2 Cause Features and Summary by Threat Vector

As discussed above, the *Cause* feature includes both proximal and contributing factors. While the existing research emphasizes the importance of the contributing factors leading to a UIT incident, the incident reports do not provide sufficient detail to determine contributing factors. For that reason, no data is currently entered for those features. Future work on UIT could include direct interviews or workshops with organizations to understand the relationship of contributing factors to specific incidents. This would allow us to flesh out the feature model and, possibly, to relate one or more contributing factors to proximal cause.

The primary reason for excluding a case study from the collection was determination of *Cause*. PHYS and PORT incidents generally have straightforward causes—an insider loses a device or a collection of non-electronic records—so we counted all cases in these two categories as UIT incidents. Determining the cause of UIT-HACK or DISC incidents is more involved because cases in these categories must include an outside attack (by a bad actor) resulting in an insider action that leads to the actual UIT event. Determining whether an incident is a UIT-HACK or DISC requires analysis of the incident and specific information that may not be known, may be ambiguous, or may not be disclosed for security or privacy reasons. Most of the case studies we found and later rejected from the collection were rejected due to insufficient information. For example, an incident that results from malware may be a UIT-HACK if an insider inadvertently introduces malware into a system. However, we could not assume that an unintentional action led to a UIT-HACK unless the case study explicitly stated that fact. Malware can be planted and information obtained without any insider participation. Given that the *Insider* feature is mandatory, any incident without it cannot be considered a UIT incident.

Once we determine that an incident is a legitimate UIT incident, we know that all UIT-HACK incidents derive from an outside attack with subsequent insider involvement inadvertently enabling the potential or actual entry or access of malicious code. These can be distinguished from DISC incidents where the actions of an insider alone result in data loss.

To produce a picture of the UIT threat at the highest level, we aggregated the case study data across the various industry sectors or types of organizations (i.e., businesses, educational institutions, government/military, healthcare) for cases that met the requirements. This produced a general summary of results and trends for the UIT threat vectors involving DISC, PHYS, PORT, and UIT-HACK breaches. In the future, a more detailed analysis of this data should be conducted to break down the cases according to the *Cause* feature and their respective, associated critical infrastructure sectors. For example, are UIT-HACK incidents more likely to occur in businesses or in government?

UIT-HACK incidents accounted for 17% of all incidents in the collection. This frequency is somewhat lower than that reported by the PRC data, but the PRC data for UIT-HACK also include incidents with no insider involvement. ID theft/phishing exploits were the most common and represented 50% of the UIT-HACK incidents. A small percentage of cases involved rogue

USB or other devices. The one reported in the collection resulted from failure of the insider to perform a routine malware scan of the device. It is possible that this vector can account for numerous computer security breaches that were not reported as UIT cases and that, as a result, our searches could not locate. The increasing attention devoted to USB-drive, malware-based exploits [Clark 2009, Clark 2011, Phule 2012, Booz Allen 2012] suggests that this is a real problem for which practical automated prevention and mitigation solutions are attainable. Website/watering-hole incidents were also part of the UIT-HACK vector.

While results are preliminary due to the limited amount of data collected to date, we found the following breakdown of the 35 incidents in the collection: 49% of the cases collected were associated with the DISC UIT threat vector, 6% with PHYS, and 28% with PORT. With nearly half of the incidents falling in the DISC category, the study determined that release through the internet accounted for 20% of the DISC losses and release through email accounted for 23% of losses. The combined incidence rate for PHYS and PORT (related to loss of electronic devices or non-electronic records), accounts for roughly one-third of the incidents, and points to an immediate requirement for improved handling practices.

These findings are preliminary due to the small sample size of 35 incidents. More cases must be collected to generate enough data to support more definitive analyses and conclusions. Mitigation strategies for precedent DISC incidents are covered in our Section 7, Mitigation Strategies for Unintentional Insiders. Further analysis of the collection could produce additional features to refine the definition of DISC incidents and support their mitigation. A further analysis of the case studies could reveal relationships among these three top-level features or among one or more subordinate features.

Cause	**34**
Contributing Factors	
Data Flow	
Work Setting	
Work Planning/Control	
Employee Readiness	
Proximal Cause	34
HACK	**7**
UnauthorizedAccess	1
ID theft/phishing	2
Rogue App/Malware	4
Rogue USB or other device	0
Website/Watering hole	0
Insider negligence	27
Information Leakage	27
DISC - Disclosure	15
PHYS - Loss of non-electronic data	2
PORT - Loss of electronic data	10
Computer, Laptop, Mobile device	3
Storage Device	7
Other Portable Device	0
Information Compromise	0

Figure 4: Causes of UIT Incidents

5.5.3 Mode of Data Release Features

The *Mode of Data Release* feature provides insight into how data unintentionally becomes available to parties outside an organization. At this time, these data are not correlated to roles or cause.

The data collected show that release through the internet and email account for 20% and 23% of losses, respectively. Social media, such as Facebook, accounts for 11%. Data release from an intranet accounts for 11%, a result that reveals a serious flaw in internal security: the organizations could not protect data even on internal websites, at least as reported. Most electronic data losses were unencrypted. Even using the simplest encryption techniques should reduce the impact of data loss.

Mode of data release	**34**
System	22
Internet - Online DB	6
email	7
Social Media	4
Intranet/online DB	3
Mobile/Ubiquitous Computing	1
Cloud resources	1
Data Format	12
Other, non-electronic	2
Classification Level	
Electronic Data	10
Encryption	2
Classification Level	

Figure 5: Modes of Data Release

5.5.4 Industry Features

These features are very strongly biased toward government: our analysis showed that 65% of the cases are from the government sector, though the PRC's collection includes less than half that percentage in the same category. Further analysis of our collection and collection methods could reveal why our search turned up a disproportionate percentage of government cases. As explained above, no analysis was conducted to determine the relationship among the top-level features, but such a study could show the frequency of *Cause* or *Mode of Data Release* within an *Industry* group. That study could put special emphasis on precedent types of data loss specific to the industries.

Industry	**34**
Businesses	10
Financial/Banking	4
Retail/e-commerce	1
Information technology	2
Network/telecomms	2
Manufacturing	1
Computer Hardware	1
Other products	0
Government	20
Civilian	17
Military	3
Healthcare	4
Education	0

Figure 6: Industry in Which Release Occurred

5.5.5 Patterns of Incidents

At the top level, we can identify three patterns of incidents based on the threat vector:

1. UIT-HACK constitutes a pattern where a Bad Actor initiates an action that leads to an insider action that releases data. Variations of this pattern are based on the three forms of a UIT-HACK: *Unauthorized Access*, *ID Theft/Phishing*, and *Rogue App/Malware*. Each requires a different form of mitigation.
2. DISC constitutes a pattern where a specific action of an insider results in a loss of data. As explained above, further analysis of this threat vector is required to model subordinate features and develop targeted mitigation strategies.
3. PHYS and PORT are loss patterns, where an insider action results in loss of non-electronic data or a device. While type of device was included in the model, further analysis may reveal an underlying cause for a loss such as theft, unintentional discarding, or careless handling. Again, these underlying causes each may have specific mitigations.

5.5.6 Emerging Causes of Incidents

This study examined current incident reports and UIT literature to model the *Cause* feature. The literature points to two of these causes as a potential for significant losses in the future. The cybersecurity community recognizes that the growing use of cloud resources requires additional study of security policy, especially in setting Quality of Service (QoS) standards. Even with internal corporate standards, the UIT case collection contains a significant number of DISC incidents that could have been prevented with improvements in internal security. With cloud resources, an organization becomes dependent on another layer, an outside organization or *outsourcee*, to prevent loss. Targeting this area for mitigation strategies could be highly beneficial as the dependence on such outside organizations grows.

The growth of mobile technology and especially Bring Your Own Device (BYOD) policies adds a second technology trend with its own potential for UIT. The collection includes one such case, and others are emerging. An office setting should make the insider more cognizant of his or her responsibility to control mobile technology. But insider negligence may still result in a UIT incident. Given the variety of environments in which mobile devices are used, and, potentially, the frequency of their loss via PORT incidents, this category requires special mitigation strategies. UbiComp poses a new threat. The insider may not be aware that the device, for example a smart phone operating as a WiFi hotspot or a wearable computer, is subject to a UIT-HACK or a UIT incident. The growing popularity of these devices and potential for data loss require further analysis to identify mitigation strategies.

6 Unintentional Insider Contributing Factors and Observables

As discussed in Section 3, Related Work, various distal contributing factors to human error and other related cognitive deficits and risk behaviors have been categorized in terms of four broad categories—data flow, work setting, work planning and control, and employee readiness—into which virtually all organizational best practices might fall as strategies for promoting healthy, productive work environments as well as sustaining conditions that help to reduce UIT incidents.

Of great concern are more specific contributing factors that are in play despite efforts to apply best practices. Here we focus on how to recognize signs of such failures. Table 3 shows possible contributing factors identified or inferred from published research with suggestions about how these factors might be recognized or observed. (Compare these with the factors listed in Table 1, on page 19; Table 3 focuses on factors relating to cognitive limitations, biases, and risk perception and risk tolerance.) The right two columns of the table are defined as follows:

- **ISMS (ISMS Implementation)—**implementation of a standard Information Security Management System (ISMS) framework, such as the Bell Labs Security Framework [McGee 2007] and ISO 27001-2 standards, which requires various thorough examinations of systems for security risks
- **Auto (Automated Security Systems)**—use of standard systems (antivirus, intrusion detection and prevention system [IDS/IPS], firewalls, backup systems, security information and event management [SIEM] systems, static and dynamic software code checkers, etc.) that identify errors and help identify wrongly taken risks, both to the individual and to the organization

Table 3: Some Potential Observation Methods per Factor

Factor	Observation Method	ISMS	Auto
Willingness to take risks	Willingness to take risks may be measured using the Balloon Analogue Risk Task (BART), a computerized and laboratory-based measure shown by many studies to correlate with a wide variety of risk-taking behaviors [White 2008, Lejuez 2003, Hunt 2005]. Alternatively, linguistic analysis of word use as measured by the Linguistic Inquiry Word Count (LIWC) [Tausczik 2010] has demonstrated some success in correlating particular types of words to high or low risk taking [Moons 2013]; however, the applicability of this result to an individual's general risk perception thresholds has yet to be determined. Benefits of the latter method would include simplicity, speed, and expected low cost of electronics communication monitoring for word count.	•	•
Predisposing personality	Personality tests for aspects of personality.		•
Gender	Gender is often visually observable, and it can be tested for genetically and derived from medical records.		
Age	Age range is often visually observable, and exact age can usually be derived from medical records and medical tests.		

Factor	Observation Method	ISMS	Auto
Perceived incidents	Perceived incidents, particularly the spectacular kind, are sometimes public news incidents. Similarly, some common, unspectacular risks may be well known by the organization specifically because the risks are common.		
Mood	Mood of an individual might be observed by colleagues visually noticing body language or through conversation, writing, psychological tests, or automated linguistic analysis of electronic communications.		
Particular drugs	Drug use might be observed using medical drug testing, for instance, urine sample tests, blood tests, hair sample tests, and breathalyzer tests.		
Particular hormones	Some hormones might be observed by medical testing and medical records.		
Cultures and subcultures (national, cross-national, and organizational)	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.		
Fatalism	Fatalism might be observed by coworkers through conversation. If the fatalism is derived from a particular religion or philosophy, then public membership or discussions about it on social networks might be observable.		
Business process requirements	Business process requirements should be public and therefore observable. To observe if the requirements increase risk, examination of the requirements for possible risk effects is necessary. Additionally, short and easy-to-fill-out surveys of workers asking for feedback about risks that might be caused by business process requirements would help an organization determine if the requirements are arduous or might have unintended, risk-increasing effects. System modeling is another way to better understand possible risk side effects of business process requirements.	•	
Variations over time in individuals and societies	To observe if a risk was previously evaluated at a particular level and the situation has gradually changed but the risk has not been re-evaluated, an organization might start by maintaining records of risk analyses. If a risk has not been fully re-evaluated for some time, it might fit into this category. Additional observable data could include comments, written information about risk observation, and even accidents related to the risk.		

These factors might be recognized or inferred through monitoring and surveillance methods (perhaps including, in some cases, linguistic analysis performed on samples of monitored electronic communications).

The above observation methods were identified without regard to possible legal constraints or boundaries, which must be considered. While employee monitoring can be subject to a variety of laws, the scope of this report permits us to highlight only a few of the pertinent ones. For example, identifying perceived risk threshold under some circumstances may be considered mental health testing, in which case the Americans with Disabilities Act (ADA), or the Rehabilitation Act for government employers, would apply and could limit testing and responses. Identifying philosophies such as fatalism may also employ some form of employee testing, which, as discussed above, may be subject to various regulations such as the ADA. Monitoring electronic

communications for indications of perceived risk threshold may be subject to the Electronic Communication Privacy Act's protections, requiring an employer to obtain consent or fall within another of the law's exceptions. Also, taking actions on an individual based on his or her perceived risk threshold could result in disparate treatment due to demographic factors, as discussed above. The ability of internet service providers (ISPs) to disclose information may be limited by laws such as the Electronic Communications Privacy Act and may also depend on factors such as ISPs' privacy policies and contracts.

The morality or legality of differential treatment based on gender, age, culture, or subculture is fraught with potential abuses. For example, Title VII of the Civil Rights Act of 1964 prohibits discrimination based on "race, color, religion, national origin or sex" [42 U.S.C.]. The Age Discrimination in Employment Act of 1967 prohibits discrimination in employment against those who are 40 or older [29 U.S.C.]. It is also of note that pre-employment inquiries into certain areas, including height and weight, credit rating, arrest, and conviction, may have a disparate effect on certain protected classes listed above. Often, any inquiries into these areas must have a specific business justification tailored to the job in question.

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 (although there is an exception for illegal drugs). Most states have drug testing laws, covering issues like communication of drug testing policy, types of tests, confidentiality standards, and independent review procedures. Considerations include whether or not the testing will take place for cause (e.g., after an incident) or at random, the type of drugs that will be tested for, the method of testing, as well as industry-specific concerns. For example, in *Creekmore v. Pomeroy IT Solutions, Inc*., an employer did not hire a candidate who had tested positive for phenobarbital.[10] However, phenobarbital was not on the state list of drugs that may be tested for, and the employer was found to have willfully violated the state drug law. In addition, some of the monitoring techniques above may implicate other laws such as the Genetic Information Nondiscrimination Act of 2008 (if an employer would test for genetic factors affecting risk), state laws regulating employer monitoring of off-duty behavior [Deschenaux 2009], and state law privacy protections, such as intrusion upon seclusion.[11] Monitoring regulations are very fact dependent and entail considerations such as private versus public institutions, the specific industry involved, and other factors.

Beyond legal and moral boundaries that affect monitoring for risk indicators, efficacy should also be considered. If a risk indicator is weakly correlated to increased risk, and monitoring for and mitigating responses to the risk indicator are expensive, an organization might decide against utilizing that indicator. Additional factors to consider include a return on investment (ROI) efficacy and the potential of (and separately, the likely costs of) the threat due to the risk as well as other spending priorities of the organization.

---

[10] *Creekmore v. Pomeroy IT Solutions*, 2010 U.S. Dist. LEXIS 97296 (D.C.N.D. Oklahoma, 2010); see Jackson Lewis, "Employer Testing of Applicant for Substance Not Approved by State Willful Violation of Oklahoma Law," Society for Human Resource Management, October 10, 2010 for a deeper discussion of this case.

[11] https://www.privacyassociation.org/media/presentations

7 Mitigation Strategies for Unintentional Insiders

We have reviewed literature and discussed a large number of UIT contributing factors (or potential factors), ranging from broad organizational factors, to human factors with a cognitive or psychosocial context, to other behavioral factors relating to risk tolerance, demographic and cultural influences, and even drug- and hormone-related contributing factors. Research is required to yield more definitive and actionable strategies, but we can speculate on mitigation strategies and approaches. As we have noted, 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 on usability of security tools to help overcome the most common underlying factors for UIT: user errors and negligence [Yayla 2011].

High-level organizational best practices objectives include the following:

- Review and improve management practices to align resources with tasks (avoid overworked staff and workload pressure).
- Improve data flow by enhancing communication and maintaining accurate procedures.
- Maintain productive work setting by minimizing distractions.
- Provide effective security practices (e.g., two-way authentication for access).
- Implement effective work planning and control to reduce job pressure, manage time factors, reduce task difficulty, avoid changes in routine, and reduce poor task planning and management practices.
- Maintain employee readiness (practices that reduce stress and anxiety, fatigue and boredom, and illness and injury and enhance awareness of drug side effects).
- Maintain staff values and attitudes that align with organizational mission and ethics.
- Implement security best practices throughout the organization, as defined by widely tested and implemented security norms in the industry. These best practices have been designed to help individuals and organizations perceive risks and mitigate normal human and organizational tendencies that can be problematic. Some of the security frameworks are designed to help ISMSs account for the organization's overall goals. Here is a sample list of best practices to consider:
  - NIST standards
  - standards for Information Security Management Systems, such as the Bell Labs Security Framework [McGee 2007] and ISO 27001-2 standards
  - the CERT Division's *Common Sense Guide to Mitigating Insider Threats* [Silowash 2012]
  - secure coding standards (for example, the CERT Division's Secure Coding Standards for Perl, C++, Java, etc.)
  - standards for secure systems engineering
  - standards for secure systems architecture

- standard systems (antivirus, IDS/IPS, firewalls, backup systems, SIEM systems, static and dynamic software code checkers, etc.) that identify errors and help identify wrongly taken risks, both to the individual and to the organization
- systems designed to minimize security risks, such as the CERT Division's Continuous Risk Management (CRM) and Software Risk Evaluation (SRE) methods. These methods assume multiple perspectives of risk in software development organizations and attempt to consolidate those perspectives to arrive at an organizational consensus. This philosophy was included in two early CERT risk analysis methods: the Information Security Evaluation (ISE) and the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) [Alberts 2002]. With OCTAVE, business, security, and IT staff are brought together to discuss risk from their perspectives and to create an organizational view of the current risk in relation to the organization's tolerance for risk.

Objectives for mitigations based on training and awareness may be briefly summarized as follows:

- Enhance awareness of insider threat and unintentional insider threat.
- Heighten motivation to be wary of insider threat risks.
- Recognizing phishing and other social media threat vectors.
- Instill process discipline to encourage following of policies and guidelines.
- Train continuously to maintain proper level of knowledge, skills, and ability.
- Conduct training and awareness on risk perception and cognitive biases that affect decision making.

Objectives for mitigations that employ human factors engineering are the following:

- Improve usability of security tools.
- Improve usability of software to reduce likelihood of system-induced human error.

To provide another line of defense against failures that occur despite these best efforts, one may identify a set of policies and countermeasures to guard against the impacts of such failures. For example, Milligan and Hutcheson [Milligan 2007] provide a detailed discussion of applications and associated security threats, with suggested countermeasures. An example, taken from email behavior and policies, is to address malware attacks in email by adopting and following a number of specific countermeasures and policies that encourage or enforce more stringent process discipline:

- Do not click on every link or open every attachment. Curiosity often overwhelms common sense.
- View unsolicited messages with suspicion. No click, no virus.
- Use anti-malware software.
- Connect to service providers with firewalls.
- Set options to prevent installation of executable software on mobile devices.
- Beware of unexpected connections and update confirmations.

Other countermeasures may be developed that focus on automated defense tools, such as developing software to better recognize threats in email messages, and DLP software to recognize

possible harmful sites, email practices, and other threats. Following are some examples of automated countermeasures:

- better software to recognize bogus emails
- DLP software to recognize possible harmful sites, email practices, and other threats
- firewalls
- antivirus software
- anti-malware software
- remote memory wipe for lost equipment

Table 4 summarizes countermeasure and mitigation strategies by relating appropriate countermeasures with UIT threat vectors.

Table 4: Mitigations and Countermeasures for Different UIT Threat Vectors

Threat Vector		UIT-HACK	DISC	PHYS	PORT
MITIGATION / COUNTERMEASURE	**Training to heighten awareness and reduce human error**	•	•	•	•
	Usability of software and tools to reduce human error	•	•		
	Management practices to reduce likelihood of human error	•	•	•	•
	Email safeguards (antiphishing, anti-malware)	•	•		
	Firewalls	•	•		
	Antivirus/anti-malware protection	•	•		•
	Data encryption on storage devices		•		•
	Password protection on storage devices		•		•
	Wireless and Bluetooth safeguards (disable, protect)				•
	Remote memory wipe for lost equipment				•

Finally, we discussed the need to create and adopt mitigation strategies tailored to specific risk-influencing factors. Following is a list of possible mitigations associated with different types of UIT risks and contributing factors:

- Address staff lack of awareness or inadequate risk perception or tolerance.
  - Use effective security training methods that help staff learn about security risks and how to combat the risks. These training methods must account for different learning styles. Also, the training should build on the individual's existing knowledge base and account

for human forgetfulness over time. High-fidelity simulations may be particularly effective for some learners. These education strategies could be organization-wide and could also be nationwide if cyber hygiene was considered a public health education necessity.

  - Enhance organizational awareness of risk and methods of influencing risk tolerance among staff members, accounting for tradeoffs such as creativity versus risk reduction.
  - Combat fatalism by effectively demonstrating impact. Rewards for cybersecurity training and passing tests might act as a reward that could combat fatalism.
  - Mitigations could be targeted to help correct for the human tendency to incorrectly assess risks, as noted in Schneier's list of five mistake tendencies [Schneier 2008]. Reminders about human tendencies to overestimate risks due to spectacular incidents might help people to measure their responses after spectacular incidents. Similarly, targeted reminders not to discount the probability of specific common (nonspectacular) risks might help. Mitigations might also include education on the topic of probability calculation or of historical accidents and their preceding risk estimations.
  - Develop or improve business processes to strengthen safeguards against undue risk taking, and take caution not to reward such behavior. Risk perception and awareness should be embedded within process requirements. Avoid making change too arduous to do, which could discourage people from making risk-reducing changes.

- Enhance support for employee health and well being.
  - Provide emotional health counseling and stress reduction through EAPs and workplace violence prevention programs.
  - Provide support for employee fatigue or sleepiness through EAP support and workplace stress load reduction (avoiding employee overwork).
  - Help reduce employee drug abuse problems, with health plans with free or low-cost assistance to combat drug and alcohol abuse, possibly also combined with legal workplace drug testing.
- Conduct red-teaming and unannounced exercises to test staff knowledge and behavior.
  - Organizations can intentionally seed their security systems with tests and traps that do not actually pose a danger to the organization. Those tests and traps can help detect risky behavior, offering an opportunity to educate users, identify high-risk users, and understand the exercise's effectiveness at instilling security awareness throughout the organization. For example, organizations can test users by sending out fake spam emails, which some users click on [Kumaraguru 2007]. Those tests can help the organization gauge the need for education and caution throughout the enterprise.
- Tailor strategies to risk takers.
  - Training approaches may concentrate on enhancing self-awareness of risk-comfort levels for risk-taking individuals. Awareness of one's biases and tendencies might help to avoid risk-taking behavior. Individualized counseling and instruction might be tailored to specific factors that are associated with high perceived risk threshold. High risk tolerance is associated with workplace maverickism, which in turn has linkages with entrepreneurship and ignoring the status quo (e.g., willingness to break rules to achieve results) [Gardiner 2012]. Because such traits might be valued in some organizational

contexts, it is important that training and awareness strategies avoid inappropriately stifling them.

- A mitigation strategy may use a framing approach to help modify risk behavior by (a) informing decision makers about the costs of their decision (e.g., deploying a technology to help produce better mental representations in technology-supported decision making) and (b) using positive framing rather than negative framing of problems to encourage less risky behavior and more balanced decisions.

8 Conclusions

As mentioned in the Introduction, a significant proportion of security professionals view insider threat as the greatest organizational risk and one that can accidentally jeopardize security through data leaks or similar errors [AlgoSec 2013]. The unintentional insider threat is not the same as the intentional insider threat—there are differences in motivations, indicators, and other factors that must be better understood to develop effective mitigations and countermeasures for UIT.

The range of possible cases is almost unlimited depending on the breadth of the definition of UIT. Depending on where one draws the line of responsibility, UIT could be expanded to include almost any unintended incident that exposes an organization to risk and involves an insider. That definition was too broad for the purposes of this study, so we narrowed it down to focus explicitly on cases captured with the definition provided in the Introduction.

The collection of UIT cases and subsequent analyses of the data will improve our understanding of similarities and differences among UIT incidents based on the model's features. The accumulation and analysis of incident statistics will also ultimately help stakeholders prioritize different types of UIT threats and associated mitigation strategies. This prioritization will then inform decisions about where and how to invest research and development resources to derive the greatest gains for research dollars spent.

Our preliminary study of the UIT problem has identified a number of contributing factors and mitigation strategies. The malicious insider threat and the UIT share many contributing factors that relate to broad areas of security practice, organizational processes, management practices, security culture, and other areas, but there are also significant differences. Human error plays a significant role in UIT. Countermeasures and mitigations to decrease UIT incidents should include strategies for improving and maintaining productive work environments, healthy security cultures, and human factors for increased usability of security tools to decrease the likelihood of human errors that lead to UIT incidents. As we have observed, most of the UIT cases that we collected featured data release (information disclosure), whether accidental or through negligence, without malware or other external actions.

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. While training and awareness programs can help raise awareness of accidental disclosure of sensitive information due to errors and lapses in judgment, what training can accomplish is limited. A comprehensive mitigation strategy should include new and more effective automated safeguards that seek to provide fail-safe measures when human factors or organizational systems fail to completely eliminate human errors associated with risk perception and other cognitive and decision processes.

There are resource tradeoffs to be considered: the time to make a safe culture versus maximizing output, maximizing creativity, speeding work, and maximizing worker satisfaction. Individuals often do not consciously consider risk, especially when facing high workloads and tight deadlines. We recommend that organizations analyzing risk avoidance strategies should consider proactive system designs versus reactive ones, negligence versus normal security, and usability.

Organizations must have a realistic discussion of risk avoidance that accounts for resource constraints, impediments caused by organizational structure, and rules, regulations, and their consequences.

9 Suggested Future Work

We recommend future research on UIT, with particular focus on contributing factors underlying accidental or mindless acts rather than technical problems that lead to UIT incidents, and on more effective mitigation strategies for these types of cases. As we see it, the most important contribution of this research would be to provide critical information to guide stakeholder investment in future research and development aimed at mitigating or preventing UIT. More detailed descriptions of recommended research and follow-on studies include the following:

- Continue to collect incident data to build up a large set of cases for the UIT database. These could be used for more extensive statistical analysis or investigation of best and worst practices, and to inform recommendations on where to devote resources toward mitigation or prevention options.
- Continue UIT research and data collection to help inform research and development stakeholders where to invest in new technology development, research, or practice; such analyses can help prioritize development of tools and mitigation strategies based on the most frequent threat vectors.
- Expand the CERT Division's *Common Sense Guide to Mitigating Insider Threats* [Silowash 2012] to address UIT.
- Focus new technology, research, and practice on the most frequent threat vectors or perhaps on another characteristic such as the number of records compromised or lost. Further data collection can characterize the relative frequencies of each of the UIT threat vectors, which can help prioritize the needed mitigation tools. The preliminary results of this study indicate that DISC is the most frequent threat vector.
- Continue research to inform development of more automated tools (e.g., more fail-safe security systems) to augment training and awareness programs, more effectively address the contributing factors of the UIT threat vectors, and proactively or retroactively respond to the threat (e.g., remotely erasing data on a lost smart phone). For example, as we have observed, most of the UIT cases that we collected featured data release, whether accidental or through negligence, without malware or other external actions. An area for further investigation is how to make data less available for employees to release, or at least how to put up some barriers.
- Consider organizations' responses to UIT. What are the best practices organizations should follow after suffering a UIT incident? In addition to utilizing the best mitigation and organizational response approaches that are currently available, reporting of incident data to a central clearinghouse would greatly facilitate collection and analysis of incident statistics, which would lead to better understanding of contributing factors and the effectiveness of countermeasures.
- Analyze the UIT case data in more detail, including investigation of additional sources of case data, as well as investigation to better reveal social engineering exploits and new mitigation options and to inform rough cost-benefit analyses for existing and new mitigation strategies.

- Conduct more in-depth research on factors that contribute to UIT. Many of the risk-related research results cited in this report were derived from experiments that did not directly address cybersecurity, much less relate to UIT research. Research should be conducted to help refine and validate the hypothesized application or extrapolation of these results to the cybersecurity and UIT domains.

Appendix A: Taxonomy of Negative Impacts

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 tasks fail, including intentional and unintentional actions by insiders and by outsiders. Figure 7 presents the taxonomy of negative impacts.

This taxonomy is an extension of the trust model in Castelfranchi and Falcone's book *Trust Theory* [Castelfranchi 2010]. It describes a typical delegation scenario involving four entities:

1. leader: a human who has a goal that requires completing a task
2. insider: a human to whom the leader may delegate parts of the task
3. outsider: a human who may interfere with the completion of the task
4. tool: a nonhuman agent to whom the leader may delegate parts of the task

The seven failure types appearing in the synoptic dichotomous taxonomic key[12] below include contrived but representative cases involving a leader Louise, an insider Irene, and an outsider Otto. Note that only the categories labeled with § are in the scope of this project.

1. Task fails due to direct malicious action by outsider → MALICIOUS OUTSIDER ATTACK
This is the usual information security attack: the familiar exploit of a vulnerability by an untrusted human outside the victim organization. (*Example:* Otto obtains the password for Irene's bank account and withdraws money illegally.)

1. Task does not fail due to direct malicious action by outsider: 2

> *2. Leader needs no help to execute task → EXISTENTIAL FAILURE*
> An existential failure occurs when a plan fails and there is no one to blame but oneself, or equivalently, the universe. There is no delegation involved, and the plan is overambitious or the capabilities of the leader are inadequate. If delegation were involved, this case would fall under human failure. (*Example:* Louise wants desperately to run a marathon in under 6 hours, but her body betrays her.)
>
> *2. Leader needs help to execute task: 3*

3. Leader delegates task to a tool: 4

3. Leader delegates task to an insider: 5

> *4. Task fails due to failure of tool → ENGINEERING FAILURE*
> The trust model includes delegating parts of the task to nonhuman agents, in other words, tools. In this view, a cowboy who says he *trusts* his six-shooter is not speaking metaphorically. Delegating in this way bets that the tool will behave as expected, but there is always the risk of inadequate performance. (*Example:* Presidential candidate Louise entrusts her speaking engagement to an amplifier that stops working at the highlight of her speech.)

[12] http://en.wikipedia.org/wiki/Single-access_key

5. Task fails due to malicious activity by insider → MALICIOUS INSIDER ATTACK
This is the usual insider attack, where an insider takes advantage of the trust invested in her to harm the leader. (*Example:* Louise hires Irene to move her infrastructure to the cloud, and Irene skims some intellectual property in the process.)

5. Task fails due to indirect activity by malicious outsider

5. Task fails due to nonmalicious poor performance of insider → HUMAN FAILURE §
Sometimes the nonmalicious, poor performance of the insider creates vulnerabilities that can be exploited by a malicious agent, either immediately or in the future. (*Example:* Irene accidentally misconfigures the organization's firewall, resulting in potential system compromise.) Other times, the nonmalicious, poor performance of the insider causes immediate harm, but without creating vulnerabilities that could be exploited in the future. (*Example:* Irene deletes an important report that took hours to write and for which there is no backup.)

> *6. Insider is deceived by outsider → SOCIAL ENGINEERING ATTACK §*
> A malicious outsider deceives a trusted insider into taking action that harms the organization. (*Example:* Otto uses a spear phishing attack to attract Irene to a malicious website.)
>
> *6. Insider is recruited by outsider → OUTSIDER COLLUSION ATTACK*
> In this variant on the usual insider threat, the malicious outsider persuades the insider to cause the leader's plan to fail. (*Example:* Otto convinces Irene to exfiltrate intellectual property.)

The taxonomy of negative impacts could be the basis of an instrument for determining in what way a task failed. The instrument might consist of multiple-choice questions that guide the user through the taxonomy tree to the correct conclusion about the failed task.

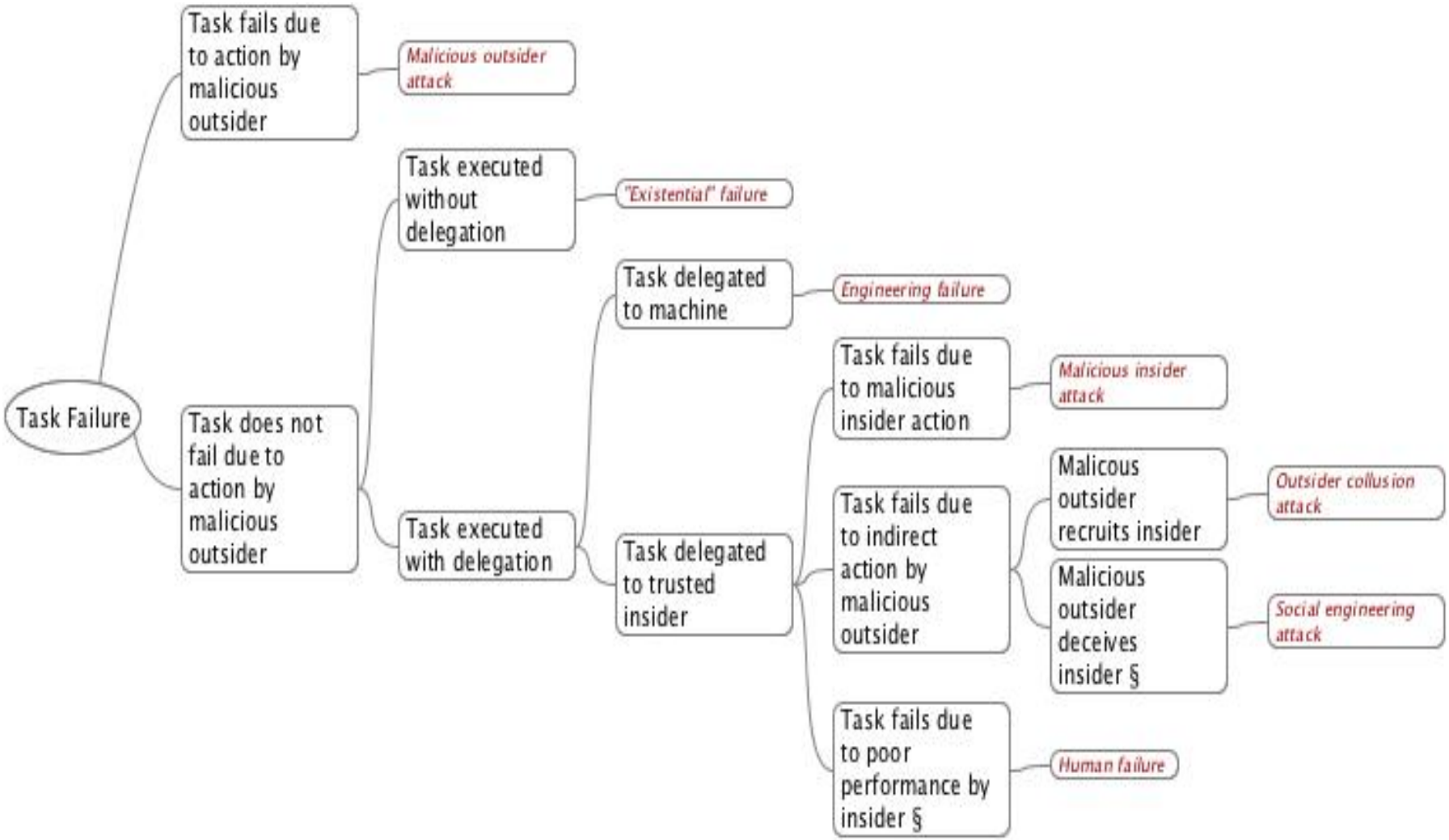

Figure 7: Taxonomy of Negative Impacts (Note that only the cases labeled with "§" are in scope for this project.)

Appendix B: UIT Incident Totals

UIThreatFeatures	Total	UIT Incident Numbers
Roles	41	
Insider	34	
Employee	18	453, 580, 598, 619, 620, 650, 743, 02, 04, 05, 08, 20, 21, 22, 23, 24, 25, 27
Job Classification	10	
ManagementTeam	5	09, 12, 16, 17, 26
Technical Staff	0	
NonTechnical Staff	5	744, 28, 29, 30, 31
Customer/User	2	11, 13
BusinessPartners	0	
Contractors	1	440
Outsourcee	3	591, 15, 17
Bad Actor	7	453, 591, 620, 743, 744, 13, 30
Cause	34	
Contributing Factors		
Data Flow		
Work Setting		
Work Planning/Control		
Employee Readiness		
Proximal Cause	34	
HACK	7	453, 591, 620, 743, 744, 13, 30
UnauthorizedAccess	1	13
ID theft/phishing	2	453, 620,
Rogue App/Malware	4	591, 743, 744, 30
Rogue USB or other device	0	
Website/Watering hole	0	
Insider negligence	27	
Information Leakage	27	
DISC - Disclosure	15	580, 598, 650, 02, 05, 06, 08, 09, 11, 12, 16, 26, 27, 28, 29
PHYS - Loss of non-electronic data	2	25, 31
PORT - Loss of electronic data	10	440, 619, 04, 15, 17, 20, 21, 22, 23, 24
Computer, Laptop, Mobile device	3	619, 22, 23
Storage Device	7	440, 04, 15, 17, 20, 21, 24
Other Portable Device	0	
Information Compromise	0	
Mode of data release	34	
System	22	
Internet - Online DB	6	580, 591, 598, 650, 05, 26
email	7	453, 620, 744, 02, 08, 12, 16,
Social Media	4	09, 27, 28, 29
Intranet/online DB	3	743, 06, 30
Mobile/Ubiquitous Computing	1	13
Cloud resources	1	11
Data Format	12	
Other, non-electronic	2	25, 31
Classification Level		
Electronic Data	10	440, 619, 04, 15, 17, 20, 21, 22, 23, 24
Encryption	2	Yes: 620, 17; No: Remainder
Classification Level		
Industry	34	
Businesses	10	
Financial/Banking	4	453, 619, 744, 06
Retail/e-commerce	1	650
Information technology	2	591, 09
Network/telecomms	2	11, 13
Manufacturing	1	743
Computer Hardware	1	743
Other products	0	
Government	20	
Civilian	17	580, 598, 620, 02, 04, 05, 08, 12, 17, 20, 21, 23, 25, 26, 29, 30, 31
Military	3	22, 27, 28
Healthcare	4	440, 15, 16, 24
Education	0	

Appendix C: UIT Features Glossary

UIThreatFeatures	**Features that characterize a UIT Threat**
Roles	Identity of individual(s) responsible for a UIT
Insider	Inside participants (Mandatory)
Employee	Organizational employees
Job Classification	Job classification of employee where known
ManagementTeam	Member of management or executive team
Technical Staff	Part of IT
NonTechnical Staff	Not part of IT
Customer/User	Customer with access to organizational data
BusinessPartners	Personnel from outside organizations that partner
Contractors	Personnel from outside organizations hired to work for organization
Outsourcee	Outside organization hired to perform specific task
Bad Actor	Outisder who initiates a HACK that is responded to by a UIT (Optional)
Cause	Threat vector and underlying reason for the incident
Contributing Factors	Contributing factors that led to the insider's action/inaction
Data Flow	Inadequate procedures/directions; poor communication
Work Setting	Distractions, insufficient resources, poor management systems, inadequate security practices
Work Planning/Control	Job pressure, time factors, task difficulty, change in routine, poor planning, and lack of skills
Employee Readiness	Inattention, stress/anxiety, fatigue/boredom, illness/injury, drugs, attitude, cognitive factors
Proximal Cause	Immediate factors that led to the incident
HACK	Electronic entry by an outside party, acquired through social engineering
UnauthorizedAccess	Access acquired without permission or obtained surreptitiously
ID theft/phishing	Using an email or other ruse to obtain login information
Rogue App/Malware	Software installed to perform the HACK
Rogue USB or other device	Use of a device to record or obtain identification and pass to BadActor
Website/Watering hole	Use of a website to obtain identification information
Insider negligence	Losses, corruption, or destruction caused directly by insider action or inaction
Information Leakage	Losses caused directly by insider action or inaction
DISC - Disclosure	Sensitive information posted publicly or sent via email, fax, or mail
PHYS - Loss of non-electronic data	Lost, discarded, or stolen non-electronic records
PORT - Loss of electronic data	Lost, discarded, or stolen non-electronic PDA, smart phone, portable memory device, CD, etc.
Computer, Laptop, Mobile device	Type of computing device lost
Storage Device	Memory stick or other storage device lost
Other Portable Device	Other portable devices
Information Compromise	Data corruption or destruction
Mode of data release	System and data format of a disclosure
System	System through which data is unintentionally released
Internet - Online DB	Data accessible through web-based access
email	Data sent directly or as an attachment via email
Social Media	Data appearing on Facebook, Twitter, etc.
Intranet/online DB	Data appearing inside the corporate netwrok
Mobile/Ubiquitous Computing	Data lost through mobile device or ubiquitous computing (e.g., wearable, vehicles)
Cloud resources	Data lost through cloud based *-as-a-service storage or processing
Data Format	Format through which data was lost
Other, non-electronic	Non-electronic
Classification Level	Option: Non-electronic may be classified
Electronic Data	PORT must result in loss of electronic data
Encryption	Electronic data may be encrypted
Classification Level	Electronic data may be classified
Industry	Sectors where incident occurred
Businesses	Commercial enterprises
Financial/Banking	Financial, including insurance, banking, brokerage, etc.
Retail/e-commerce	Retail or e-commerce enterprises
Information technology	Organizations producing software or making software services available
Network/telecomms	Organizations providing computer networking, cellular, or other phone services
Manufacturing	Manufacturing organizations
Computer Hardware	Computer hardware manufacturing
Other products	Other products
Government	Government at all levels and nationalities
Civilian	Civilian government and related
Military	Military, including civilian military agencies
Healthcare	Healthcare including medical care, research, etc.
Education	Organizations providing any level of educational services

Appendix D: UIT Incident Features

This section discusses the features of each case used for research in this Foundational Study. Each case is listed alongside the features of that case, as referenced in the Feature Model and used in the analysis of trends in UIT cases.

Source	Roles	Cause (UIT Classification)	Mode of Data Release	Encryption	Industry
MERIT ID 440, PRC (Jun 30, 2010)	Contractor	**PORT** (Storage Device)	Electronic Data	No	Healthcare
MERIT ID 453	Employee & Bad Actor	**HACK** (ID Theft/Phishing)	Email	No	Financial/Banking
MERIT ID 580, PRC (Jun 17, 2011)	Employee	**DISC**	Internet/Online DB	No	Government (Civilian)
MERIT ID 591	Outsourcee & Bad Actor	**HACK** (Rogue App/Malware)	Internet/Online DB	No	Information Technology
MERIT ID 598	Employee	**DISC**	Internet/Online DB	No	Government (Civilian)
MERIT ID 619	Employee	**PORT** (Laptop)	Electronic Data	No	Financial/Banking
MERIT ID 620	Employee & Bad Actor	**HACK** (ID Theft/Phishing)	Email	Yes	Government (Civilian)
MERIT ID 650	Employee	**DISC**	Internet/Online DB	No	Retail/Ecommerce
MERIT ID 743, PRC (Feb 22, 2013)	Employee & Bad Actor	**HACK** (Rogue App/Malware)	Intranet/Online DB	No	Manufacturing (Computer HW)
MERIT ID 744	Employee (NTS) & Bad Actor	**HACK** (Rogue App/Malware)	Email	No	Financial/Banking
Web 02	Employee	**DISC**	Email	No	Government (Civilian)
Web 04	Employee	**PORT** (Storage Device)	Electronic Data	No	Government (Civilian)
Web 05	Employee	**DISC**	Internet/Online DB	No	Government (Civilian)
Web 06, PRC (Jan 14, 2010)	Employee (Mgmt. Team)	**DISC**	Intranet/Online DB	No	Financial/Banking

Source	Roles	Cause (UIT Classification)	Mode of Data Release	Encryption	Industry
Web 08, PRC (Jan 27, 2010)	Employee	**DISC**	Email	No	Government (Civilian)
Web 09	Employee (Mgmt. Team)	**DISC**	Social Media	No	Information Technology
Web 11	Customers/Users	**DISC**	Cloud Resources	No	Network/ Telecomms
Web 12	Employee (Mgmt. Team)	**DISC**	Email	No	Government (Civilian)
Web 13	Customers/Users & Bad Actor	**HACK** (Unauthorized Access)	Mobile/Ubiq. Communication	No	Network/ Telecomms
Web 15	Outsourcee	**PORT** (Storage device)	Electronic Data	No	Healthcare (Government)
Web 16	Employee (Mgmt. Team)	**DISC**	Email	No	Healthcare
Web 17	Outsourcee	**PORT** (Storage device)	Electronic Data	Yes	Government (Civilian)
Web 20, PRC (May 28, 2010)	Employee	**PORT** (Storage device)	Electronic Data	Yes	Government (Civilian)
Web 21, PRC (May 22, 2006)	Employee	**PORT** (Storage device)	Electronic Data	No	Government (Civilian)
Web 22, PRC (May 22, 2006)	Employee	**PORT** (Computer)	Electronic Data	No	Government (Military)
Web 23	Employee	**PORT** (Computer)	Electronic Data	No	Government (Civilian)
Web 24, PRC (Apr 21, 2010)	Employee	**PORT** (Storage device)	Electronic Data	No	Healthcare
Web 25	Employee	**PHYS** (Documents)	Non-Electronic Data	Classified	Government (Civilian)
Web 26, PRC (Jan 30, 2013)	Employee (Mgmt. Team)	**DISC**	Internet/Online DB	No	Government (Civilian)
Web 27	Employee	**DISC**	Social Media	No	Government (Military)
Web 28	Employee (Non-Tech staff)	**DISC**	Social Media	No	Government (Military)
Web 29	Employee (Non-Tech staff)	**DISC**	Social Media	No	Government (Civilian)

Source	Roles	Cause (UIT Classification)	Mode of Data Release	Encryption	Industry
Web 30, PRC (Jun 13, 2006)	Employee (NTS) & Bad Actor	**HACK** (Rogue App/Malware)	Intranet/ Online DB	No	Government (Civilian)
WEB 31	Employee (Non-Tech staff)	**PHYS** (Cases of Cards)	Non-Electronic Data	Not Classified	Government (Civilian)

Bibliography

URLs are valid as of the publication date of this document.

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

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

[Akerstedt 1998]
Akerstedt, Torbjorn. "Shift Work and Disturbed Sleep/Wakefulness." *Occupational Medicine 53*, 2 (2000): (89-94).

[Alberts 2002]
Alberts, Christopher & Dorofee, Audrey. *Managing Information Security Risks: The OCTAVE Approach*. Addison-Wesley Professional, 2002.

[AlgoSec 2013]
AlgoSec. *The State of Network Security 2013: Attitudes and Opinions*. AlgoSec, Inc., 2013. http://www.algosec.com/resources/files/Specials/Survey%20files/State%20of%20Network%20Security%202013_Final%20Report.pdf

[Ajzen 1977]
Ajzen, I. & Fishbein, M. (1977). "Attitude-Behavior Relations: A Theoretical Analysis and Review of Empirical Research." *Psychological Bulletin 84*, 5 (September 1977): 888-918.

[Andrews 2011]
Andrews, D. H. & Jabbour, K. T. "Mitigating Cyber Friendly Fire: A Sub-Category of Cyber Mishaps." *High Frontier 7*, 3 (2011): 5-8.

[Au 2003]
Au, K.; Chan, F.; Wang, D.; & Vertinsky, I. "Mood in Foreign Exchange Trading: Cognitive Processes and Performance." *Organizational Behavior and Human Decision Processes 91*, 2 (2003): 322-338. http://www.sciencedirect.com/science/article/pii/S0749597802005101

[Barnabe 2010]
Barnabe, D.; Goodnight, J.; Hamilton, D.; Horowitz, B.; Neuman, C.; & Tarchalski, S. *Systems Security Engineering Final Technical Report* (SERC-2010-TR-005). http://www.sercuarc.org/uploads/files/SERC-2010-TR-005-Security-100823_01%281%29.pdf (2010).

[Bless 1990]
Bless, Herbert, et al. "Mood and Persuasion: A Cognitive Response Analysis." *Personality and Social Psychology Bulletin 16*, 2 (1990): 331-345.

[Boholm 2003]
Boholm, Asa. "The Cultural Nature of Risk: Can There Be an Anthropology of Uncertainty?" *Ethnos: Journal of Anthropology 68*, 2 (2003): 159-178.

[Booz Allen 2012]
Booz Allen. *The Accidental Insider Threat: Is Your Organization Ready?* September 25, 2012. http://www.boozallen.com/media/file/Accidental-Insider-Threat-Panel-Discussion-Transcript.pdf

[Broadbent 1982]
Broadbent, D. E.; Cooper, P. F.; et al. (1982). "The Cognitive Failures Questionnaire (CFQ) and Its Correlates." *The British Journal of Clinical Psychology 21,* 1 (1982):1-16.

[Brown 2013]
Brown C.; Watkins, A.; & Greitzer, F. L. "Predicting Insider Threat Risks through Linguistic Analysis of Electronic Communication," 1849-1858. *46th Hawaii International Conference on Systems Sciences (HICSS-46).* Wailea, Maui, HI, Jan. 2013. http://origin-www.computer.org/csdl/proceedings/hicss/2013/4892/00/4892b849.pdf

[Burke 2009]
Burke, Brian E., & Christiansen, Christian A. *Insider Risk Management: A Framework Approach to Internal Security.* IDC, 2009. http://www.rsa.com/solutions/business/insider_risk/wp/10388_219105.pdf

[Byrnes 1999]
Byrnes, James P.; Miller, David C.; & Schafer, William D. "Gender Differences in Risk Taking: A Meta-Analysis." *Psychological Bulletin 125*, 3 (1999): 367.

[Caldwell 2003a]
Caldwell, J.; Caldwell, J. L.; Brown, D.; Smythe, N.; Smith, J.; Mylar, J.; Mandichak, M.; & Schroeder, C. *The Effects of 37 Hours of Continuous Wakefulness on the Physiological Arousal, Cognitive Performance, Self-Reported Mood, and Simulator Flight Performance of F-117A Pilots.* U.S. Air Force Research Laboratory (AFRL-HE-BR-TR-2003-0086), 2003.

[Caldwell 2003b]
Caldwell, J. A. & Caldwell, J. L. *Fatigue in Aviation: A Guide to Staying Awake at the Stick.* Ashgate Publishing Company, 2003.

[Caldwell 2012]
Caldwell, J. A. "Crew Schedules, Sleep Deprivation, and Aviation Performance." *Current Directions in Psychological Science 21,* 2 (Apr. 2012): 85-89.

[Carver 2008]
Carver, Joseph M. *Love and Stockholm Syndrome: The Mystery of Loving an Abuser*. Gale Encyclopedia of Medicine, 2008.

[Castelfranchi 2010]
Castelfranchi, Cristiano & Falcone, Rino. *Trust Theory : A Socio-Cognitive and Computational Model*. John Wiley & Sons, 2010.

[Charette 1989]
Charette, Robert. *Software Engineering Risk Analysis and Management.* McGraw-Hill, 1989.

[Charette 1990]
Charette, Robert. *Applications Strategies for Risk Analysis.* McGraw-Hill, 1990.

[Cheyne 2006]
Cheyne, J. A.; Carriere, J. S. A.; & Smilek, D. (2006). "Absent-Mindedness: Lapses in Conscious Awareness and Everyday Cognitive Failures." *Consciousness and Cognition 15,* 3 (Sep. 2006): 578-592.

[Cisco 2008a]
Cisco Systems. *Data Leakage Worldwide: Common Risks and Mistakes Employees Make.* Cisco Systems, 2008. http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns895 /white_paper_c11-499060.pdf

[Cisco 2008b]
Cisco Systems. *Data Leakage Worldwide: The Effectiveness of Security Policies.* Cisco Systems, 2008. http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/ white_paper_c11-503131.html

[Clark 2009]
Clark, J.; Leblanc, S.; & Knight, S. 2009. "Hardware Trojan Horse Device Based on Unintended USB Channels," 1-8. *Third International Conference on Network and System Security* (*NSS '09).* Gold Coast, QLD, October 19-21, 2009. IEEE Computer Society, 2009.

[Clark 2011]
Clark, J.; Leblanc, S.; & Knight, S. "Risks Associated with USB Hardware Trojan Devices Used by Insiders," 201-208. *Systems Conference (SysCon*). Montreal, QC, April 4-7, 2011. IEEE International, 2011.

[Claycomb 2012]
Claycomb, William R.; Huth, Carly L.; Flynn, Lori; McIntire, David M.; & Lewellen, Todd B. "Chronological Examination of Insider Threat Sabotage: Preliminary Observations." *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications 3,* 4 (2012): 4-20. http://isyou.info/jowua/papers/jowua-v3n4-1.pdf

[Clifford 1986]
Clifford, James & Marcus, George E. *Writing Culture: The Poetics and Politics of Ethnography*. University of California Press, 1986.

[Co 1999]
Co, E. L.; Gregory, K. B.; Johnson, J. M.; & Rosekind, M. R. *Crew Factors in Flight Operations XI: A Survey of Fatigue Factors In Regional Airline Operations* (NASA Technical Memorandum No. 1999-208799). NASA Ames Research Center, 1999.

[Conzola 2001]
Conzola, V. C. & Wogalter, M. S. "A Communication-Human Information Processing (C-HIP) Approach to Warning Effectiveness in the Workplace." *Journal of Risk Research 4*, 4 (2001): 309-322.

[Courtenay 2000]
Courtenay, W. "Engendering Health: A Social Constructionist Examination of Men's Health Beliefs and Behaviors." *Psychology of Men & Masculinity 1,* 1 (Jan. 2000): 4-15.

[Creekmore 2010]
Creekmore v. Pomeroy IT Solutions. U.S. Dist. LEXIS 97296 (D.C.N.D. Oklahoma), 2010.

[Crosby 1979]
Crosby, J. V. & Parkinson, S. "A Dual Task Investigation of Pilot's Skill Level." *Ergonomics 22,* 12 (Dec. 1979): 1301-1313.

[Damos 1978]
Damos, D. "Residual Attention as a Predictor of Pilot Performance." *Human Factors: The Journal of the Human Factors and Ergonomics Society 20,* 4 (Aug. 1978): 435-440.

[Davies 1982]
Davies, D. R. & Parasuraman, R. *The Psychology of Vigilance*. Academic Press, 1982.

[de Fabrique 2007]
de Fabrique, Nathalie; Romano, Stephen J.; Vecchi, Gregory M.; & van Hasselt, Vincent B. "Understanding Stockholm Syndrome." *FBI Law Enforcement Bulletin (Law Enforcement Communication Unit) 76,* 7 (July 2007): 10-15.

[Dekker 2002]
Dekker, S. *The Field Guide to Human Error Investigations*. Ashgate, 2002.

[Deschenaux 2009]
Deschenaux, Joanne. *Dealing with Employees' Offensive Blogs and Facebook Postings.* Society for Human Resource Management. www.shrm.org/legalissues/stateandlocalresources/pages/offensiveblogsfacebookpostings.aspx (2009).

[Dill 2013]
Dill, Diana. *The Boiled Frog Syndrome: Or How You Can Behave Unethically Without Realizing It*. http://dianadill.org/doc/slippery_slope.pdf (2013).

[Dinges 1990]
Dinges, D. F. "The Nature of Subtle Fatigue Effects in Long-Haul Crews," 258-267. *Proceedings of the 43rd International Air Safety Seminar, Flight Safety Foundation*. Rome, Italy, November 19-22, 1990. Flight Safety Foundation, 1990.

[DoC 2013]
U.S. Department of Commerce. *National Institute of Standards and Technology Initiates Development of New Cybersecurity Framework.* Department of Commerce, 2013. http://www.commerce.gov/news/press-releases/2013/02/13/national-institute-standards-and-technology-initiates-development-new

[Douglas 1982]
Douglas, Mary & Wildavsky, Aron. *Risk and Culture*. University of California Press, 1982.

[Douglas 1992]
Douglas, Mary. *Risk and Blame*. Routledge, 1992.

[Dutt 2011]
Dutt, Varun; Ahn, Young-Suk; & Gonzalez, Cleotilde. "Cyber Situation Awareness: Modeling the Security Analyst in a Cyber-Attack Scenario Through Instance-Based Learning." *Data and Applications Security and Privacy XXV* (2011): 280-292.

[EEOC 2012]
Equal Employment Opportunity Commission. *Screening by Means of Pre-Employment Testing*. Society for Human Resource Management. January 10, 2012.

[EEOC 1982]
Equal Employment Opportunity Commission. *Policy Guidance on the Consideration of Arrest Records in Employment Decisions under Title VII of the Civil Rights Act of 1964, as amended, 42 U.S.C. §2000e et seq. (1982)*. http://www.eeoc.gov/policy/docs/arrest_records.html (1982).

[EEOC 1967]
Equal Employment Opportunity Commission. *Questions and Answers on EEOC Final Rule on Disparate Impact and "Reasonable Factors Other Than Age" Under the Age Discrimination in Employment Act of 1967*. http://www.eeoc.gov/laws/regulations/adea_rfoa_qa_final_rule.cfm (1967).

[Eisenecker 2000]
Eisenecker, U. W. & Czarnecki, K. *Generative Programming: Methods, Tools, and Applications*. Addison-Wesley, 2000.

[Endsley 1995]
Endsley, M. R. "A Taxonomy of Situation Awareness Errors," 287-292. *Human Factors in Aviation Operations: Proceedings of the 21st Conference of the European Association for Aviation Psychology*. Gower Technical, 1995.

[Endsley 1998]
Endsley, M. R. & Rodgers, M. D. "Distribution of Attention, Situation Awareness, and Workload in a Passive Air Traffic Control Task: Implications for Operational Errors and Automation." *Air Traffic Control Quarterly 6*, 1 (1998): 21-44.

[Endsley 1999]
Endsley, M. R. "Situation Awareness and Human Error: Design to Support Human Performance." *Proceedings of the High Consequence Systems Surety Conference.* Albuquerque, NM, 1999. http://www.satechnologies.com/Papers/pdf/Sandia99-safety.pdf

[Endsley 2000]
Endsley, M. R. *Situation Awareness Analysis and Measurement.* Lawrence Erlbaum Associates, Inc. (2000).

[esurance 2013]
esurance. "Why Women Pay Less for Car Insurance." http://www.esurance.com/car-insurance-info/women-pay-less-for-car-insurance (2013).

[Faulhaber 2011]
Faulhaber, Joe, et al. *Microsoft Security Intelligence Report, Volume 11*. Microsoft, 2011. www.microsoft.com/security/sir/archive/default.aspx

[Feldman 2001]
Feldman, A. "Philocetes Revisited. White Public Spaces and the Political Geography of Public Safety." *Social Text 19*, 3 (Fall 2001): 57-89.

[Fetterman 2009]
Fetterman, David M. *Ethnography: Step by Step*, 3rd edition. Sage, 2009.

[Figner 2011]
Figner, B., & Weber, E. "Who Takes Risks When and Why?" *Current Directions in Psychological Sciences 20*, 4 (Aug. 2011): 211-216.

[Finucane 2000]
Finucane, Melissa L., et al. "Gender, Race, and Perceived Risk: The 'White Male' Effect." *Health, Risk & Society 2*, 2 (2000): 159-172.

[Flynn 1994]
Flynn, J.; Slovic, P.; & Mertz, C. "Gender, Race, and Perception of Environmental Health Risks." *Risk Analysis 14*, 6 (December 1994): 1101-1108.

[Gardner 1989]
Gardner, G. & Gould, L. "Public Perceptions of the Risks and Benefits of Technology." *Risk Analysis 9*, 2 (June 1989): 225-242.

[Gander 1998]
Gander, P. H.; Gregory, K. B.; Connell, L. J.; Graeber, R. C.; Miller, D. L.; & Rosenkind, M. R. "Flight Crew Fatigue IV: Overnight Cargo Operations. *Aviation, Space & Environmental Medicine 69*, 9 (Sep. 1998): B26-B36.

[Gander 2002]
Gander, P.H.; Nesdale, A.; & Signal, L. *A Review of Locomotive Engineers' Extended Hours of Service.* 2002

[Gander 2008]
Gander, P. H.; van den Berg, M.; & Signal, L. "Sleep and Sleepiness of Fisherman on Rotating Shifts." *Chronobiology International 25*, 2&3, (Apr. 2008): 389-398.

[Gardiner 2012]
Gardiner, E. & Jackson., C. J. "Workplace Mavericks: How Personality and Risk-Taking Propensity Predicts Mavericksism." *British Journal of Psychology 103*, 4 (November 2012): 497-519.

[Geertz 1983]
Geertz, Clifford. *Local Knowledge*. Basic Books, 1983.

[Gonzalez 2005]
Gonzalez, Cleotilde; Dana, Jason; Koshino, Hideya; & Just, Marcel. "The Framing Effect and Risky Decisions: Examining Cognitive Functions with fMRI." *Journal of Economic Psychology 26*, 1 (Feb. 2005): 1-20.

[Gordon 2007]
Gordon, P. *Data Leakage - Threats and Mitigation.* SANS Institute, 2007. http://www.sans.org/reading_room/whitepapers/awareness/data-leakage-threats-mitigation_1931

[Graves 1995]
Graves, K. L. "Risky Sexual Behavior and Alcohol Use Among Young Adults: Results from a National Survey." *American Journal of Health Promotion 10*, 1 (Sep./Oct. 1995): 27-36.

[Greitzer 2010]
Greitzer, F. L.; Frincke, D. A.; & Zabriskie, M. (2010). "Social/Ethical Issues in Predictive Insider Threat Monitoring," 132-161. *Information Assurance and Security Ethics in Complex Systems: Interdisciplinary Perspectives.* Information Science Reference IGI Global, 2010.

[Greitzer 2012]
Greitzer F. L.; Kangas, L. J.; Noonan, C. F.; Dalton, A. C.; & Hohimer, R. E. "Identifying At-Risk Employees: A Behavioral Model for Predicting Potential Insider Threats," 2392-2401. *45th Hawaii International Conference on System Sciences (HICSS-45).* Wailea, Maui, HI, Jan. 2012. http://origin-www.computer.org/csdl/proceedings/hicss/2012/4525/00/4525c392.pdf

[Guttman 1995]
Guttman, B. & Roback, E. *The Introduction to Computer Security: The NIST Handbook* (Special Publication 800-12). http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf (1995).

[Hart 1990]
Hart, S. G. & Wickens, C. D. "Workload Assessment and Prediction," 257-300. *MANPRINT: An Emerging Technology. Advanced Concepts for Integrating People, Machines and Organizations.* Van Nostrand Reinhold, 1990.

[Hartel 1989]
Hartel, C. E.; Smith, K.; & Prince, C. "Defining Aircrew Coordination: Searching Mishaps for Meaning." *Proceedings of the Fifth International Symposium on Aviation Psychology*. Columbus, OH, April 17-20, 1989. University of Queensland, 1989.

[HealthyPeople.gov 2013]
HealthyPeople.gov. *Substance Abuse*. http://healthypeople.gov/2020/LHI/substanceAbuse.aspx (2013).

[Helton 2009]
Helton,W. S.; Kern, R. P.; & Walker, D. R. "Conscious Thought and the Sustained Attention to Response Task. *Consciousness and Cognition 18*, 3 (Sep. 2009): 600-607.

[Hoffmann 2011]
Hoffmann, H.-P. *Systems Engineering Best Practices with the Rational Solution for Systems and Software Engineering*. Available on https://www.ibm.com (2011).

[Ho 2009]
Ho, Karen. "Disciplining Investment Bankers, Disciplining the Economy: Wall Street's Institutional Culture of Crisis and the Downsizing of Corporate America." *American Anthropologist 111*, 2 (2009): 177-189.

[Hockey 1986]
Hockey, G. R. J. "Changes in Operator Efficiency as a Function of Environmental Stress, Fatigue, and Circadian Rhythms," 1-49. *Handbook of Perception and Human Performance, Volume II: Cognitive Processes and Performance.* Wiley, 1986.

[Holbrook 2012]
Holbrook, Emily. *Author Dan Gardner Talks Risk, Decisions and Psychology at the 2012 RIMS Canada Conference*. http://www.riskmanagementmonitor.com/author-dan-gardner-talks-risk-decisions-and-psychology-at-the-2012-rims-canada-conference/ (2012).

[Hollnagle 1993]
Hollnagle, E. *Human Reliability Analysis: Context and Control*. Academic Press, 1993.

[Hopko 2006]
Hopko, Derek R.; Lejuez, C. W.; Daughters, Stacey B.; Aklin, Will M.; Osborne, Amanda; Simmons, Burnetta L.; & Strong, David R. "Construct Validity of the Balloon Analogue Risk Task (BART): Relationship with MDMA Use by Inner-City Drug Users in Residential Treatment." *Journal of Psychopathology and Behavioral Assessment 28*, 2 (2006): 95-101.

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

[Huey 1993]
Huey, M. B. & Wickens, C. D. *Workload Transition: Implications for Individual and Team Performance*. National Academy Press, 1993.

[Hunt 2005]
Hunt, Melissa K.; Hopko, Derek R.; Bare, Robert; Lejuez, C. W.; & Robinson, E. V. "Construct Validity of the Balloon Analog Risk Task (BART) Associations with Psychopathy and Impulsivity." *Assessment 12*, 4 (2005): 416-428.

[Isen 1988]
Isen, Alice M.; Nygren, Thomas E.; & Ashby, F. Gregory. "Influence of Positive Affect on the Subjective Utility of Gains and Losses: It Is Just Not Worth the Risk." *Journal of Personality and Social Psychology 55*, 5 (1988): 710-717.

[ISO 2009]
ISO 27000 Directory. *An Introduction to ISO 27001, ISO 27002.....ISO 27008.* http://www.27000.org/ (2009).

[Ivers 2009]
Ivers, R.; Senserrick, T.; Boufous, S.; Stevenson, M.; Chen, H.-Y.; Woodward, M.; & Norton, R. "Novice Drivers' Risky Driving Behavior, Risk Perception, and Crash Risk: Findings from the DRIVE Study." *American Journal of Public Health 99*, 9 (Sep. 2009): 1638-1644.

[Jackson Lewis 2010]
Jackson Lewis Law Firm. "Employer Testing of Applicant for Substance Not Approved by State Willful Violation of Oklahoma Law." *Society for Human Resource Management.* http://www.shrm.org/LegalIssues/StateandLocalResources/Pages/EmployerTestingofApplicant.aspx (2010).

[James 1892]
James, W. Ch. XI, "The Stream of Consciousness." *Psychology*. Henry Holt and Co., 1892.

[Johnson 2011]
Johnson, A.; Dempsey, K.; Ross, R.; Gupta, S.; & Bailey, D. *Guide for Security-Focused Configuration Management of Information Systems* (NIST Special Publication 800-128). http://csrc.nist.gov/publications/nistpubs/800-128/sp800-128.pdf (2011).

[Jordan 1994]
Jordan, Ann T. "Organizational Culture: The Anthropological Approach." *Annals of Anthropological Practice 14*, 1 (1994):3-16.

[Jordan 2003]
Jordan, Ann T. *Business Anthropology*. Waveland Press Inc., 2003.

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

[Keil 2000]
Keil, M.; Wallace, L.; Turk, D.; Dixon-Randall, G.; & Nulden, U. "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 (Aug. 2000): 145-157.

[Klinger 1978]
Klinger, E. Ch. 8, "Modes of Normal Conscious Flow." *The Stream of Consciousness: Scientific Investigations into the Flow of Human Experience.* Plenum, 1978.

[Kryger 1994]
Kryger, M. H.; Roth, T.; & Carskadon, M. A. "Circadian Rhythms in Humans: An Overview." *Principles and Practice of Sleep Medicine*. Saunders, 1994.

[Kumaraguru 2007]
Kumaraguru, Ponnurangam, et al. "Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System," 905-914. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. San Jose, CA, April 28-May 3, 2007. ACM, 2007.

[Kvavilashvili 2004]
Kvavilashvili, L. & Mandler, G. "Out of One's Mind: A Study of Involuntary Semantic Memories." *Cognitive Psychology 48*, 1 (2004): 47-94.

[Larison 1999]
Larison, J. H. & Hoffman, J. "Drug Use, Workplace Accidents and Employee Turnover." *Journal of Drug Issues 29*, 2 (1999): 341-364.

[Lejuez 2002]
Lejuez, C. W.; Read, Jennifer P.; Kahler, Christopher W.; Richards, Jerry B.; Ramsey, Susan E.; Stuart, Gregory L.; Strong, David R.; & Brown, Richard A. "Evaluation of a Behavioral Measure of Risk Taking: The Balloon Analogue Risk Task (BART)." *Journal of Experimental Psychology Applied 8*, 2 (2002): 75-84.

[Lejuez 2003]
Lejuez, C. W.; Aklin, Will M.; Jones, Heather A.; Richards, Jerry B.; Strong, David R.; Kahler, Christopher W.; & Read, Jennifer P. "The Balloon Analogue Risk Task (BART) Differentiates Smokers and Nonsmokers." *Experimental and Clinical Psychopharmacology 11*, 1 (2003): 26.

[Lowrance 1976]
Lowrance, W.W. *Of Acceptable Risk: Science and the Determination of Safety.* Kaufmann, William Inc., 1976.

[Lupien 2007]
Lupien, S. J.; Maheu, F.; Tu, M.; Fiocco, A.; & Schramek, T. E. "The Effects of Stress and Stress Hormones on Human Cognition: Implications for the Field of Brain and Cognition." *Brain and Cognition 65*, 3 (Apr. 2007): 209–237.

[Lyon 2012]
Lyon, D. *Systems Engineering: Required for Cost-Effective Development of Secure Products*. http://www.sans.org/reading_room/whitepapers/physcial/systems-engineering-required-cost-effective-development-secure-products_34000 (2012).

[Madhavan 2012]
Madhavan, Poornima; Lacson, Frank C.; Gonzalez, Cleotilde; & Brennan, Patricia C. "The Role of Incentive Framing on Training and Transfer of Learning in a Visual Threat Detection Task." *Applied Cognitive Psychology 26*, 2 (Mar./Apr. 2012): 194-206.

[McCrae 2010]
McCrae, R. R. "The Place of the FFM in Personality Psychology." *Psychological Inquiry 21* (2010): 57-64.

[McCullah 2011]
McCullah, S. *Drug Abusers and Small Businesses*. Ezine Articles. http://ezinearticles.com/?Drug-Abusers-and-Small-Businesses&id=6516929 (August 24, 2011).

[McGee 2007]
McGee, Andrew R.; Bastry, Frank A.; Chandrashekhar, Uma; Vasireddy, S. Rao; & Flynn, Lori A. "Using the Bell Labs Security Framework to Enhance the ISO 17799/27001 Information Security Management System." *Bell Labs Technical Journal 12*, 3 (Nov. 2007): 39-54.

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

[Moons 2013]
Moons, W. G., et al. "Certainty Broadcasts Risk Preferences: Verbal and Nonverbal Cues to Risk-Taking." *Journal of Nonverbal Behavior 37*, 2 (June 2013): 79-89.

[Moore 2011]
Moore, A. P.; Hanley, M.; & Mundie, D. "A Pattern for Increased Monitoring for Intellectual Property Theft by Departing Insiders," 1-17. *Proceedings of the Conference on Pattern Languages of Programs.* Portland, OR, October 21-23, 2011. http://www.hillside.net/plop/2011/papers/D-6-Moore.pdf (2011).

[Moray 1982]
Moray, N. "Subjective Mental Workload." *Human Factors 24*, 1 (1982): 25-40.

[Moore 2013]
Moore, A. P.; McIntire, D.; Mundie, D.; & Zubrow, D. *Justification of a Pattern for Detecting Intellectual Property Theft by Departing Insiders* (CMU/SEI-2013-TN-013). Software Engineering Institute, Carnegie Mellon University, 2013. http://www.sei.cmu.edu/library/abstracts/reports/13tn013.cfm

[Nicholson 2005]
Nicholson, N.; Soane, E.; Fenton-O'Creevy, M.; & Willman, P. "Personality and Domain-Specific Risk Taking." *Journal of Risk Research 8*, 2 (2005): 157-176.

[Nickerson 1998]
Nickerson, R. S. "Confirmation Bias: A Ubiquitous Phenomenon in Many Guises." *Review of General Psychology 2*, 2 (June 1998): 175-220.
http://psy2.ucsd.edu/~mckenzie/nickersonConfirmationBias.pdf

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

[NIST 2010]
National Institute of Standards and Technology. *Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements* (NISTIR 7628). http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf (2010).

[Norman 1983]
Norman, D. A. "Design Rules Based on Analyses of Human Error." *Communications of the ACM 26*, 4 (April 1983): 254-258.

[Nygren 1996]
Nygren, T.; Isen, A.; Taylor, P.; & Dulin, J. "The Influence of Positive Affect on the Decision Rule in Risk Situations: Focus on Outcome (and Especially Avoidance of Loss) Rather Than Probability." *Organizational Behavior and Human Decision Processes 66*, 1 (Apr. 1996): 59-72.

[Pahnila 2007]
Pahnila et al. "Employees' Behavior Towards IS Security Policy Compliance." *Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS '07).* Waikoloa, Big Island, HI, January 3-6, 2007. IEEE Computer Society, 2007.

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

[Parmar 2013]
Parmar, Bimal. "Employee Negligence: The Most Overlooked Vulnerability." *Computer Fraud & Security 2013*, 3 (Mar. 2013): 1-20.

[Phule 2012]
Phule, P. "A Low Cost Hardware Trojan Horse Device Based on Unintended USB Channels and a Solution." *International Journal of Advanced Computer Research 2*, 7 (Dec. 2012): 114-118.

[PMI 2008]
Project Management Institute. *A Guide to the Project Management Body of Knowledge (PMBOK Guide), Fourth Edition*. Project Management Institute, 2008.

[Pond 2003]
Pond, D. J. & Leifheit, K. R. “End of an Error.” *Security Management 47*, 5 (2003): 113-117.

[Ponemon 2012]
Ponemon Institute. *Study on Patient Privacy & Data Security*. Ponemon Institute, 2012.

[Powell-Griner 1997]
Powell-Griner, Eve; Anderson, John E.; & Murphy, Wilmon. “State- and Sex-Specific Prevalence of Selected Characteristics—Behavioral Risk Factor Surveillance System, 1994 and 1995.” *MMWR. CDC Surveillance Summaries: Morbidity and Mortality Weekly Report. CDC Surveillance Summaries/Centers for Disease Control 46*, 3 (Aug. 1997): 1-29. http://www.cdc.gov/mmwr/preview/mmwrhtml/00048737.htm

[Prince 2000]
Prince, Carolyn & Salas, Eduardo. “Team Situation Awareness, Errors, and Crew Resource Management: Research Integration for Training Guidance.” *Situation Awareness Analysis and Measurement* (2000): 325-347.

[Privacy Rights Clearinghouse 2005]
Privacy Rights Clearinghouse. *Chronology of Data Breaches –Security Breaches 2005-Present.* http://www.privacyrights.org/data-breach (2005).

[pure-systems GmbH 2012]
pure systems. *pure::variants User’s Guide, Version 3.0 for pure::variants 3.0*. pure-systems GmbH, 2012.

[Reid 2005]
Reid, K. J. & Zee, P. C. Ch. 41, “Circadian Disorders of the Sleep-Wake Cycle.” *Principles and Practice of Sleep Medicine.* Elsevier Saunders, 2005.

[Reno 2011]
Reno, Joshua. “Beyond Risk: Emplacement and the Production of Environmental Evidence.” *American Ethnologists 38*, 3 (July 2011): 516-530.

[Rodgers 2000]
Rodgers, M. D.; Mogfor, R. H.; & Strauch, B. Ch. 4, “Post Hoc Assessment of Situation Awareness in Air Traffic Control Incidents and Major Aircraft Accidents.” *Situation Awareness Analysis and Measurement.* Lawrence Erlbaum Associates, 2000.

[Rosekind 1994]
Rosekind, M. R.; Weldon, K. J.; Co, E. L.; Miller, D. L.; Gregory, K. B.; Smith, R. M.; Johnson, J. M.; Gander, P. H.; & Lebacqz, J. V. “Fatigue in Operational Settings: Examples from the Aviation Environment.” *The Journal of the Human Factors and Ergonomics Society*, *36*, 2 (June 1994): 327-338.

[Rosenquist 2007]
Rosenquist, Matthew. *Measuring the Return on IT Security Investments*. http://communities.intel.com/community/openportit/blog/2007/12/11/whitepaper-measuring-the-return-on-it-security-investments (2007).

[Rouse 2009]
Rouse, M. *What Is ISO 27001?* http://searchsecurity.techtarget.co.uk/definition/ISO-27001 (September 2009).

[Salter 2011]
Salter, C.; Saydjari, O. S.; Schneier, B.; & Wallner, J. *Toward A Secure Engineering Methodology*. http://www.schneier.com/paper-secure-methodology.pdf (August 13, 2011).

[Saner 2009]
Saner, Lelyn D. & Gonzalez, Cleotilde. "Naturalistic Decision Framing in Computer Mediated Scientific Exploration." *Department of Social and Decision Sciences, Paper 81* (2009): 138-143.

[Schneier 2008]
Schneier, B. *The Psychology of Security*. http://www.schneier.com/essay-155.html (January 18, 2008).

[Schwartzman 1993]
Schwartzman, Helen B. *Ethnography in Organizations* (Volume 27). Sage Publications, Inc., 1993.

[Sedgwick 1888]
Sedgwick, William. "A Monograph of the Development of Peripatus Capensis." *Studies from the Biological Laboratory*. Johns Hopkins University, 1888.

[SEI 2013]
Software Engineering Institute. *CERT Secure Coding Standards*. https://www.securecoding.cert.org/confluence/display/seccode/CERT+Secure+Coding+Standards (2013).

[Seibert 1991]
Seibert, P. S. & Ellis, H. C. "Irrelevant Thoughts, Emotional Mood States and Cognitive Performance." *Memory & Cognition 19*, 5 (1991): 507–513.

[Shanteau 1993]
Shanteau, J. & Dino, G. A. Ch. 19, "Environmental Stressor Effects on Creativity and Decision Making." *Time Pressure and Stress in Human Judgment and Decision Making*. Plenum, 1993.

[Signal 2006]
Signal, L.; Ratieta, D.; & Gander, P. *Fatigue Management in the New Zealand Aviation Industry* (ATSB Research and Analysis Report, Aviation Safety Research Grant B2004/0048). Australian Transport Safety Bureau, 2006.

[Silowash 2012]
Silowash, George; Cappelli, Dawn; Moore, Andrew; Trzeciak, Randall; Shimeall, Timothy; & Flynn, Lori. *Common Sense Guide to Mitigating Insider Threats, 4th Edition* (CMU/SEI-2012-TR-012). Software Engineering Institute, Carnegie Mellon University, 2012. http://www.sei.cmu.edu/library/abstracts/reports/12tr012.cfm

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

[Sitkin 1995]
Sitkin, S. B. & Weingart, L. R. "Determinants of Risky Decision-Making Behaviour: A Test of the Mediating Role of Risk Perceptions and Propensity." *Academy of Management 38*, 6 (Dec. 1995): 1573-1592.

[Smallwood 2003]
Smallwood, J. M.; Baracaia, S. F.; Lowe, M.; & Obonsawin, M. "Task Unrelated Thought Whilst Encoding Information." *Consciousness and Cognition 12*, 3 (Sep. 2003): 452-484.

[Smallwood 2004]
Smallwood, J.; Davies, J. B.; Heim, D.; Finnigan, F.; Sudberry, M.; O'Connor, R.; & Obonsawin, M. "Task Engagement and Disengagement During Sustained Attention." *Consciousness and Cognition 13*, 4 (Dec. 2004): 657-690.

[Smallwood 2006]
Smallwood, J. & Schooler, J. W. "The Restless Mind." *Psychological Bulletin 132*, 6 (2006): 946-958.

[Smallwood 2007a]
Smallwood, J.; Fishman, D. J.; & Schooler, J. W. "Counting the Cost of an Absent Mind: Mind Wandering as an Underrecognized Influence on Educational Performance." *Psychonomic Bulletin & Review 14*, 2 (Apr. 2007): 230-236.

[Smallwood 2007b]
Smallwood, J.; McSpadden, M.; & Schooler, J. W. "The Lights Are on But No One's Home: Meta-Awareness and the Decoupling of Attention When the Mind Wanders." *Psychonomic Bulletin & Review 14*, 3 (June 2007): 527-533.

[Smallwood 2008]
Smallwood, J. M.; McSpadden, M.; & Schooler, J. W. "When Attention Matters: The Curious Incident of the Wandering Mind." *Memory & Cognition 36*, 6 (Sep. 2008): 1144-1150.

[Smith 1995]
Smith, K. & Hancock, P. A. "Situation Awareness Is Adaptive, Externally Directed Consciousness." *Human Factors 37*, 1 (1995): 137-148.

[Spindler 1999]
Spindler, George. "Three Categories of Cultural Knowledge Useful in Doing Cultural Therapy." *Anthropology & Education Quarterly 30*, 4 (Dec. 1999): 466-472.

[Stagman 2011]
Stagman, S.; Schwarz, S. W.; & Powers, D. *Adolescent Substance Use in the U.S.* http://www.nccp.org/publications/pub_1008.html (May 2011).

[Stokes 1994]
Stokes, A. & Kite, K. *Flight Stress*. Ashgate, 1994.

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

[Tickell 1990]
Tickell, C. "Human Effect of Climate Change: Excerpts from a Lecture Given to the Society on 26 March 1990." *The Geographical Journal 156*, 3 (Nov. 1990): 325-329.

[Trzeciak 2013]
Trzeciak, R. *Understanding and Protecting Against Multiple Faces of Insider Threat*. Elsevier, 2013.

[Verbrugge 1985]
Verbrugge, L. "Gender and Health: An Update on Hypotheses and Evidence." *Journal of Health and Social Behavior 26*, 3 (Sep. 1985): 156-182.

[Verizon 2013]
Verizon RISK Team. *2013 Data Breach Investigations Report.* Verizon, 2013. http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf

[Wachtel 1968]
Wachtel, P. L. "Anxiety, Attention and Coping with Threat." *Journal of Abnormal Psychology 73*, 2 (Apr. 1968): 137-143.

[Weber 2008]
Weber, E. J. Ch. 10, "Decisions under Uncertainty: Psychological, Economic, and Neuroeconomic Explanations of Risk Preference," 127-144. *Neuroeconomics: Decision Making and the Brain.* Elsevier Academic Press, 2008.

[Weller 2010]
Weller, J. L. "Do Individual Differences in Iowa Gambling Task Performance Predict Adaptive Decision Making for Risky Gains and Losses?" *Journal of Clinical and Experimental Neuropsychology 32*, 2 (Feb. 2010): 141-150.

[Weltman 1971]
Weltman, G.; Smith, J. E.; & Egstrom, G. H. "Perceptual Narrowing During Simulated Pressure-Chamber Exposure." *Human Factors 13*, 2 (Apr. 1971): 99-107.

[White 2008]
White, Tara L.; Lejuez, C. W.; & de Wit, Harriet. "Test-Retest Characteristics of the Balloon Analogue Risk Task (BART)." *Experimental and Clinical Psychopharmacology 16*, 6 (Dec. 2008): 565.

[Wogalter 1999]
Wogalter, M. S.; DeJoy, D. M.; & Laughery, K. R. *Warnings and Risk Communication*. CRC Press, 1999.

[Woods 1994]
Woods, D. D.; Johannesen, L. J.; Cook, R. I.; & Sarter, N. B. *Behind Human Error: Cognitive Systems, Computers, and Hindsight* (State of the Art Report CSERIAC 94-01). Wright-Patterson AFB, CSERIAC Program Office, 1994.

[Yayla 2011]
Yayla, A. "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).

[Yarkoni 2010]
Yarkoni, T. "Personality in 100,000 Words: A Large-Scale Analysis of Personality and Word Use Among Bloggers." *Journal of Research in Personality 44*, 3 (June 2010): 363-373.

[Yerkes 1908]
Yerkes R. M. & Dodson J. D. "The Relation of Strength of Stimulus to Rapidity of Habit-Formation." *Journal of Comparative Neurology and Psychology 18*, 5 (Nov. 1908): 459-482.

[Zakay 1993]
Zakay, D. "The Impact of Time Perception Processes on Decision Making Under Time Stress," 59-72. *Time Pressure and Stress in Human Judgment and Decision Making*. Plenum, 1993.

[Zald 2008]
Zald, D. H.; Cowan, R. L.; Riccardi, P.; Baldwin, R. M.; Ansari, M. S.; Li, R.; Shelby, E. S.; Smith, C. E.; McHugo, M.; & Kessler, R. M. "Midbrain Dopamine Receptor Availability Is Inversely Associated with Novelty-Seeking Traits in Humans." *The Journal of Neuroscience 28*, 53 (Dec. 2008): 14372-14378.

[Zaloom 2004]
Zaloom, Catelin. "The Production Life of Risk." *Cultural Anthropology 19*, 3 (Aug. 2004): 365-391.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	August 2013	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Unintentional Insider Threats: A Foundational Study	FA8721-05-C-0003

6. AUTHOR(S)

The CERT Insider Threat Team

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2013-TN-022

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFLCMC/PZE/Hanscom Enterprise Acquisition Division 20 Schilling Circle Building 1305 Hanscom AFB, MA 01731-2116	n/a

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

This report examines the problem of unintentional insider threat (UIT) by developing an operational definition of UIT, 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 presenting initial thinking 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.

14. SUBJECT TERMS	15. NUMBER OF PAGES
unintentional, insider, threat, human, factors, decision, risk, mitigation	91

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL