

2018

# The Impact of Mindfulness on Non-Malicious Spillage within Images on Social Networking Sites

Angela D. Landress

Nova Southeastern University, [landress@mynsu.nova.edu](mailto:landress@mynsu.nova.edu)

This document is a product of extensive research conducted at the Nova Southeastern University [College of Engineering and Computing](#). For more information on research and degree programs at the NSU College of Engineering and Computing, please click [here](#).

Follow this and additional works at: [https://nsuworks.nova.edu/gscis\\_etd](https://nsuworks.nova.edu/gscis_etd)

 Part of the [Computer Sciences Commons](#)

## Share Feedback About This Item

---

### NSUWorks Citation

Angela D. Landress. 2018. *The Impact of Mindfulness on Non-Malicious Spillage within Images on Social Networking Sites*. Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, College of Engineering and Computing. (1050) [https://nsuworks.nova.edu/gscis\\_etd/1050](https://nsuworks.nova.edu/gscis_etd/1050).

This Dissertation is brought to you by the College of Engineering and Computing at NSUWorks. It has been accepted for inclusion in CEC Theses and Dissertations by an authorized administrator of NSUWorks. For more information, please contact [nsuworks@nova.edu](mailto:nsuworks@nova.edu).

The Impact of Mindfulness on Non-Malicious Spillage within  
Images on Social Networking Sites

by

Angela D. Landress

A dissertation submitted in partial fulfillment of the  
requirements for the degree of Doctor of Philosophy in  
Information Systems

College of Engineering and Computing  
Nova Southeastern University

We hereby certify that this dissertation, submitted by Angela Landress, conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.



James L. Parrish, Ph.D.  
Chairperson of Dissertation Committee

5/29/2018  
Date



James Smith, Ph.D.  
Dissertation Committee Member

5/24/2018  
Date



Bennet Hammer, Ph.D.  
Dissertation Committee Member

5/29/2018  
Date

Approved:



Yong X. Tao, Ph.D., P.E., FASME  
Dean, College of Engineering and Computing

5/29/2018  
Date

College of Engineering and Computing  
Nova Southeastern University

2018

An Abstract of a Dissertation Submitted to Nova Southeastern University in  
Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

## The Impact of Mindfulness on Non-Malicious Spillage within Images on Social Networking Sites

by  
Angela D. Landress  
May 2018

Insider threat by employees in organizations is a problematic issue in today's fast-paced, internet-driven society. Gone are the days when securing the perimeter of one's network protected their business. Security threats are now mobile, and employees have the ability to share sensitive business data with hundreds of people instantaneously from mobile devices. While prior research has addressed social networking topics such as trust in relation to information systems, the use of social networking sites, social networking security, and social networking sharing, there is a lack of research in the mindfulness of users who spill sensitive data contained within images posted on social networking sites (SNS). The author seeks to provide an understanding of how non-malicious spillage through images relates to the mindfulness of employees, who are also deemed insiders. Specifically, it explores the relationships between the following variables: mindfulness, proprietary information spillage, and spillage of personally identifiable information (PII). A quasi-experimental study was designed, which was correlational in nature. Individuals were the unit of analysis. A sample population of business managers with SNS accounts were studied. A series of video vignettes were used to measure mindfulness. Surveys were used as a tool to collect and analyze data. There was a positive correlation between non-malicious spillage of sensitive business, both personally identifiable information and proprietary data, and a lack of mindfulness.

## Acknowledgements

This dissertation signals the end of a long journey. It represents my life's work. It is part of a legacy that will be left behind one day when I am no longer here. However, I did not accomplish it alone. I've ridden on the backs of all the women in the field who have come before me, who have made sacrifices, who have been treated less than, who surpassed the doubt, fear, harassment, and belittlement and molded those impediments into stepping stones to female empowerment, equality and success. These women made it possible for future women, like me, to be competitive in this field, because in the face of adversity, they never gave up. To these historical figures who carved a path for me to walk upon, thank you.

I have so much love and gratitude in my heart for my parents, Darell and Norma Landress, who sacrificed the very little they had to give me what I needed. They provided in all the ways that count. They were a constant support and my biggest cheerleaders. A huge thanks goes to my son, Ethan, who involuntarily gave up years of his mom's full attention, so that I could be better and do better. He never complained. He always believed in me, even during times when I was doubtful and frustrated. He, more than anyone else, knew I could finish what I started. He offered continuous encouragement, and his admiration of my hard work pushed me to succeed, in hopes that one day he will succeed in something that requires great effort.

I'm appreciative for my dissertation adviser, Dr. James Parrish, who lent his time and talents in ensuring I had the tools I needed to succeed. I'm also thankful for the rest of my dissertation committee, Dr. Hammer Bennett and Dr. James Smith, who took time away from their busy schedules and families to review and critique my work, ensuring it met the rigorous expectations of the University.

I am absolutely indebted to my tribe of close friends who pushed me when I needed it. Audra Cozort, Lani LaGuardia, Tonya Miller, I couldn't have done this without you. Thank you for lending an ear or a shoulder, for babysitting, and dogsitting, and all the many things you've done to make my busy life possible.

Lastly, even when I doubted it, God was with me step by step, day by day. He has shown his favor to me, a daughter of the King, and I am truly blessed to receive his grace. He taught me to be humble, yet fiercely forthright, when required. He kept me focused and steadfast, even when I was tempted to waiver. He led me to this place of closure, and I am forever grateful.

"Nevertheless, she persisted." Thank you, Senate Majority Leader Mitch McConnell, for reminding me of the profound effect a persistent woman can have on the world. I'm inspired to be that woman. After all, giving up was never really an option.

## Table of Contents

Acknowledgements .....	iv
Table of Contents.....	1
List of Tables .....	2
Chapter 1 Introduction .....	4
Background.....	4
Problem Statement .....	7
Research Question and Hypotheses .....	11
Relevance and Significance .....	11
Barriers and Issues .....	17
Definition of Key Terms .....	18
Summary.....	18
Chapter 2 Review of the Literature.....	20
Introduction.....	20
Chapter 3 Methodology.....	32
Overview of Research Methodology .....	32
Research Questions and Hypotheses.....	32
Data Necessary to Answer the Research Questions.....	33
Instrument Development.....	35
Population and Sample.....	36
Chapter 4 Results .....	47
Introduction.....	47
Chapter 5 Conclusions .....	68
Introduction.....	68
Appendix A.....	76
Appendix B.....	80
Appendix C.....	82
Appendix D.....	83
<b>References .....</b>	<b>90</b>

## List of Tables

### Tables

Table 1: Definition of Terms.....	18
Table 2: Gender, Age, Geographic Region of Responders.....	49
Table 3: Social Networking Experience.....	52
Table 4: Descriptive Statistics Group 1 – PII Spillage Detection.....	52
Table 5: Descriptive Statistics Group 2 – Proprietary Information Spillage Detection....	53
Table 6: Descriptive Statistics Group 3 – Control Group.....	53
Table 7: Box’s Test of Equality of Covariance Matrices – Group 1.....	54
Table 8: Classification Results – Group 1 – PII Spillage Detection.....	55
Table 9: Standard Canonical Discriminant Function Coefficients – Group 1.....	56
Table 10: Structure Matrix – Group 1.....	57
Table 11: Box’s Test of Equality of Covariance Matrices – Group 2 .....	58
Table 12: Classification Results – Group 2 – Proprietary Data Spillage Detection.....	58
Table 13: Standard Canonical Discriminant Function Coefficients – Group 2.....	59
Table 14: Structure Matrix – Group 2.....	60
Table 15: Box’s Test of Equality of Covariance Matrices – Group 3 Control Group.....	60
Table 16: Classification Results – Group 3 – Control Group.....	61
Table 17: Standard Canonical Discriminant Function Coefficients – Group 3.....	62
Table 18: Structure Matrix – Group 3.....	62
Table 19: Likert Scale.....	64
Table 20: Final Mindfulness Score.....	79

## List of Figures

### Figures

Figure 1: Verizon 2016 Data Breach Investigation Report, Percent of Data Breaches Per Asset Category.....	5
Figure 2: Verizon 2016 Data Breach Investigation Report, Delta of Number of Vulnerabilities Opened Each Week and Number Closed.....	6
Figure 3: Conceptual Framework .....	10
Figure 4: Data Analysis Example .....	39
Figure 10: Video Vignette 1 .....	41
Figure 11: Video Vignette 2 .....	42
Figure 12: Video Vignette 3 (Control Group) .....	42
Figure 5: Variables.....	50
Figure 13: Social Networking Security Training.....	70



## Chapter 1 Introduction

### **Background**

There are many motives for people to post to social networking sites. A study conducted by a marketing platform in 2015 stated that posts that contain photos attract 120% more engagement (likes and comments) than posts without photos (Comcowich, 2015). The fast-paced growth of social networking is related to security issues in businesses. It is very easy for employees to upload photos to SNS because of their increasing popularity in pop culture (Ho, Maigo, & Aimeur, 2009). By risking their personal privacy and security by uploading posts on social networks (Wall, 2013), users are also potentially put their employer's information at risk. To improve efficiencies and their ability to deliver services, nearly all organizations exchange information electronically, rather than physically. Because of this shift, businesses must refocus energy and resources from protecting their networks from outsiders to protecting their network from insiders, or employees (Wall, 2013). Most insider incidents, whether malicious or not, are more damaging to companies than outsider incidents (CERT, 2011). Since the rise of social networking in everyday life, including work life, mitigating spillage by educating employees is paramount.

Exacerbating this issue for employers, photos of people at work can be shared on SNS like Facebook, which makes them more accessible for people to view. (Besmer & Lipford, 2010). In addition, new social networking programs, like Instagram, Pinterest and Snap Chat, have been growing in numbers of active users. SNS have been able to retain tens of millions of mobile users by making it easy to share photographs (Smith, 2012).

Brumfield (2016) wrote in Verizon’s 2016 Data Breach Investigations Report that cyber attacks occurred in a variety of organizations spanning across 82 countries. One of the fastest growing threat action types is “social.” Within that threat action type, the “person” category trended upward due to humans falling victim to social cyber threats. The “user device” category trended upward due to desktops falling prey to malware, which is directly associated with human social behavior. Verizon cites this as a loss of integrity based on human behavior. The graphic below displays the information within the report.

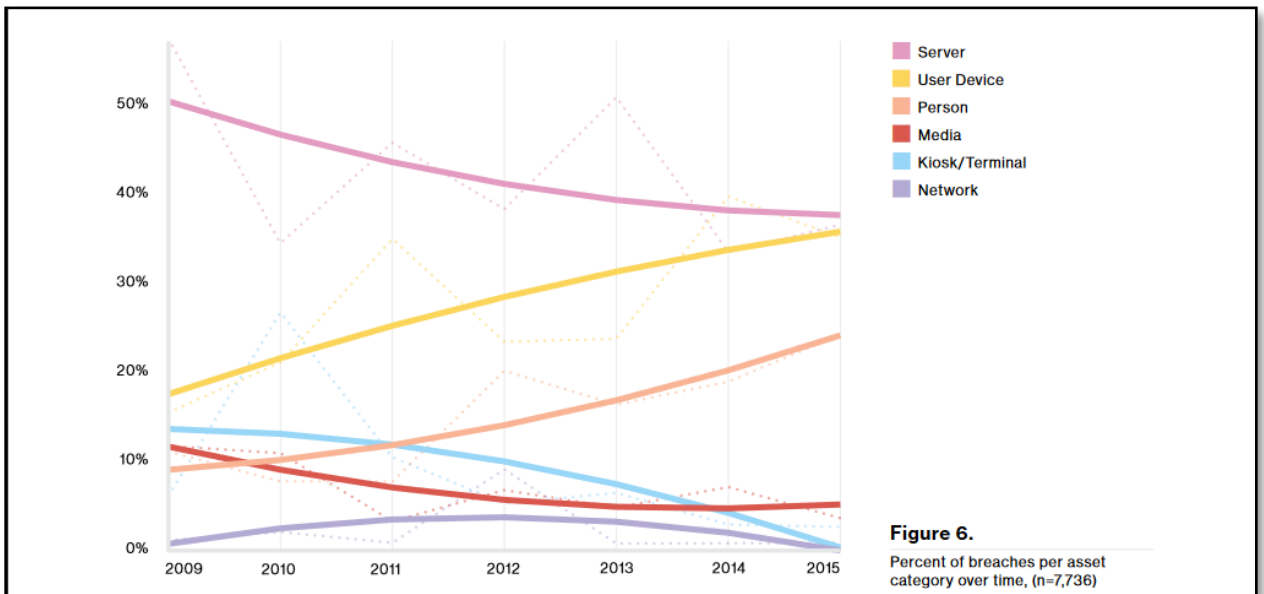


Figure 1: Verizon 2016 Data Breach Investigation Report, Percent of Data Breaches Per Asset Category. Adapted from “Verizon’s 2016 data breach investigations report finds cybercriminals are exploiting human nature,” by J. Brumfield, 2016. Retrieved from Verizon: <http://www.verizon.com/about/news.verizons-2016-data-breach-investigations-report-findscybercriminals-are-exploiting-human-0>.

The report also revealed that in cyber attacks where there is a human element, attackers are quicker than ever at compromising their victims. The following graphic shows how many vulnerabilities are being opened, and how many are being closed. As you analyze the graph, notice that vulnerabilities are being discovered at an alarming rate

compared to the number being closed.

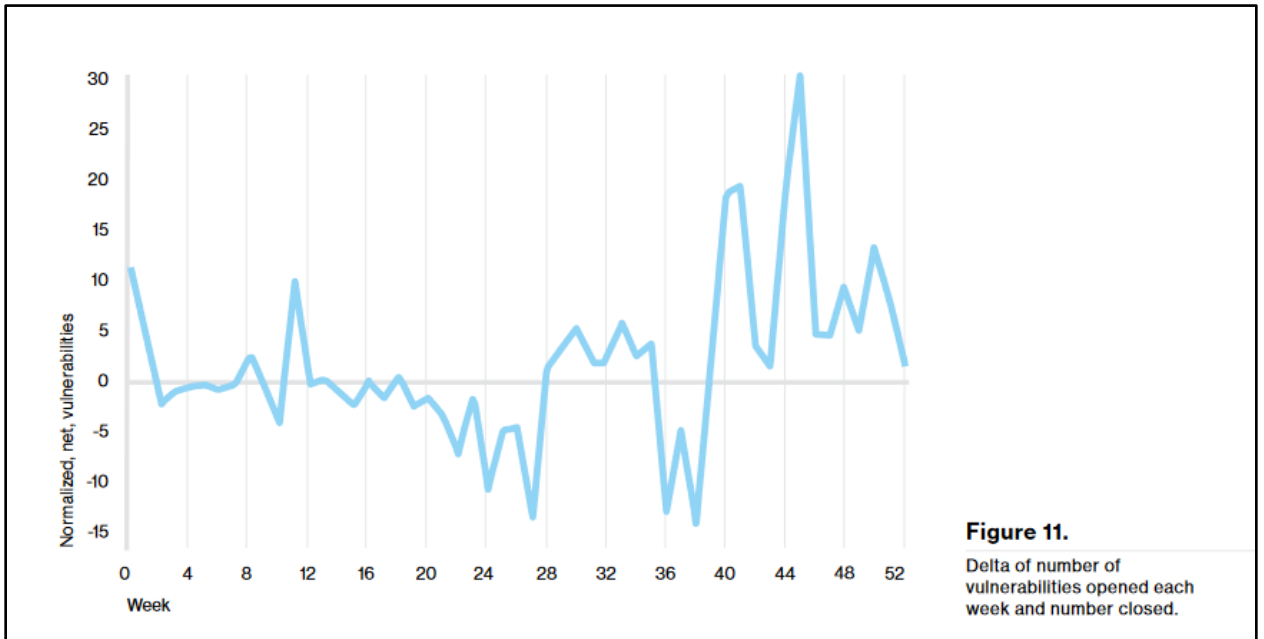


Figure 2: Verizon 2016 Data Breach Investigation Report, Delta of Number of Vulnerabilities Opened Each Week and Number Closed. Adapted from “Verizon’s 2016 data breach investigations report finds cybercriminals are exploiting human nature,” by J. Brumfield, 2016. Retrieved from Verizon: <http://www.verizon.com/about/news.verizons-2016-data-breach-investigations-report-finds-cybercriminals-are-exploiting-human-0>.

Organizations should be distressed when putting together the pieces of what this report revealed, which is that human and social elements are trending upward dramatically, people are falling victim to cyber attacks more often, and computer vulnerabilities are being opened at a faster rate than they can be closed. The Verizon report also points out that since social attacks are what affect organizations most, there is a clear lack of communication between the organization and its employees (Brumfield, 2016). Employees must understand the consequences of cyber breaches and spillages to their organization’s livelihood, because employees are the first line of defense against these attacks, even when they are non-malicious.

Many non-malicious spillages are related to a lack of mindfulness and could

potentially be mitigated through policy updates and training methods (Hoy & Milne, 2010). In a 2010 study, it was noted that 77% of users neglected to read a SNS privacy policy before signing up on a site. (Hoy & Milne, 2010).

This paper is a quasi-experimental survey study designed to investigate the relationships amongst mindfulness and non-malicious spillage of sensitive business information. A sample population of managers with SNS accounts were studied. Purposive sampling was conducted to narrow the population appropriately. Video vignettes were used to measure user mindfulness of managers who notice social networking spillage, and nominal response surveys were used to take a self-assessment survey, as well as to make correlations between mindfulness and non-malicious spillage. There are approximately 23.8 million employed individuals in the United States, according to the U.S. Bureau of Labor Statistics. In 2016, 16% of those employed were managers (Hamel & Zanini, 2016). 350 participants from various organizations in the United States were randomly selected to be the sample population. Business managers cost the United States more than \$3 trillion per year, according to the Harvard Business Review (Hamel & Zanini, 2016). Businesses hire managers to enforce rules and policies upon employees to protect their investment. They also rely on managers to maintain a budget and provide performance reviews. It is reasonable to assume that these activities require a certain level of advanced education. For this reason, managers in the United States with social networking accounts were selected to be the sample population for this study.

### **Problem Statement**

While prior research has addressed social networking topics such as trust in relation to information systems, the use of social networking sites, social networking security, and

social networking sharing, there is a lack of research in non-malicious spillage of sensitive data contained within photos posted on social networking sites (SNS) by employees.

Malicious insiders account for few of these incidents. Almost all insider threat incidents can be traced back to employee oversight, or mindlessness, and bad business practices (Gordon, 2007). 80% of large U.S. companies have reported that they use an instant messaging application, which are capable of file transferring. Understanding how to properly use email and avoid non-malicious spillage is important as well. For example, employees should be trained on encryption techniques to protect their employer's sensitive information (Gordon, 2007). These can also be effectively translated to employees through social networking policies. Phone cameras are also noted by Gordon (2007) as threat vectors, due to the ease of taking photos on built-in phone cameras and transmitting them electronically.

Potential new attack vectors, like phone cameras, coupled with a lack of mindfulness of social networking site users, can provide even more danger for businesses who are coping with protecting their business investments in an online centric society. Because SNS have platforms like messaging, the same phishing threats and exploits that can happen by email can happen through SNS as well (Bicen & Cavus, 2011).

A lack of mindfulness is a major contributing factor to non-malicious data spillage, and so it is also an integral part of implementing security policies within organizations to combat security threats (Parrish & Kuhn, 2008). Securing one's information gets harder as technology gets farther reaching and more complex. This dilemma puts more responsibility to safeguard IT systems and data on the user. While security policies help, they are not one size fits all. As new technologies are introduced, old security policies become outdated and

not useful. It is postulated by Parrish & Kuhn (2008) that by connecting organizational mindfulness with an organization's security policy, the security posture of the organization can be increased.

### **Dissertation Goal**

The goal of this study is to understand the relationship between mindfulness factors related to non-malicious online spillage associated with posting photos that have sensitive business information contained within to social networking sites. To support this goal, a conceptual framework has been established.

### **Conceptual Framework**

The framework of this study is based on factors of the construct of mindfulness and users of SNS who make decisions to post, and it measures the ability of a manager to detect spillage in the event the employee is not mindful in their posting decisions. The manager's experience in social networking and access to information are covariates of detecting whether he or she is able to detect proprietary information spillage and personally identifiable information (PII) spillage. The graphic below describes the relationships.

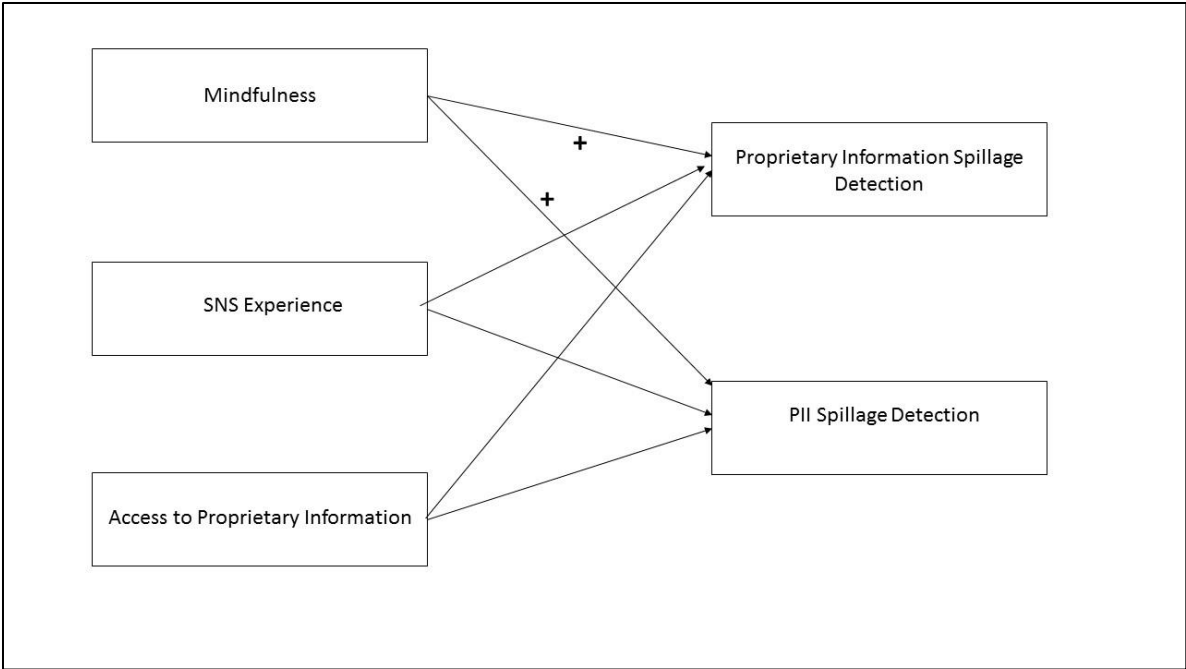


Figure 3: Conceptual Framework

## **Research Question and Hypotheses**

The following research questions were posed during the course of this study.

RQ1: Is an individual's level of mindfulness positively associated with recognizing non-malicious spillage within photos on a SNS?

The proposed research question determined the effectiveness of an individual's level of mindfulness to detect non-malicious spillage in photos in social networking sites. If an employee practices mindfulness by being resilient in their SNS activity, they were able to avoid spillage altogether. The concept of mindfulness, and what it constitutes, is explored. Spillage and leakage are differentiated as constructs in the field of Information Systems (IS), as the two are often confused and the focus for this study is on spillage. Malicious spillage is distinguished from non-malicious spillage and the connection is made between detecting non-malicious spillage and mindfulness.

Based on the given information, the overarching hypothesis in this study follows.

H1: There is a positive correlation between mindfulness and the detection of non-malicious spillage on social networking sites.

More specifically, the author hypothesized the following:

H1a: There is a positive correlation between mindfulness and the detection of proprietary information spillage within photos on social networking sites.

H1b: There is a positive correlation between mindfulness and the detection of personally identifiable information (PII) spillage within photos on social networking sites.

## **Relevance and Significance**

This study advances current research by relating mindfulness to non-malicious



online spillage, which has the potential to cost businesses a significant amount of money, and potentially, their reputation. Most insider threat incidents can be traced back to employee oversight, or mindlessness, and bad business practices (Gordon, 2007). A lack of mindfulness and user security awareness is far-reaching. Strano (2008) found that Facebook users are interested in choosing photos to post that would either classify as attractive or be perceived as having fun or being humorous. When combining a lack of mindfulness with ego-driven social motives like popularity gain, non-malicious spillage becomes an inevitable threat to businesses.

A study conducted by Zeadally, S., Yu, B., Jeong, D. H., & Liang, L. (2012). cited a Verizon study that revealed 48% of data breaches in 2009 were conducted by insiders of organizations. As of 2012, more than 66 million status updates were posted on Facebook every day. Not only is personal information readily available, but these sites can also be used as platforms to recruit insiders. A follow up Verizon study in 2016 revealed that these numbers are rising at an alarming rate. As a matter of fact, the human and social elements of attacks are trending upward, and attackers are compromising victims at a faster pace than ever before (Brumfield, 2016). Organizations are finding it difficult to put the right policies in place that balance confidentiality with sharing information. The authors recommend that designing automated tools that are innovative and cost effective is the best solution to mitigate the insider threat. They also explore other techniques used to combat insider threats; however, the authors state that many implementations have failed because of the complexity of the human factors involved (Zeadally et al, 2012).

Defense in Depth is a global trend that many organizations implement to detect and prevent external threats. In fact, this has become a \$35 billion industry (Gordon, 2007).

While security solutions are good at setting up an external perimeter to deter attacks and secure internal networks, they do not sufficiently protect against insider threats. Insider threats can cause organizations great damages, not only financially, but also to their reputation. In 2011, a study was conducted with the Secret Service and the CERT program at Carnegie Mellon Institute that stated that insider attacks account for 52% of data breaches, and attacks are becoming more sophisticated and increasing in numbers (Gordon, 2007). Malicious insiders only account for 1% of these incidents. 99% of insider threat incidents can be traced back to employee oversight, or mindlessness, and bad business practices. Most insider attacks are handled internally because there is insufficient evidence to prosecute and it's very difficult to identify the insider. This makes it hard to understand the real impact of attacks on organizations. Only 19% of attacks are detected with automated tools; the rest are detected manually. The key is to detect proactively, before an event happens, using mitigation activities like increased user training and improved security awareness (Gordon, 2007).

Curran & Lennon (2011) proposed five core beliefs that influence a person's attitude toward social networking. A person's attitude toward social networking has a direct correlation to posting trends and the use of SNS. They cite them as "ease of use, usefulness, enjoyment, social influence, and drama." It was found that enjoyment was the strongest factor affecting attitude and directly correlates to one's intention to use a social networking site. Also, social influence bears a positive effect on one's attitude; however, it represents a negative influence on one's intentions. When conducting the cost-benefit analysis, enjoyment and social influence act as positive motivators to post on social networking sites (French & Read, 2013).

Non-malicious spillage is of growing concern to business and security practitioners. Employees who post personal data on social networks can unintentionally expose themselves to elements that can damage their reputation and their employer's reputation (Bishop & Gates, 2008). Maasberg, M., Warren, J., & Beebe, N. L. (2015) study cites the business insider as partially responsible for the increase in computer crimes and information system security concerns, and technical controls are blamed in giving a false sense of security to practitioners, because the problems are easy to identify and solve. The Dark Triad theory is proposed, which is composed of Machiavellianism, narcissism, and psychopathy, as a possible explanation of insider threat. The Theory of Planned Behavior and Capability Means Opportunity model is used to investigate the motive and trigger of the offender. These theories are combined to explain the motive behind insider threat attacks. In doing so, the authors describe unintentional insider threat as a significant problem for businesses as well. Unintentional insider threat occurs when an insider causes harm inadvertently, or by accident. This is usually due to ignorance, user error, inexperience, gullibility, or purposeful but non-malicious abuses of known security policies, which makes intent hard to identify.

Employee training is also a major threat to businesses combating insider threats and spillage (Parrish & San Nicolas-Roca, 2012). While many organizations have emphasized information systems security training to combat organizational breaches, the author argues that it is ineffective due to flaws in the training and implementation of it in the workplace. Data breaches are expensive for organizations, citing an average cost of \$6.75 million USD for companies in 2009 alone (Parrish & San Nicolas-Roca, 2012). Many of these breaches have been associated with employee behavior that lacks a mindfulness of security policy.

If mindfulness were integrated into information systems security training, it can be argued that these security breaches can be avoided. Mindlessness is described as a state of reduced attention, whereas mindfulness is described as paying attention to the things that are new in our environment. Being present and more aware is imperative to avoiding security breaches. There are three ways in which mindfulness relate to information systems security training. The first way is for personnel to be engaged in security training. The second way is for personnel to be aware of situations that are hotbeds of security policy violation. The third way is to establish a culture of mindfulness within the organization (Parrish & San Nicolas-Roca, 2012).

Machine learning techniques have also been proposed to attempt to predict insider threats as a method of mitigation and avoidance (Schultz, 2002). While practitioners have advanced their security methods of implementing perimeter security, intrusion detection, encryption, and access control, insider threats and attacks seem to be on the rise. Most insider attacks are attributed to misuse, psychological make-up, criminology and computer competency. Schultz's (2002) study focuses on a lack of computer competency. He lists potential attack indicators as deliberate markers, meaningful errors, preparatory behavior, correlated usage patterns, verbal behavior, and personality traits. By inserting these factors into an equation, or algorithm, that can be plugged into a machine learning tool, he argues that he has presented a novel approach to predicting and detecting insider attacks. However, while the idea is innovative, it is not proven, and validation testing still needs to be completed. Additionally, while machine learning techniques may assist in predicting insider threats, they do nothing to mitigate a non-malicious spillage caused by an insider.

Zeadally et al (2012) explores various computer-based methods to mitigate threats

to the network. Intrusion detection systems are known in industry as being useful for detecting external threats. One system-call-based approach describes recording all system activities, as opposed to logs that record only some of the events. Because system call monitoring systems couple tightly with the operating system, attackers almost always leave behind evidence of the intrusion. Certain data-centric approaches are appropriate when a large amount of data analysis is required to achieve real-time threat detection. Non-negative matrix factorization (Zeadally et al, 2012) minimizes the amount of data that needs to be processed. Honeypot approaches have also been proposed, which is usually deployed in a DMZ and attracts attackers to it, which provides organizations with an early warning of malicious attackers. However, these actions will not always prevent a non-malicious insider threat attack. Insiders have privileged access to computer systems and data (Bishop & Gates, 2008). Security approaches like honeypots and algorithms do not protect against insiders.

It is obvious that computer-based approaches are not able to mitigate against spillage caused by non-malicious insider threats. It is worth investigating what causes an insider to non-maliciously disclose sensitive or confidential business information when posting photos on SNS.

This research seeks to answer questions that will undoubtedly add significance to the under-explored topic of social networking security. Does non-malicious spillage through photos relate to a lack of mindfulness on the part of the user? Does the insider have access to proprietary or sensitive information? A potential topic for future research could investigate an employee's understanding of the social networking security policies in their organizations that are designed to protect their employer's proprietary information.

## **Barriers and Issues**

Many researchers and practitioners have spent countless dollars and energy focusing on implementing computer-based solutions to mitigate insider threat when the problem is a “people and processes” problem, and not a technology problem. The problem is so costly, that if it were a technology problem, a solution would have already been proposed and implemented (Schultz, 2002). Unfortunately, the hardest problems are usually created in the hearts and minds of people. Once the relationships between the variables are identified, researchers and practitioners can get closer to alleviating the threat. This paper seeks to assist in reaching that goal, but the author appreciates the barriers understanding the human mind presents. To achieve overcoming that obstacle, this research study examined the variables that are measurable by conducting an experiment through a series of video vignettes and surveys that will answer the research questions.

## **Assumptions**

The following assumptions were made within the context of this study. Managers are educated people hired by employers to enforce security policy and have the ability to detect activity that is harmful to the organizations they work for. Managers and employees have access to proprietary data of their employer. Employees who post sensitive information within photos on social networking sites have no ill intention and are acting in a non-malicious fashion, even when the spillage has a negative impact on the organization employing them.

## Definition of Key Terms

Table 1.0

### *Definition of Key Terms*

Term	Definition
Insider threat	Insider threats are threats by insiders who are legitimate users of the IT system, or a trusted entity that is given the power to violate one or more rules in a given security policy' (Bishop & Gates, 2008).
Mindfulness	“High sensitivity of perception and high flexibility of behavior to respond to diverse, changing stimuli (p.505).” (Levinthal and Rerup, 2006)
Non-malicious spillage	Non-malicious spillage is confidential business data that is shared by a valued employee who cuts corners to fulfill job duties that may be otherwise hard to complete, but puts the organization at risk by ignoring, or side-stepping, security policies (Wall, 2011).
Personally identifiable information (PII)	PII is a type of information spillage that contains personal information about a person that, if released to the public, could be damaging to that person.
Proprietary information	Proprietary information is business information or data that has potential to be harmful to the business if shared.
Social networking sites (SNS)	A social networking site is a social platform that emphasizes on facilitating social relations among social network users who share similar interests, activities, backgrounds, or real-life connections.

## Summary

The purpose of chapter one was to introduce the study, present the research problem, and discuss the dissertation goal. While prior research has addressed social networking topics such as trust in relation to information systems, the use of social networking sites,

social networking security, and social networking sharing, there is a lack of research in non-malicious spillage of sensitive data contained within images posted on social networking sites (SNS) by employees. This research is significant, because it is so far reaching. Non-malicious spillage has the potential to cost businesses significant amounts of money directly and indirectly by damaging their reputation. 99% of insider threat incidents can be traced back to employee oversight, or mindlessness, and bad business practices (Gordon, 2007).

The main goal of this study is to understand the relationship between mindfulness factors related to non-malicious spillage associated with posting photos that have sensitive business information contained within to social networking sites. The author sought to show positive correlation between mindfulness and the detection of non-malicious spillage on social networking sites. More specifically, the author sought to show a positive correlation between mindfulness and the detection of proprietary information spillage within photos on social networking sites; as well as a positive correlation between mindfulness and the detection of personally identifiable information (PII) spillage within photos on social networking sites.



## Chapter 2 Review of the Literature

### **Introduction**

In this chapter, a literature review examined the various proposed causes of non-malicious spillage due to exposing sensitive business data within images posted to SNS. Specifically, the review provides an overview of what social networking sites are, defines the business insider, information disclosure and security research in information systems, including a better understanding of the differences between spillage and leakage, non-malicious spillage and malicious spillage, and mindfulness and awareness. These factors play an important role in an individual's decision to post to an SNS.

### *Social Networking*

A SNS is a social platform that emphasizes on facilitating social relations among social network users who share similar interests, activities, backgrounds, or real-life connections. One can locate friends, interact with people, and formulate discussions online (Bohnert & Ross, 2010). Kane et al, 2009 described SNS as a way of communicating by using a collaborative tool to accelerate group formation and influence. Users of SNS, which are online communities, have the ability to share their online profile, see others' profiles, and see the relationships of their SNS friends in relation to other people in their friend groups (Bicen & Cavus, 2011).

Facebook is one of the most commonly used and preferred SNS today (Bicen & Cavus, 2011). The usage of social networking sites is increasing daily. Over 1 billion users spend at least 9.7 billion minutes per day on social networking platform (Wilson, Gosling, & Graham, 2012). Users share billions of pieces of content daily, including photos

(Wilson, Gosling, & Graham, 2012). Photos allow social network users to create an online identity to communicate to their respective communities (Hum et al, 2011).

Social network users are known to share a wide range of personal information online. Recent studies show that Facebook social networkers upload over 2 billion photos per month, collectively (Wright, K. B., Abendschein, B., Wombacher, K., O'Connor, M., Hoffman, M., Dempsey, M., ... & Shelton, A. (2014).). The social construct of social networking effectively tries to explain why people post to social networking sites, and it also serves to warn business owners to approach social networking with caution (Zingale, 2013). Social networking is a form of artificial intelligence that the creators can use to identify patterns and acquire knowledge, and it has invaded society. Facebook alone has over 1 billion users. Social networking is limited on two phenomenological fronts: when taken out of context, a person's imagination objectifies conditions and doesn't have the ability to understand the whole; and that language itself doesn't allow for wholeness of expression in a situation. Zingale (2013) postulated that there is a gap between understanding and imagination that social networking cannot account for. In order to make a circumstance understandable, people leave things out to interpret what part of the circumstance is meaningful. This forces people to assert the parts that are left out. They define "telling" as being able to tell the difference between facts. Sometimes telling is also sharing. When people share something, they must realize that they only have part of the whole. This requires imagination, which comes into play when one is forced to figure out what to do in the face of the unknown. Connaturality is a way in which humans know and love each other through feelings. This form of sharing is challenging in social networking, because it infers that for someone to share in an experience, or appreciate it fully, they must

be present in a way that it can be taken as a whole. While social networks cannot replace physically being present to experience a situation, it is recommended that business managers cautiously move ahead with social networking by understanding the benefits while appreciating its limitations (Zingale, 2013).

### *Information Disclosure*

In Palledegara and Warren's (2016) study on spillage, it is concluded that even though organizations have social network policies in place, unauthorized disclosure by insiders in research is still not given its due attention. They state that recent incidents where insiders of organizations have spilled confidential information on social networking sites are increasing in frequency. Organizations do not understand how to address this issue in an effective manner. Molok, N. N. A., Ahmad, A., & Chang, S. (2010) defines information disclosure as "a breach of confidentiality of information, through disclosure of internal information into the public domain or to unauthorized third parties." Palledegara & Warren (2016) determined that social networking sites are the most challenging forums to mitigate unauthorized information disclosure, and that accidental disclosure, or spillage, has the ability to cause just as much damage as malicious information disclosure. Social networking is more challenging than spillage in other mediums because of its ease of use, simplicity, and compatibility, therefore, the risk exposure is higher. Once exposed, the information is available to the public instantaneously, due to the network effect, as opposed to information that is transferred during a face-to-face conversation (Molok et al, 2010). Additionally, information can be retrieved at a later date through search engines like Google. Palledegara and Warren's (2016) study also pointed out that organizations have failed to describe to employees what

is deemed confidential, and have failed to guide them properly on tactics to avoid unauthorized disclosure on social networking sites. Also, current organizational policies are not sufficient to address the complexities of social networking site usage.

Historically, organizations have focused on the criminal outsider. However, businesses have seen negative impacts due to employees spilling their proprietary data trending. Wall's (2011) study explores the concept of redefining insider threat due to the frequency and consequence of organizational spillage. The author equates non-malicious spillage with the well-meaning insider. In other words, this is a valued employee who cuts corners to fulfill job duties that may be otherwise hard to complete, but puts the organization at risk by ignoring, or side-stepping, security policies. Frequently, these actions act as a prequel for other, larger attacks, by hackers. Wall (2011) states that this distinction between malicious and non-malicious insiders is important for current and future research and has two implications. First, developing the insider profile is imperative to create an appropriate response. Also, practitioners should begin to take a more risk-based approach to insiders, rather than the typical perimeter hardening approach. To further granulate, the author categorizes non-malicious risk groups. Underminers make a habit of undermining security systems to get better, or more privileged, access. The over-ambitious non-malicious insider knowingly takes risks because they feel following security practices or policies takes too long and is too bureaucratic. They hope they can achieve organizational goals faster and better if they ignore security, hence introducing risk. The socially-engineered insider is usually a lower paid employee in a more entry position that has a public-facing job. These insiders are victims of social engineering attacks by malicious outsiders. They give data away in good

faith, hoping to serve their customer. The final category Wall (2011) identifies is the data leaker, or whistleblower. This person leaks confidential data to the public through social networking means in the spirit of ethics. Unlike the socially engineered, this person acts against the organization. The author proposes they are not malicious, because they are acting in the best interest of the public.

Schultz (2002) proposes a new framework to understand and predict insider threats and attacks. While practitioners have advanced their security methods of implementing perimeter security, intrusion detection, encryption, and access control, insider threats and attacks seem to be on the rise. They present various definitions of insider attacks by prior researchers, but state that applying the definitions is an arduous task in practice. They review common myths and misconceptions about insider attacks, trace them back to their origination, and argue them with validated research. By inserting factors of misuse, whether non-malicious or purposeful, into an equation, or algorithm, that can be plugged into a machine learning tool, the authors argue that they have presented a novel approach to predicting and detecting insider attacks. They admit that while the idea is innovative, it is not proven, and the next step for future research is to perform validation testing.

Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005) also postulates that the problem of insider threat has created a paradigm where information systems security is regarded as a people issue or an organizational issue. Insider threats pose more of a risk than external threats, and unfortunately, firewalls and intrusion detection systems are not effective in mitigating this risk. Misuse of information systems by insiders is defined as delinquent workplace behavior. To protect themselves from insider threats, practitioners should pose sanctions, reinforce access control, and implement

training and awareness programs.

Magklaras & Furnell (2005) describe the threat to confidentiality, integrity, and availability (CIA) due to insider attacks, and the authors call out insider threat as a separate category of threats. They identify user sophistication as a main component of computer crimes, which makes the insider threat especially dangerous, since they are legitimate users of the IT system(s). They present a way to automate the level of sophistication a user may have and define what an insider is and explain why IT systems are so vulnerable. They have potential to control air traffic, telecommunications, defense, energy, and water distribution systems, to name a few. Parker's (1998) general model of computer crime attacks is used as a baseline and built upon it. Neumann (1999) is cited as another author who called out sophistication as an insider threat factor. They differentiated advanced users from ordinary users and novice users. A one-to-one association was created between an application program and a score of the level of system knowledge. The more knowledge required by the insider, the greater the score. The results of the experiment conducted indicated that the proposed model can classify end user sophistication. It's possible that this model can be used in future research as a component of a wider insider threat prediction model. It can also be used to measure the productivity of IT systems users.

By integrating photo taking into every day mobile devices usage, the process of sharing personal photographs on SNS is commonplace, and since photographs do not just commemorate special occasions, but record the everyday lives and social interactions of the social network user (Stefanone et al, 2011), this can pose a significant challenge for employers. Because SNS users expose themselves to greater risks by sharing photos (Fogel & Nehmad, 2009), by default employees now open themselves up to malicious

attacks and cybercrime if their employees are not properly educated on social network usage. Social networkers develop a sense of false trust on SNS without realizing the dangers imposed on them (Sledgianowski & Kuliwat, 2009).

### *Mindfulness*

Mindfulness is a concept that originated from the ancient religion and traditions of Buddhism (Kang & Wittingham, 2010). One of the most recognized researcher of mindfulness and mindlessness, Ellen J. Langer of Harvard University, recently stated that people are taught as young children that all of their traits and characteristics should follow a normal distribution, and when they do not, they are not meeting society's expectation of them. (Langer, 2016). This is a mindless view. She quotes Shakespeare who said, "Things are neither good nor bad but thinking makes it so." Children who are evaluated and do not fall within the normal distribution of grades are judged harshly, regardless of how caring the teachers and parents are. Langer (2016) describes these judgements as encouraging the mindless society view of rote memorization learning, and eventually these views become our own. By labeling people into fixed characteristics and skillsets, we ignore that not everyone behaves the same in all situations. Langer (2016) believes that noticing these changes and differences is the hallmark of being mindful. She writes about seven myths that plague not only the learning environment of school systems, but many other industries as well. Mindful and mindless traits can be generalized across a variety of trades and businesses. These seven things have been engrained into peoples' minds since childhood and have created a society in which they are believed to be absolute truth:

- 1. The basics must be learned so well that they become second nature.*
- 2. Paying attention means staying focused on one thing at a time.*
- 3. Delaying gratification is*

*important. 4. Rote memorization is necessary in education. 5. Forgetting is a problem. 6. Intelligence is knowing “what’s out there.” 7. There are right and wrong answers (Langer, 2016).*

These myths undermine a person’s ability to be mindful (Langer, 2016). In an environment like information systems and social networking, being mindful is a necessary trait in order to not succumb to security threats.

Although the construct of mindfulness originated from the ancient religion and traditions of Buddhism (Kang & Wittingham, 2010), in today’s society, it has evolved to be equated with ideals of responding to mental stress skillfully (Bishop et al, 2004). To date, scientists have made a generalization that awareness and “present-moment attention” are important constituents of mindfulness (Wallace, 2008; Kang & Wittingham, 2010; Mikulas, 2011). Mindfulness was measured first in 2001 by Buchheld & Walach (2002) with the creation of the Freiburg Mindfulness Inventory (FMI). To date, there are 11 scales that one can measure mindfulness with (Phang et al, 2015). There are many instruments that measures the general propensity to be attentive in everyday life. Perhaps the most widely used are the Mindful Attention Awareness Scale (MAAS) (Brown & Ryan, 2003) and Langer’s (1989) measures of mindfulness. MAAS is a 15-item scale that measures open awareness of, and attention to, the happenings of the present. Langer (1989) developed a mindfulness scale utilizing a 21-question survey that will be used in this study to self-assess a business manager’s level of mindfulness.

In a study conducted by Pirson & Langer (2015), the Mindfulness scale that Langer (1989) created was extended by applying Western definitions of mindfulness, along with empirical measures, rather than the typical Eastern mindfulness characterizations. It is



stated that mindfulness is a positive action affecting a person's creativity, psychological posture, and physical well-being. Organizational researchers have also cited positive organizational outcomes due to mindfulness. It is described by the authors as a mindset that is open to novelty, which pursues an agenda of learning, being situated in the present, sensitive to context and perspective, and guided by rules and routines. If one adheres to a single perspective or a mindset of rigidity, they are considered mindless. Clinical psychologists have made advancements in measuring mindfulness and have extended it as a contemplative concept focusing on attention, awareness, and the absence of judgement (Pirson & Langer, 2015). Langer uses the old fairy tale of Hansel and Gretel to demonstrate mindfulness and mindlessness. Hansel and Gretel had terrible parents who were determined to walk them so far out into the forest, they wouldn't find their way home. However, upon overhearing this conversation between their parents, Hansel and Gretel put bread in their pockets and while walking through the woods they dropped little pieces of bread as a method to find their way back. Unfortunately, that bread was eaten or moved by various creatures in the forest, so the two children struggled to find their way home. Langer (2016) postulates that had they been more mindful in their journey and opened their mind to noticing their surroundings, they would have seen landmarks that they could have used to find their way back home. This is because mindfulness enables us to be open to context and notice the present. It also enables us to be sensitive to the ways information can present itself differently in fluctuating situations.

Mindfulness was the focus of Parrish Jr, J. L., Kuhn Jr, J. R., & Courtney, J. F. (2008) research on social networking and is cited as an integral part of implementing security policies and preventing spillages within organizations to combat information

technology security threats. Securing one's information gets harder as technology gets farther reaching and more complex. This dilemma puts more responsibility to safeguard IT systems and data on the user. While security policies help, they are not one size fits all. As new technologies are introduced, old security policies become outdated and not useful. Mindfulness is a significant part of electronic communication in modern organizations. Wall (2013) states that insider threats are more prevalent in businesses than outsider attacks. An insider is 'a trusted entity that is given the power to violate one or more rules in a given security policy' (Bishop & Gates, 2008). Ponemon (2009) reported that insider threat activities caused American businesses \$7.2M in 2010 and that the trend is a rise, not a decline, in incidents and associated cost due to spillage. Forty percent of data spillages in US organizations were caused by user negligence. Additionally, Ponemon's (2009) study showed it significant to delineate between malicious and non-malicious spillage. Randazzo et al (2005) was able to come up with a threat profile of the organizational insider who spills. According to their study, the offenders were technically unsophisticated and most spilled for financial gain. Whether malicious or not, the study concluded that organizational spillage by insiders more damaging and costly than attacks that were committed by outsiders.

In organizations, Weick et al (2006) reveal that mindfulness is positively associated with safety climates, attention to detail, IT security and creativity, and innovation and learning. Pirson & Langer's (2015) study focuses on applying Western measures of mindfulness to organizations, rather than typical Eastern measures of mindfulness to individuals. This is reinforced by Levinthal and Rerup's (2006) study of organizational mindfulness, which described it as "high sensitivity of perception and high flexibility of behavior to respond to diverse, changing stimuli (p.505)."

In Langer's (2016) work, she draws a correlation between behaving in a rote, unthinking manner and mediocrity in students. Because people have learned how to be mindless as children through teaching methods like rote memorization, we must be taught how to be mindful as adults. People do not find it difficult to pay attention when seeking novelty in play. Langer (2016) says this is because when something is novel people notice all the different things about it with ease, as opposed to being a strain. She conducted a study in which she concluded that varying the target of a person's attention improves their ability to remember it. So, the most effective way to pay attention better is to look for novelty in any given situation. She promotes a concept called soft vigilance. Rather than being hyper vigilant and focusing all of one's attention on one thing, soft vigilance allows for the person to open their mind to other hazards that may exist in the periphery. Teaching people to draw distinctions is another tactic that can be used to teach mindfulness. Langer (2016) advocates for people to be open to new information, creating new categories, and being aware of different perspectives. One should create working definitions of concepts, rather than closing themselves off to potential solutions, once they think they have solved the problem at hand.

Langer (2016) draws attention to the concept of a changing world by referencing the lamplighter in the well-known children's' book, *The Little Prince*. Every day the lamplighter turned the lamp on and off at the same time every day, even after it became unnecessary. He was following the instructions in a rote fashion, and, behaving mindlessly. His routine stayed fixed, even after the context had changed (Langer, 2016). IT professionals must keep up with the fast-paced changes of attack vectors by both malicious actors and mindless insiders. The security posture of organizations will continue to decline if security routines stay fixed, even after the context has changed. Being mindful must be an integral component of employee training and practices Ponemon (2009).

## **Summary**

The review of the literature revealed the nature of social networking sites and their prevalence, not only in society, but in business relations, and the lack of research regarding the spillage of business data on social networking sites. Spillage is defined by prior research and non-malicious spillage is differentiated from malicious spillage. Mindfulness is identified as a concept originated in eastern culture but transferred over time to concepts related to society in western culture. Langer's (Pirson & Langer, 2015) mindfulness measures and the evolution of those measures are used to understand the relationship between the social networking site user and spillage of confidential business data within pictures on those sites.

## Chapter 3 Methodology

### **Overview of Research Methodology**

The author conducted a quasi-experimental survey study to investigate the correlation between mindfulness and non-malicious spillage of sensitive business information within images on SNS. A sample population of managers with SNS accounts was studied. Purposive sampling was conducted to narrow the population appropriately. Video vignettes were used to measure user awareness of social networking spillage, and nominal response surveys were used to take a mindfulness survey and to make correlations between user awareness, mindfulness, and non-malicious spillage.

There are approximately 23.8 million employed individuals in the United States, according to the U.S. Bureau of Labor Statistics. In 2016, 16% of those employed were managers, which equates to 12.5 million people (Hamel & Zanini, 2016). 400 participants from various organizations in the United States were selected using the Target Audience capability in the online survey tool, SurveyMonkey, to be the sample population. Business managers cost the United States more than \$3 trillion per year, according to the Harvard Business Review (Hamel & Zanini, 2016). Businesses hire managers to enforce rules upon employees to protect their businesses. They also rely on managers to maintain a budget and provide performance reviews. It is reasonable to assume that these activities require a certain level of advanced education. For this reason, managers in the United States with social networking accounts were selected to be the sample population for this study.

### **Research Questions and Hypotheses**

The following research questions were posed during the course of this study.

RQ1: Is an individual's level of mindfulness positively associated with recognizing non-malicious spillage within photos on a SNS?

Based on the given information, the following will be hypothesized.

H1: There is a positive correlation between mindfulness and the detection of non-malicious spillage in photos on social networking sites.

More specifically, the author will hypothesize the following:

H1a: There is a positive correlation between mindfulness and the detection of proprietary information spillage within photos on social networking sites.

H1b: There is a positive correlation between mindfulness and the detection of personally identifiable information (PII) spillage within photos on social networking sites.

### **Data Necessary to Answer the Research Questions**

The data that is necessary to answer the research questions was collected using video vignettes and a survey based on the instrument used in the study conducted by Langer (1989), followed by a series of video vignettes and follow up questions pertaining to them. The author used SurveyMonkey to recruit the participants. A purposive sampling of business managers from various businesses throughout the United States responded to a survey that was sent in an e-mail through the online survey tool to 400 participants. Out of the 400 respondents, only 338 qualified in the data analysis. The participants were presented with the background information of the study and invited to participate in the survey. They were notified that they were not required to participate in the study, and that they reserved the right to leave this research study at any time. If they left the research study before it was completed, there would be no penalty to them, nor would they lose any benefits to which they were entitled. There was also an "attention question" that assured the

researcher that the participants were engaged and reading the entirety of the questions before answering. Nearly 100% of the participants passed the attention question, and the researcher did not count the responses in the data analysis of those who didn't.

Langer's (1989) mindfulness questionnaire was distributed to the participants before they watch the vignettes to assess their rate of mindfulness. Please refer to Appendix A. Two scenarios were played out in video vignettes that helped the author measure the participants' level of mindfulness. Please refer to Appendix B. Questions were asked to the participants after they watched two different scenarios in the video vignettes. Please refer to Appendix C.

The quantitative data necessary to answer the research questions and test the hypotheses were collected using a 7-point Likert scale (1= strongly disagree and 7 = strongly agree).

## **Instrument Development**

The following section will address the instrument development and methods that will provide validity and reliability to the study. One of the survey instruments is a mindfulness survey developed in a study conducted by Langer (1989), a highly regarded and reputable professor at Harvard University, whose life's work has centered around the topic of mindfulness.

The purpose of the video vignettes, which will be the second instrument used, is to measure the mindfulness of the manager who detects the spillage and give the researcher the ability to show the participant more than one type of scenario. A follow up survey will be distributed to the participants and the survey questions will focus specifically on the scenarios in the video vignettes to reduce any biases from this study.

### *Reliability*

Reliability within a research study exists when there is consistency among the different measures of a construct (Ahire & Devaraj, 2001). The reliability of this research study will be tested for internal consistency using Cronbach's Alpha (Cronbach, 1951). Tavakol and Dennick (2011) state that an instrument can't be valid unless it's reliable. However, reliability does not depend on an instrument's validity. Calculating Alpha is widely used in research and only requires one test administration. In any study, as the estimate of reliability increases, the portion of the test score that is attributable to error should decrease.



## *Validity*

Validity is a significant component of any research study. This study was proven valid in a variety of ways. The author will utilize a methodology that has been validated in prior research, firstly. The author also employed discriminant analysis, which is the extent to which a concept and its indicators differ from another construct and its indicators (Campbell and Fiske, 1959). Vignette experiments, like the one conducted in this study, are said to be a welcome relief from monotonous survey instruments. They are also flexible and can be utilized to avoid socially desirable and politically correct answers, according to (Steiner et al 2016; Hall, Mero & Chermie (2017). Experiments in survey research are gaining popularity, because the internal validity of the experiment is improved by the survey's external validity (Steiner et al, 2016). Due to the vignette's ability to replicate situations, the correlating survey questions have a realistic context.

A pilot study was conducted using 10% of the sample size (31 participants). The results of the pilot study validated the approach that the author took to collect the data by showing that the surveys accurately measured what the author envisioned (Straub et al, 2004).

## **Population and Sample**

This study was conducted using a sample size of 338 participants recruited from various organizations throughout the United States. The participants of the study will include many recruiters and hiring managers from various organizations throughout the United States. Hill (2012) points out that the reason for a sample population is to ensure that the sample statistic is as close to the true statistic of the entire population under review as possible. Therefore, the sample size is sufficient based on the methodology

chosen.

This study used a purposive sampling technique to obtain participants. The author used an online survey tool to recruit an audience of managers from United States businesses, which is considered a target population. (Tongco, 2007).

### **Data Collection**

The survey was distributed through a web link using online survey software. The participants were asked to participate in the study via an email. Appendix A contains the survey they were invited to complete. Additionally, the 338 participants were asked to watch a series of video vignettes, which was the second instrument used. The video vignette script can be located in Appendix B. Follow up questions were distributed, via the same means, to the participants focusing specifically on the video vignettes, and that survey can be seen in Appendix C. The participants were divided into three groups. The first group watched the video that contained personally identifiable information (PII) spillage, the second group watched the video with proprietary information spillage, and the third group, the control group, watched a video with no spillage. All groups answered a series of mindfulness questions that can be found in Appendix A, so the author could identify relationships between mindfulness and information spillage. The participants' answers to the mindfulness questions were rated on a 7-point Likert scale.

### *Ethical Considerations*

Each participant was asked to give informed consent to be a participant in the study. The participant's identity will be kept confidential by not associating survey responses with any specific individual. Answers will remain anonymous. The participants will not be harmed physically or emotionally. They will acknowledge in

writing that they understand that all scenarios used in the study were hypothetical.

#### *Institutional Review Board (IRB)*

Prior to conducting the study and interacting with participants, the author was required by Nova Southeastern University to obtain approval from the Institutional Review Board (IRB). CITI training was completed in May 2015. The surveys were distributed via an email link by the survey tool company shortly after receiving IRB approval.

#### **Data Analysis**

The data was analyzed using Discriminant Analysis. Discriminant Analysis is established when two variables are expected to be uncorrelated, and when they are measured, the measurement indeed proves no correlation exists (Skearan & Bougie, 2013). There are two types of discriminant analysis: canonical and classification. Classification was appropriate for this study, because it examined the probability of classifying people into groups based on a set of discriminating variables. In this type of analysis, the categorical variables are detection of PII spillage and the detection of proprietary information spillage. These are the dependent variables. The discriminating variable, mindfulness, is the variable being predicted. Since the discriminating variables are used to form a composite, this is considered a multivariate method. Each of the individual aspects of mindfulness, when taken as a composite variable, will result in mindfulness itself. In order to use classification analysis, the researcher must examine the p-value of the Wilkes Lambda F calculation. The analysis conducted in this study provided that the two dependent variables were discriminant and passed the following assumptions: there are two or more groups; there are at least two cases per group;

multivariate normality exists amongst discriminating variables; discriminating variables are measured at least at the interval level; the covariance matrices for each group must be approximately equal; and, lastly, there are any number of discriminating variables so long as it is less than the number of cases, minus two.

The graphic below theorizes the author’s proposed data analysis.

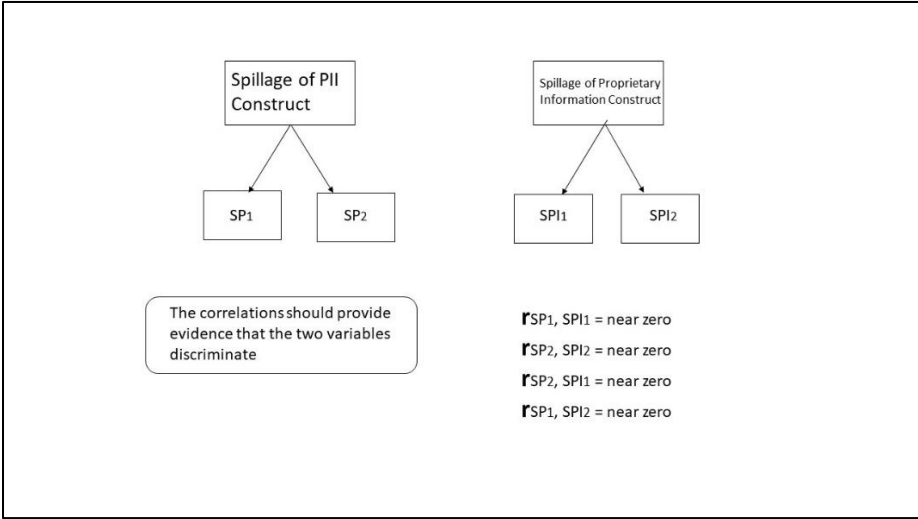


Figure 4: Data Analysis Example

This is a valid and frequently used statistical analysis method for experiments and quasi-experiments. The framework of this study is based on factors of the construct of mindfulness and users of SNS who make decisions to post and measures the ability of a manager to detect spillage in the event the employee is not mindful in their posting decisions.

The purpose of the investigation was to determine if business managers could detect PII spillage and proprietary data spillage on SNS. Classification Discriminant Analysis was most appropriate because covariance matrices across groups were not statistically significant.

### *Step 1*

The first step of conducting Classification Discriminant Analysis was to conduct a Box's Test of Equality of Covariance Matrices. This method tests the null hypothesis that the covariance matrices of the dependent variables are equal across groups.

### *Step 2*

Review the squared canonical correlations to ensure that function 1 somewhat contributes to successful classification. Using Wilkes lambda, this should result in statistical significance. For the purpose of this study, only one function was tested and proved significant in two of the three groups.

### *Step 3*

Utilize the cross validation output in SPSS to review the percentage of original grouped cases that are correctly classified. The researcher should decide if the percentage is large enough to be considered correctly classified. The standardized canonical discriminant function coefficients and structure matrix should also be reviewed to determine viable classification.

The 338 participants were divided into three groups; one was a control group, and the other two were the experiment groups. One-third of the participants were shown personally identifiable information. One-third were shown proprietary information, and the last third were in the control group. All assignments to the groups were randomly selected using logic in the online survey tool. Each group was shown a video vignette of a hypothetical situation in which a person unknowingly spilled, or in the case of the control group didn't spill, confidential business data. The first group answered Langer's mindfulness survey questions, then watched the PII video vignette. After watching, they

were asked if they noticed any proprietary or personal information.



Figure 5: Video Vignette 1

The second group answered Langer's mindfulness survey questions, then watched the PII video vignette. After watching, they were asked if they noticed any proprietary or personal information.

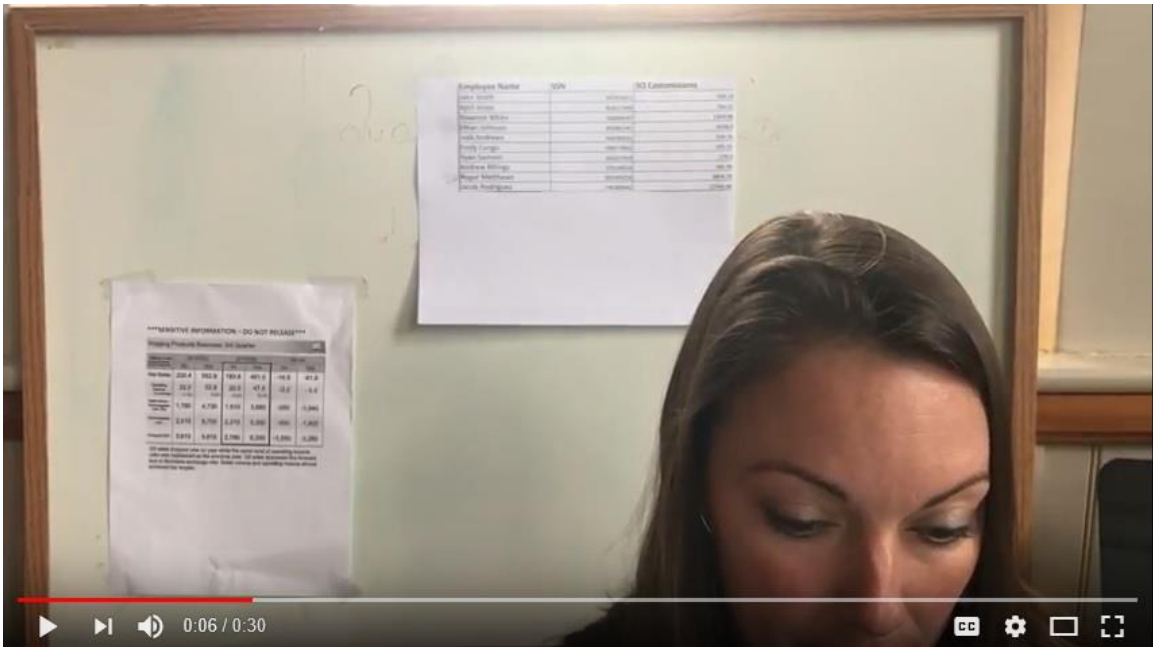


Figure 6: Video Vignette 2

The third group answered Langer’s mindfulness survey questions, then watched the PII video vignette. After watching, they were asked if they noticed any proprietary or personal information.

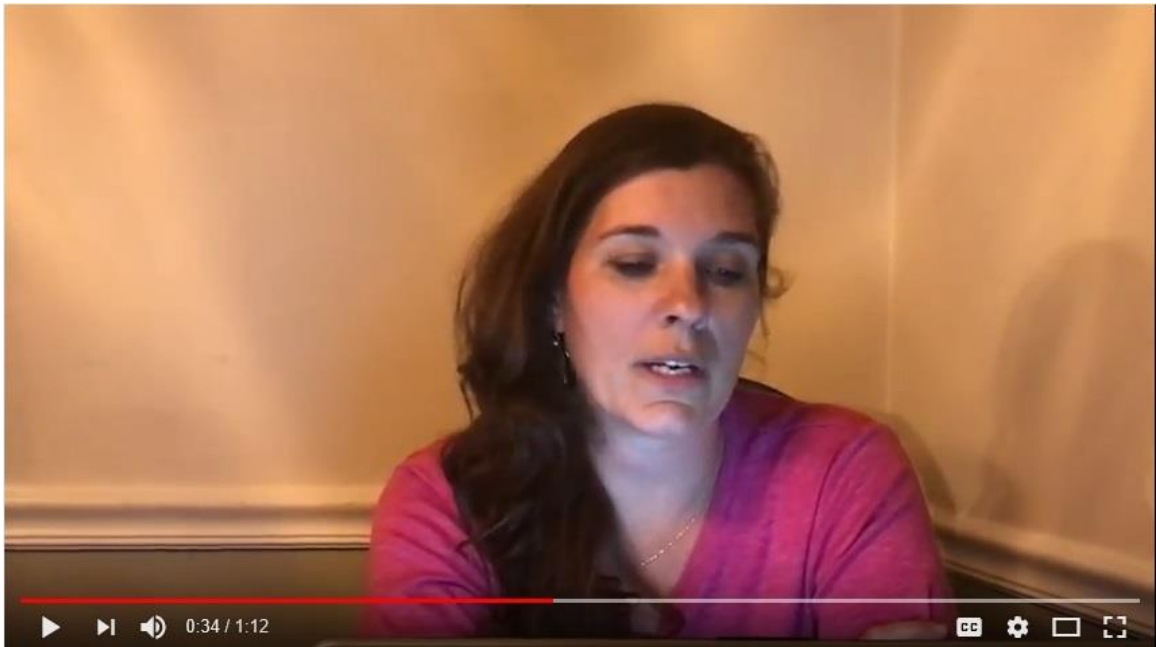


Figure 7: Video Vignette 3 (Control Group)

*Step 1: Build the data set*

The researcher used the Statistical Package for the Social Sciences (SPSS) software to manipulate the collected data. When inputting the data, it became clear that some of the variable properties needed to be redefined, because it was difficult to identify a value or identifier for each of the Groups. After redefining some of the variable properties, recoding variables into new variables, then converting string variables to numeric, the data was then organized based on the research questions. The researcher then only selected those participants who answered “Yes” to the in the response box indicating they had watched the video.

*Step 2: Run the data in SPSS*

The second step in the analysis was to score the responses for questions 4-22 in Appendix C, which were the “Mindfulness” questions which were answered on a Likert scale. Questions 4-22 in Langer’s (1989) mindfulness questionnaire equate to questions 4-22 in the mindfulness questionnaire in this study. The author produced a total score for the subject’s level of mindfulness, which was the independent variable in the study. This required reverse coding, per Langer’s (1989) mindfulness questionnaire:

*In the spaces numbered 1-21 below, record your answers from your actual survey.*

*However, you must reverse score the following items.*

2      5      7      8      9      15      19      21

*For example, this means that if you scored item 2 as a 1, you would record it as a 7.  
as a 3, you would record it as a 5.  
as a 4, you would record it as a 4.  
as a 5, you would record it as a 3.  
as a 6, you would record it as a 2.  
as a 7, you would record it as a 1.*

Next, the researcher ran the covariance matrices for the corresponding video for each



group. The PII subjects were labeled Group 1. The Proprietary Information subjects were labeled Group 2, and Group 3 watched the video with no spillage, and were the control group. The participants were asked:

1. Watch this video before answering the question below. Once you have watched the video, enter yes in the response box. Only watch the video once.
2. When watching the video, did you notice any personally identifiable information (PII) or proprietary information in it? Yes, or no.

The researcher went on to run the Box's Test of Equality of Covariance Matrices for each of the video groups. This test measures the degree that the null hypothesis that the observed covariance matrices of the dependent variables are equal across groups. The researcher then reviewed the squared canonical correlations to ensure that function 1 contributes to successful classification. The result of the Wilk's Lambda calculation should be statistically significant to ensure the function is capable of correctly classifying a large enough percentage of the original cases. Cross validation is conducted next to ensure fitting the function to the original data does not overestimate the success of the function.

*Step 3: Analyze the output*

Below are the statistical results for each hypothesis.

H1: There is a positive correlation between mindfulness and the detection of non-malicious, PII spillage in photos on social networking sites.

The statistical result for this hypothesis was .581  $p > .05$ .

H1a: There is a positive correlation between mindfulness and the detection of proprietary information spillage within photos on social networking sites.

The statistical result for this hypothesis was .596  $p > .05$ .

The statistical result for the control group was .202  $p > .05$ .

The objective of the content analysis was to answer the following research question: Is an individual's level of mindfulness positively associated with recognizing non-malicious spillage within photos on a SNS? The researcher's objective is to draw conclusions based on the data analysis in relation to answering the research question.

### **Resources**

The resources the researcher required to conduct this study were gathered using the online survey tool, SurveyMonkey. There were 338 participants who responded to the survey questions. They indicated they were business managers in various organizations across the United States. The data indicated they were from appropriate age groups, income ranges, and regions in the country.

The participants responded to a survey that asked them questions that nominally scored their level of mindfulness, then asked them to watch video vignettes that either contained or didn't contain spillage of PII or proprietary data. They were asked to indicate whether they were able to recognize spillage in the video. The data analyzed made correlations about their level of mindfulness in relation to their ability to detect online spillage in social networking photos. The researcher used Statistical Package for the Social Sciences (SPSS), which is a commonly used data analytics software, to analyze the data.

### **Summary**

Chapter three explored the methodology the author used in the research. A quasi-experimental study with a targeted population was conducted using a modified version of Langer's (1989) mindfulness questionnaire, followed by the observation of video vignettes and questions related to detection of spillage within the videos. 338 participants were

recruited from 9 different regions in the United States. Their age ranges were representative of business managers in the United States. A pilot study was conducted prior to the research study to validate the methodology and research instruments. The pilot study confirmed that the data sets were valid, all external links were reachable, the logic in the survey worked, and that pilot sample business managers understood the survey questions.

First, the researcher built the data set. Then she ran the data through Statistical Package for the Social Sciences (SPSS). She used a Classification Discriminant Analysis to draw relationships from mindfulness to SNS spillage. The quantitative data was collected using a 7-point Likert scale. There were a few questions that produced dichotomous nominal, yes or no, responses. Next, she analyzed the output, drew conclusions from the data and interpreted the results.

## Chapter 4 Results

### **Introduction**

This chapter presents an impartial analysis of the research study. The data collection process is described, as well as the methods used to statistically analyze the data. What the data analysis depicts is the measurement of mindfulness, based on Langer's (1989) mindfulness scale, and the relationship that mindfulness has to the detection of non-malicious spillage in images on social networking sites. Demographic data is displayed and depicts that the age range, genders, and geographic locations of the participants is typical of business managers in the United States. It also describes the generalized level of sophistication the participant has with SNS, and answers whether the respondent has received any SNS training. All data in the study is quantitative. The chapter concludes with a summary of the results.

### **Data Collection**

A pilot study was conducted to assist in identifying issues with the survey before it was sent out to 400 potential respondents. In turn, the embedded videos in the study were tested successfully, the experimental and control groups were validated, and the sample business managers affirmed that the questions in the survey made sense to them. The researcher reorganized the questions in the survey based on the pilot participants' feedback. Once this was completed successfully, the survey was distributed via an online survey tool, SurveyMonkey. The software tool used email as the method of distribution. The participants were recruited based upon qualifiers the researcher entered into the survey tool, such as "business managers," and "United States citizen." The survey tool sent the email to 400 participants, to account for a margin of error in case participants declined to

participate. Once the potential participant opened the email, they were presented with background information about the study and were invited to participate.

### **Data Analysis**

The data was checked for accuracy prior to completing the analysis. An inspection of the data was conducted, and it was found that some participants had not watched the video by responding “no” to the question, “Watch this video before answering the question below. Once you have watched the video, enter yes in the response box.” An “attention question” was also used to ensure all participants were reading the whole question before answering. 99% of the participants answered the attention question correctly. Out of 386 total responses, it was found that 338 responses were valid. 74% of the respondents were female and 26% were male. The distribution of the data indicated that the gender of the purposive sampling was representative of business managers in the United States (Hamel & Zanini, 2016). Additionally, 4.9% of the respondents were between the ages of 18-26, 11.89% were between the ages of 27-35, 24.48% were between the ages of 36-44, 9.09% were between the ages of 45-53, 49.65% older than 53. This age range is representative of a population containing business managers in the United States (Hamel & Zanini, 2016). The data also depicted that 4.9% of the respondents were located in New England, 12.14% were located in the Middle Atlantic, 12.14% were located in the East North Central region of the United States, 14.29% were located in the West North Central region of the United States, 20% were from the South Atlantic, 3.57% were located in the East South Central region, and 8.57% were located in the West South Central region. The distribution of the data collected indicates that the geographic region of the sample appeared to be representative

of the major businesses in the United States.

Table 2.0

*Gender, Age, Geographic Region of Respondents*

Respondent	Frequency	Percentage
<i>Gender</i>		
Male	37	26%
Female	106	74%
<i>Age Range</i>		
18-26	7	4.90%
27-35	17	11.89%
36-44	35	24.48%
45-53	13	9.09%
53+	71	49.65%
<i>Region</i>		
New England	6	4.29%
Mid Atlantic	17	12.14%
East North Central	17	12.14%
West North Central	20	14.29%
South Atlantic	28	20.00%
East South Central	5	3.57%
West South Central	12	8.57%
Mountain	10	7.14%
Pacific	25	17.86%

*Description of Variables and Descriptive Statistics*

The dependent variables in this study are proprietary information spillage detection and personally identifiable information spillage detection. The independent variable is mindfulness. The manager's social networking experience and access to proprietary information are mediating variables. The graphic below shows the relationships between the variables in this study.

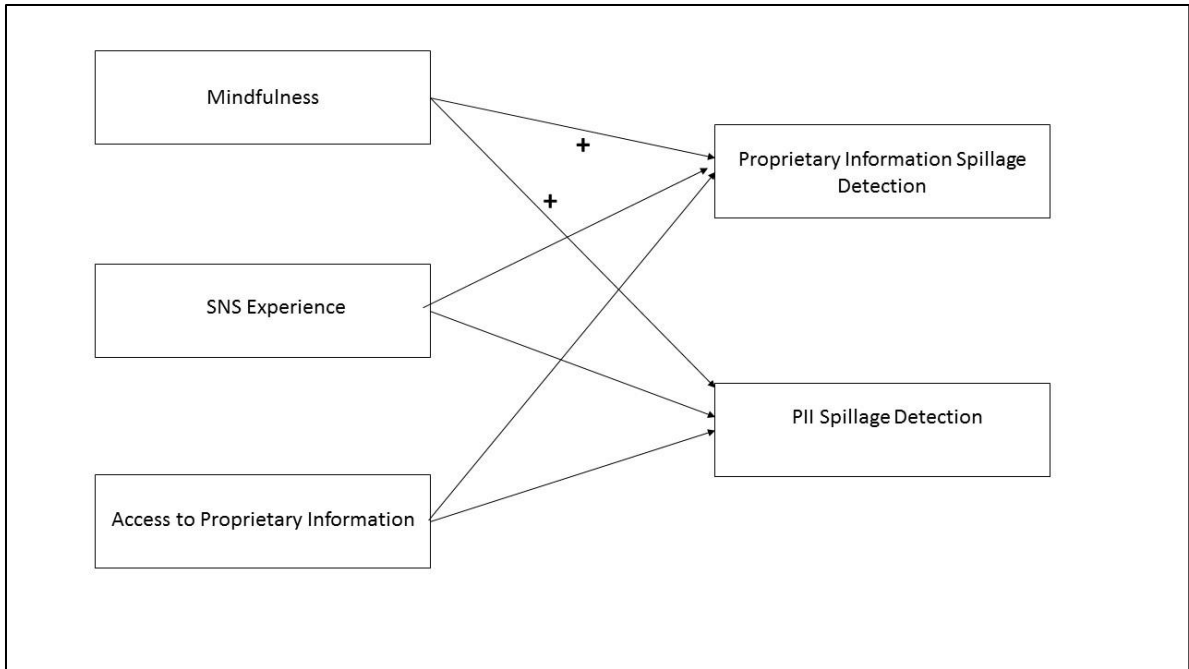


Figure 8: Variables

During data analysis, the data was checked for accuracy. First, the author conducted an automatic inspection of the data. She found that 385 respondents had taken the survey, but not all respondents had not answered all the questions, or had not watched the video vignettes, which were a pertinent part of the study. Therefore, a total of 338 responses were used for the data analysis. Of the respondents, 74% were female and 26% were male. The distribution of the data collected indicates that the gender of the sample was representative of the population of business managers in the United States (Hamel & Zanini, 2016).

Additionally, 4.9% of the respondents were between the ages of 18-26, 11.89% were between the ages of 27-35, 24.48% were between the ages of 36-44, 9.09% were between the ages of 45-53, 49.65% older than 53. This age range is representative of a population containing business managers in the United States (Hamel & Zanini, 2016).

4.9% of the respondents were located in New England, 12.14% were located in

the Middle Atlantic, 12.14% were located in the East North Central region of the United States, 14.29% were located in the West North Central region of the United States, 20% were from the South Atlantic, 3.57% were located in the East South Central region, and 8.57% were located in the West South Central region. The distribution of the data collected indicates that the geographic region of the sample appeared to be representative of the major industry locations in the United States.

It's important to note the amount of social networking experience the participants had, since they must understand how social networks operate to be able to detect spillage on them. 9.79% of the respondents reported they were not very knowledgeable about SNS. However, most of the respondents, 69.23% answered that they were somewhat knowledgeable about SNS. Almost 20% indicated they were very knowledgeable, and a small percentage, 1.4%, considered themselves experts in the use of SNS. The distribution of the data indicates that the average number of participants have adequate experience in SNS.

The responses to the background questions are presented in Table 3. Specifically, 30.07% of the participants indicated to have received social networking security training, while 69.93% of the participants have never received social networking security training. When asked how knowledgeable the participants were about social networking, 9.79% indicated they were not knowledgeable at all. 69.23% indicated they were somewhat knowledgeable, 19.58% answered they were very knowledgeable, and 1.4% considered them social networking experts. Brown and Vaughn (2011) indicate that managers use Facebook to make hiring decisions in their 2011 study. This research shows that the majority of managers in the sample are somewhat knowledgeable about social networking



sites. Table 3 shows the respondents' indication of social networking experience.

Table 3.0

*Social Networking Experience*

Respondent	Frequency	Percentage
Not knowledgeable	14	9.79%
Somewhat knowledgeable	99	69.23%
Very knowledgeable	28	19.58%
Expert	2	1.4%

The researcher split the purposive sample into three groups. The first group watched the video that contained personally identifiable information (PII) spillage, the second group watched the video with proprietary information spillage, and the third group, the control group, watched a video with no spillage. All groups answered a series of mindfulness questions that can be found in Appendix A, so the author could identify relationships between mindfulness and information spillage. The participants' answers to the mindfulness questions were rated on a 7-point Likert scale. Below is a table that displays descriptive characteristics by group. The descriptive characteristics include region in the United States, household income, gender and age.

Table 4.0

*Descriptive Statistics Group 1 = PII Spillage Detection*

		Region	Household income	Gender	Age
N	Valid	107	107	107	107
	Missing	0	0	0	0
Mean		5.60	5.92	1.70	3.84
Median		6.00	5.00	2.00	4.00
Mode		8	4	2	3
Std Deviation		2.543	2.689	.460	.963
Range		8	9	1	3

Table 5.0

*Descriptive Statistics Group 2 – Proprietary Information Spillage*

		Region	Household Income	Gender	Age
N	Valid	110	112	112	112
	Missing	2	0	0	0
Mean		5.03	6.20	1.79	3.80
Median		5.00	5.00	2.00	4.00
Mode		3	11	2	3
Std Deviation		2.666	3.099	.406	.957
Range		8	9	1	3

Table 6.0

*Descriptive Statistics Group 3 – Control Group*

		Region	Household Income	Gender	Age
N	Valid	132	135	135	135
	Missing	3	0	0	0
Mean		5.25	6.13	1.74	3.83
Median		5.00	5.00	2.00	4.00
Mode		5	5	2	3
Std Deviation		2.530	2.926	.440	.966
Range		8	10	1	3

*Discriminant Analysis*

The data was analyzed using Discriminant Analysis. Out of the two types of discriminant analysis: canonical and classification, classification was appropriate for this study, because it examined the probability of classifying people into groups based on a set of discriminating variables. In this type study, the categorical variables are detection of PII spillage and the detection of proprietary information spillage, which are also the

dependent variables. The discriminating variable, mindfulness, is the variable being predicted, and is the independent variable. Since the discriminating variables are used to form a composite, this is considered a multivariate method. Each of the individual aspects of mindfulness, when taken as a composite variable, will result in mindfulness itself. In order to use classification analysis, the researcher must examine the p-value of the Wilks Lambda F calculation (Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L., 1998).

**Group 1 Data Analysis Using Discriminant Analysis**

This is a valid and frequently used statistical analysis method for experiments and quasi-experiments. The below tables depict mindfulness correlations with detection of non-malicious spillage for Group 1. Correlation coefficients can be between -1 and +1 to be considered statistically significant. The measure of Group 1, who detected PII spillage, was .581, which is significant. The participants who scored higher on the various levels of mindfulness, detected PII more frequently. This supports the following hypothesis:

H1b: There is a positive correlation between mindfulness and the detection of personally identifiable information (PII) spillage within photos on social networking sites.

Table 7.0

*Box’s Test of Equality of Covariance Matrices – Group 1 – PII Spillage Detection*

Box’s M		8.814
F	Approx.	.849
	df1	10
	df2	48702.741
	Sig.	.581

A review of the squared canonical correlations for Group 1 suggest that function 1 contributes to successful classification, explaining 7.84%  $((2.80)^2 * 100)$  of the variation in the group membership. This is important, since classifying into mindfulness groups help the reader to understand the association of the level of mindfulness to detection of non-malicious online spillage on SNS. The groups the participants were classified in are Novelty Seeking, Novelty Producing, Engagement, and Flexibility. The following result is statistically significant, Wilk's  $\lambda = .040$ ,  $\chi^2(4) = 10.018$ ,  $p < .050$ . One can gauge the precision of the result for classification functions by examining the p-value of the Wilks Lambda F statistic. Wilks Lambda is a MANOVA test that shows how well each level of independent variable contributes to the model. The scale range is from 0 to 1. 0 describes total discrimination, and 1 equals no discrimination. The squared structure coefficients will show how much variation each dependent variable shares with each underlying composite variable.

Table 8 reveals that function 1 is capable of correctly classifying 62.2% of the original cases. If the squared canonical correlation is small, the associated function contributes little to successful classification. If the squared canonical correlation is large, the associated function contributes a lot to successful classification.

Table 8.0

*Classification Results – Group 1 – PII Spillage Detection*

Original	Count		1	2	Total
			Predicted Group Membership		
		DV_Notice	1	2	Total
Original	Count	1	30	19	49
		2	29	49	78

	%	1	61.2	38.8	100.0
		2	37.2	62.8	100.0
Cross-validated <sup>c</sup>	Count	1	25	24	49
		2	32	46	78
	%	1	51.0	49.0	100.0
		2	41.0	59.0	100.0

---

1

Because fitting the function to the original data tends to overestimate the success of the function a cross validation of the results was conducted in which many functions are derived as there are people in the study. Each function is derived with one case omitted so that the omitted case can be subsequently classified. The classification results for this showed 42.6% of the cases were correctly classified.

To determine which of the independent variables contributes most to the underlying composite, and maximizes group classification, the standardized discriminant function weights suggest that responses to the engagement variable score highest, followed by flexibility, then novelty producing, and lastly, novelty seeking. Refer to Table 9.

Table 9.0

*Standard Canonical Discriminant Function Coefficients – Group 1*

Variable	Function 1
Novelty Seeking	-.665
Novelty Producing	.138
Flexibility	.579

---

<sup>1</sup>a. VidPath = 1

b. 62.2% of original grouped cases correctly classified.

c. Cross validation is done only for those cases in the analysis. In cross validation, each case is classified by the functions derived from all cases other than that case.

d. 55.9% of cross-validated grouped cases correctly classified.

Engagement .850

---

The structure coefficients suggested that Engagement accounted for 72.25% of the function's variance, followed by Flexibility at 33.5%, and Novelty Producing at 1.9%. See table 10.<sup>2</sup>

Table 10.0

*Structure Matrix – Group 1*

---

Variable	Function 1
Engagement	.801
Flexibility	.680
Novelty Producing	.595
Novelty Seeking	.236

---

**Group 2 Data Analysis Using Discriminant Analysis**

The below tables depict mindfulness correlations with detection of non-malicious spillage for Group 2. Correlation coefficients can be between -1 and +1. The measure of Group 2, who detected proprietary data spillage, was .596, which is significant. Correlation coefficients can be between -1 and +1 to be considered statistically significant. The participants who scored higher on the various levels of mindfulness, detected proprietary data spillage more frequently. This supports the following hypothesis:

H1b: There is a positive correlation between mindfulness and the detection of proprietary data spillage within photos on social networking sites.

---

<sup>2</sup> Variables ordered by absolute size of correlation within function.

Table 11.0

*Box's Test of Equality of Covariance Matrices – Group 2 – Proprietary Data Spillage*

Box's M		8.919
F	Approx.	.834
	df1	10
	df2	9152.000
	Sig.	.596

A review of the squared canonical correlations for Group 2 suggest that function 1 contributes to successful classification, explaining 16%  $((.400)^2 * 100)$  of the variation in the group membership. This result is statistically significant, Wilk's  $\lambda = .002$ ,  $\chi^2(4) = 17.450$ ,  $p < .050$ .

Table 12 reveals that function 1 is capable of correctly classifying 68.3% of the original cases.

Table 12.0

*Classification Results – Group 2 – Proprietary Data Spillage Detection*

Original	Count	Predicted Group Membership			Total
		DV_Notice	1	2	
Original	Count	1	17	8	25
		2	25	54	79
	%	1	68.0	32.0	100.0
		2	31.6	68.4	100.0
Cross-validated <sup>c</sup>	Count	1	17	8	25
		2	25	54	79
	%	1	68.0	32.0	100.0
		2	31.6	68.4	100.0

Because fitting the function to the original data tends to overestimate the success of the function a cross validation of the results was conducted in which many functions are derived as there are people in the study. Each function is derived with one case omitted so that the omitted case can be subsequently classified. The classification results for this showed 68.3% of the cases were correctly classified.

To determine which of the independent variables contributes most to the underlying composite, and maximizes group classification, the standardized discriminant function weights suggest that responses to the engagement variable score highest, followed by flexibility, then novelty producing, and lastly, novelty seeking. Refer to Table 13.

Table 13.0

*Standard Canonical Discriminant Function Coefficients – Group 2*

Variable	Function 1
Novelty Seeking	.080
Novelty Producing	.671
Flexibility	.112
Engagement	.326

The structure coefficients suggested that Novelty Producing accounted for 45.02% of the function's variance, followed by Engagement at 10.62%, Flexibility at 1.25% and

<sup>3</sup>a. VidPath = 1

b. 68.3% of original grouped cases correctly classified.

c. Cross validation is done only for those cases in the analysis. In cross validation, each case is classified by the functions derived from all cases other than that case.

d. 68.3% of cross-validated grouped cases correctly classified.



Novelty Seeking at .05%. See table 14.<sup>4</sup>

Table 14.0

*Structure Matrix – Group 2*

Variable	Function 1
Engagement	.940
Flexibility	.760
Novelty Producing	.697
Novelty Seeking	.589

**Group 3 Data Analysis Using Discriminant Analysis**

The below tables depict mindfulness correlations with detection of non-malicious spillage for Group 3. Correlation coefficients can be between -1 and +1. The measure of Group 3, who detected nothing, was .202. The author expected this outcome from the control group, since no data was spilled in the third video.

Table 15.0

*Box's Test of Equality of Covariance Matrices – Group 3 – Control Group*

Box's M		14.224
F	Approx.	1.341
	df1	10
	df2	13229.081
	Sig.	.202

A review of the squared canonical correlations for Group 2 suggest that function 1 contributes to successful classification, explaining .46%  $((.068)^2 * 100)$  of the variation in

<sup>4</sup> Variables ordered by absolute size of correlation within function.

the group membership. This result is statistically significant, Wilk's  $\lambda = .002$ ,  $\chi^2(4) = .482$ ,  $p < .050$ .

Table 16 reveals that function 1 is capable of correctly classifying 55.1% of the original cases.

Table 16.0

*Classification Results – Group 3 – Control Group*

Original	Count	Predicted Group Membership			Total
	DV_Notice	1	2		
Original	Count	1	14	15	29
		2	33	45	78
	%	1	48.3	51.7	100
		2	42.3	57.7	100
Cross-validated <sup>c</sup>	Count	1	7	22	29
		2	41	37	78
	%	1	24.1	75.9	100
		2	52.6	47.4	100

5

Because fitting the function to the original data tends to overestimate the success of the function a cross validation of the results was conducted in which many functions are derived as there are people in the study. Each function is derived with one case omitted so that the omitted case can be subsequently classified. The classification results for this

<sup>5</sup>a. VidPath = 3

b. 55.1% of original grouped cases correctly classified.

c. Cross validation is done only for those cases in the analysis. In cross validation, each case is classified by the functions derived from all cases other than that case.

d. 41.1% of cross-validated grouped cases correctly classified.

showed 55.1% of the cases were correctly classified.

To determine which of the independent variables contributes most to the underlying composite, and maximizes group classification, the standardized discriminant function weights suggest that responses to the novelty producing variable score highest, followed by engagement, then flexibility, and lastly, novelty seeking. Refer to Table 17.

Table 17.0

*Standard Canonical Discriminant Function Coefficients – Group 3*

Variable	Function
Novelty Seeking	.876
Novelty Producing	.160
Flexibility	.169
Engagement	-.135

The structure coefficients suggested that Novelty Seeking accounted for 76.73% of the function's variance, followed by Flexibility at 2.8%. See Table 18.<sup>6</sup>

Table 18.0

*Structure Matrix – Group 3*

Variable	Function 1
Engagement	.984
Flexibility	.642
Novelty Producing	.606
Novelty Seeking	.494

The researcher expected that the control group would not see any spillage, since

<sup>6</sup> Variables ordered by absolute size of correlation within function.

there was no spillage displayed in the video vignette. The data shown supported this expectation.

### **Summary of Results**

The results of the data analysis show positive correlation between mindfulness and the detection of personally identifiable information posted in photos on social networking sites. H1 and H1a is supported. The results confirm that there is statistical significance in correlating a high mindfulness score, using Langer's (1989) mindfulness measures, and frequent detection of PII and proprietary information spillage on SNS by business managers.

### **Summary**

Chapter four described the results of the data analysis completed in this study. A pilot study was conducted to validate the worthiness of the questions, ensure the embedded videos worked in the survey tool, and verify the credibility of the data sample with 10% of the projected population. After this was accomplished, the author used an online survey tool to administer the survey to 400 purposive sampling population. 338 participants responded with valid data and were used for the analysis. Three groups were generated from these respondents.

The first group who watched a video vignette with personally identifiable information (PII) in it had high mindfulness scores. This indicated there was a positive correlation between mindfulness and detection of PII in photos on SNS. The second group who watched a video vignette with proprietary information displayed also had high mindfulness scores. The data also indicated a statistically significant positive correlation between levels of mindfulness and the detection of spillage of proprietary business data on

SNS. The control group behaved as the researcher expected. The majority of the respondents did not see spillage in the video vignette, since no spillage existed.

See below table for a summary of the data analysis.

Table 19.0

*Group Analysis*

<b>Box's Test of Equality of Covariance Matrices</b>					
	Box's M	Sig			
<b>Group 1</b>	F	.581			
<b>Group 2</b>	F	.596			
<b>Group 3</b>	F	.202			
<b>Classification Results</b>					
<b>Predicted Group Membership</b>					
<b>Group 1</b>	Or Count	DV Notice	1	2	Total
		1	30	19	49
		2	29	49	78
		1	61.2	38.8	100.0
		2	37.2	62.8	100.0
<b>Cross Validated Count</b>		1	25	24	49
		2	32	46	78
		1	51.0	49.0	100.0
		2	41.0	59.0	100.0
62.2% were classified correctly					

<b>Group 2</b>	Or Count	DV Notice	1	2	Total
		1	17	19	49
		2	25	49	78
		1	68.0	38.8	100.0
		2	31.6	62.8	100.0
<b>Cross Validated Count</b>		1	17	24	49
		2	25	46	78
		1	68.0	49.0	100.0
		2	31.6	59.0	100.0
68.3% were classified correctly					

<b>Group 3</b>	Or Count	DV Notice	1	2	Total
		1	14	15	29
		2	33	45	78
		1	48.3	51.7	100
		2	42.3	57.7	100
<b>Cross Validated Count</b>			7	22	29
		2	41	37	78
		1	24.1	75.9	100
		2	52.6	47.4	100
55.1% were classified correctly					

**Standard Canonical Discriminant Function Coefficients**

<b>Group 1</b>	Function
<b>Novelty Seeking</b>	-.665

<b>Novelty Producing</b>	.138
<b>Flexibility</b>	.579
<b>Engagement</b>	.850

<b>Group 2</b>	<b>Function</b>
<b>Novelty Seeking</b>	.080
<b>Novelty Producing</b>	.671
<b>Flexibility</b>	.112
<b>Engagement</b>	.326

<b>Group 3</b>	<b>Function</b>
<b>Novelty Seeking</b>	.876
<b>Novelty Producing</b>	.160
<b>Flexibility</b>	.169
<b>Engagement</b>	-.135

**Structure Matrix**

<b>Group 1</b>	<b>Function</b>
<b>Engagement</b>	.801
<b>Flexibility</b>	.680
<b>Novelty Seeking</b>	.595
<b>Novelty Producing</b>	.236

<b>Group 2</b>	
----------------	--

<b>Engagement</b>	.940
<b>Flexibility</b>	.760
<b>Novelty Seeking</b>	.697
<b>Novelty Producing</b>	.589
<b>Group 3</b>	
<b>Engagement</b>	.984
<b>Flexibility</b>	.642
<b>Novelty Seeking</b>	.606
<b>Novelty Producing</b>	.494



## Chapter 5 Conclusions

### **Introduction**

This chapter presents the conclusions drawn from conducting this study. The researcher also describes the research questions and hypotheses and describes the implications of the study. Future research is proposed as well.

### **Conclusions**

The main goal of this study was to understand the relationship between mindfulness levels related to non-malicious spillage associated with posting photos that have sensitive business information contained within to social networking sites, and the ability of business managers to detect it. The author sought to show positive correlation between mindfulness and the detection of non-malicious spillage on social networking sites. More specifically, the author sought to show a positive correlation between mindfulness and the detection of proprietary information spillage within photos on social networking sites; as well as a positive correlation between mindfulness and the detection of personally identifiable information (PII) spillage within photos on social networking sites. The hypothesis (H1) stated that there would be a positive correlation between mindfulness and the detection of proprietary business information on a SNS. The hypothesis (H1a) stated that there would be a positive correlation between mindfulness and the detection of personally identifiable information (PII) on SNS by business managers. The data analysis found that both hypotheses were statistically significant, positively correlating detection of PII and proprietary data, and the mindfulness levels of business managers.

A research question was asked during the introduction of the study. RQ1: Is an individual's level of mindfulness positively associated with recognizing non-malicious

spillage within photos on a SNS?

The proposed research question is asked to determine the effectiveness of an individual's level of mindfulness to detect non-malicious spillage in photos in social networking sites. The study supports the research question by correlating mindfulness with the detection of PII and proprietary data in SNS. If an employee practices mindfulness by being resilient in their SNS activity, they should be able to avoid spillage. The results of the study show that the business managers recognized PII when it was shown in the video and potentially had enough training and knowledge to understand that it should not be shown on a social networking site. When comparing the groups with spillage in the videos to the control group, it was apparent the control group did not see any spillage, as intended, but they also scored lower as a group on the mindfulness scale.

### **Implications**

Implications can be made about the data that was not found to be statistically significant. The business managers detected PII and proprietary information. When looking at the descriptive data, one must examine the age and level of social network security training of the individuals participating. Almost 50% of the sample population was over the age of 53. This makes sense, considering the target population was business managers. It takes time and experience to manage people in a business. The age difference between the average respondent and recent college graduates who take middle management positions, but have a wealth of experience in technology and video conferencing are important to note. The respondents are likely to differ as time goes by. It is also worthy to note that only 30% of the respondents stated they took social network security training. See figure 12 below.

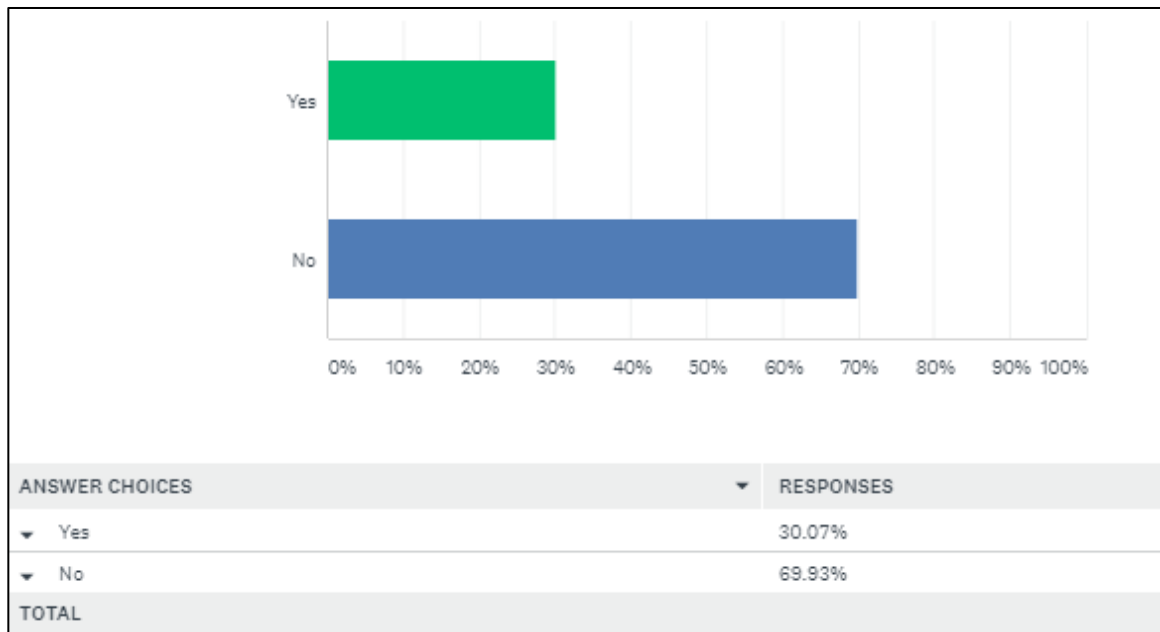


Figure 9: Social Networking Security Training

Since the participants of this study were business managers, it is prudent to note that there is a potential industry gap in social networking security training and general knowledge of social networking sites. This is interesting, since other studies indicate that employee training is a major threat to businesses combating insider threats and spillage (Parrish & San Nicolas-Roca, 2012). Parrish & San Nicholas-Roca (2012) also argue that there are three ways in which mindfulness relate to information systems security training. The first way is for personnel to be engaged in security training. The second way is for personnel to be aware of situations that are hotbeds of security policy violation. The third way is to establish a culture of mindfulness within the organization (Parrish & San Nicolas-Roca, 2012). While prior research emphasizes the importance of social networking security training, it may not be implemented in the field as often as necessary to combat spillage of proprietary business information.

This study also extended Langer’s (1989) mindfulness questionnaire and measures by correlating the quantitative data with dichotomous nominal variables of PII and

proprietary data spillage. While Langer (1989) focused on mindfulness from a psychosocial perspective, this study combines it with the concepts of information security in the ever-growing field of cyber security.

An additional important implication is the pervasiveness that social networking sites have into Americans' daily lives. According to Brown and Vaughn (2011), managers commonly use Facebook to make hiring decisions on a frequent basis. There seems to be a gap between business manager's use of social networking sites and their level of training and sophistication with the use of them.

### **Limitations**

The first limitation of the study is that the business managers were limited to watching only one video per group. A better representative sample could have been obtained by showing the participants a collection of like videos to average how many times they detected spillage. The information presented to the respondents was limited.

The video vignettes were created by professional actors, as opposed to in the field by individuals in a real situation. While the situation was realistic in nature, it is only natural that the participant knew the actors were pretending to spill the data. When presented with a real situation in their own lives, the participants may behave more vigilantly.

While choosing a target audience was necessary to answer the research questions for this study, opening the study up to a broader audience may have altered the results based on the geographic location of the participants. Also, it is possible the control group figured out that they were supposed to be looking for spillage in the control group video, which may have impacted the results of the control group responses.

### **Future Research**

Future research should focus on further granulating the data in Langer's (1989) mindfulness measures. A future researcher could extend the study to assign participants to Langer's (1989) Flexibility, Novelty-Seeking, Novelty-Producing, and Engagements groups. To take it a step further, the future researcher could compare the scores to those of the 2014 Harvard University and General Population samples.

Another future research recommendation is to expand the topics of training and social networking security. One could identify relationships between a lack of training and spillage on SNS, or completion of an effective training program and detection of spillage on SNS.

### **Summary**

This dissertation examined the relationship between mindfulness amongst business managers and their ability to detect online spillage on social networking sites. There were two types of spillages investigated. The first type was personally identifiable information, or PII. Specifically, the PII shown was employee names and social security numbers on a memorandum taped to a whiteboard in the background of a photo that an employee posted online. Actors were employed to create video vignettes in which they non-maliciously spilled this data. There was statistical significance in the data that showed that the higher the mindfulness score of the business manager, the more frequent the participants detected the spillage. The other type of spillage was proprietary business data. Specifically, the third quarter financials of a company were displayed in the background of a video with the words "CONFIDENTIAL – Do not release" typed on the memorandum. Again, the memorandum was affixed to a wall behind the person acting in the video. This type of spillage was harder for the business managers to detect.

Again, the results were statistically significance and correlated this spillage with a lack of mindfulness. This study is an extension of Langer's (1989) mindfulness studies in which she measured mindfulness in social-behavioral studies. While there are many studies that measure mindfulness in the workplace (Bodner, 2001; Haigh, et al 2011), very few have related mindfulness to social networking or cybersecurity topics. With the prevalence of both industries in our daily lives, it is prudent to investigate their relationships to spillage. Spillage can cost a large business its reputation and millions of dollars, and a small business its existence.

This study addressed the following research question:

RQ1: Is an individual's level of mindfulness positively associated with recognizing non-malicious spillage within photos on a SNS?

The following statements were hypothesized:

H1: There is a positive correlation between mindfulness and the detection of non-malicious spillage on social networking sites.

More specifically, the author hypothesized the following:

H1a: There is a positive correlation between mindfulness and the detection of proprietary information spillage within photos on social networking sites.

H1b: There is a positive correlation between mindfulness and the detection of personally identifiable information (PII) spillage within photos on social networking sites.

To address the research question and accompanying hypotheses, an extended survey was developed that extended Langer's (1989) work and incorporated videos and questions about spillage. The participants were asked to view the videos and report if they saw any spillage. The participants were divided into three equal groups. The first group

viewed PII spillage on an SNS, the second group viewed proprietary data spillage, and the third group viewed no spillage and were the control group. The researcher found that there was statistical significance in the first group that viewed the PII spillage. Their overall mindfulness score was high, as well as their ability to detect the spillage.

The data was analyzed using a Classified Discriminant Analysis, which is the extent to which a concept and its indicators differ from another construct and its indicators (Campbell and Fiske, 1959). Vignette experiments, like the one conducted in this study, are said to be a welcome relief from monotonous survey instruments. They are also flexible and can be utilized to avoid socially desirable and politically correct answers, according to Steiner et al (2016). Due to the vignette's ability to replicate situations, the correlating survey questions have a realistic context.

There are two types of discriminant analysis: canonical and classification. Classification was appropriate for this study, because it examined the probability of classifying people into groups based on a set of discriminating variables. In this type of analysis, the categorical variables are detection of PII spillage and the detection of proprietary information spillage. These are the dependent variables. The discriminating variable, mindfulness, is the variable being predicted.

Overall, the results of the study suggest that there is a relationship between a business manager's level of mindfulness and their ability to detect PII and proprietary data spillage on a social networking site. The data also suggests there may be a training gap for business managers and their sophistication on social networking sites. Many reported as being novice users or only being somewhat knowledgeable about social networking security.





## Appendix A

### Langer's Mindfulness Scale

#### Personal Outlook Scale

Instructions: Below are a number of statements that refer to your personal outlook. Please rate the extent to which you agree with each of these statements. If you are confused by the wording of an item, have no opinion, or neither agree nor disagree, use the "4" or "NEUTRAL" rating. Thank you for your assistance.

Table 19.0

#### *Likert Scale*

7-Point Likert Scale						
1	2	3	4	5	6	7
Strongly Disagree	Disagree	Slightly Disagree	Neutral	Slightly Agree	Agree	Strongly Agree

I like to investigate things.  
 I generate few novel ideas.  
 I am always open to new ways of doing things.

I get involved in almost everything I do.  
 I do not actively seek to learn new things.  
 I make many novel contributions.

I stay with the old tried and true ways of doing things.  
 I seldom notice what other people are up to.  
 I avoid thought provoking conversations.

I am very creative.  
 I can behave in many different ways for a given situation.  
 I attend to the big picture.

I am very curious.  
 I try to think of new ways of doing things.  
 I am rarely aware of changes.

I have an open-mind about everything, even things that challenge my core beliefs.  
 I like to be challenged intellectually.  
 I find it easy to create new and effective ideas.

I am rarely alert to new developments.  
 I like to figure out how things work.  
 I am not an original thinker.

## Scoring of LMS-21

In the spaces numbered 1-21 below, record your answers from your actual survey. However, you must reverse score the following items.

2      5      7      8      9      15      19      21

For example, this means that if you scored item 2 as a 1, you would record it as a 7.  
as a 3, you would record it as a 5.  
as a 4, you would record it as a 4.  
as a 5, you would record it as a 3.  
as a 6, you would record it as a 2.  
as a 7, you would record it as a 1.

Question number:

- |           |           |
|-----------|-----------|
| 1. _____  | 12. _____ |
| 2. _____  | 13. _____ |
| 3. _____  | 14. _____ |
| 4. _____  | 15. _____ |
| 5. _____  | 16. _____ |
| 6. _____  | 17. _____ |
| 7. _____  | 18. _____ |
| 8. _____  | 19. _____ |
| 9. _____  | 20. _____ |
| 10. _____ | 21. _____ |
| 11. _____ |           |

## Determination of scores:

- 1.) Remember those items that are reverse scored.
- 2.) On all scales, higher scores indicate more of the designated dimension.

To determine your OVERALL MINDFULNESS SCORE, sum all items (1-21).

To determine your FLEXIBILITY SUBSCALE SCORE, sum items 3, 7, 11, and 16.

To determine your NOVELTY SEEKING SUBSCALE SCORE, sum items 1, 5, 9, 13, 17, and 20.

To determine your NOVELTY PRODUCING SUBSCALE SCORE, sum items 2, 6, 10, 14, 18, and 21.

To determine your ENGAGEMENT SUBSCALE SCORE, sum items 4, 8, 12, 15, and 19.

## SOME SELECTED CORRELATES OF LMS-21 OVERALL AND SUBSCALE SCORES

*Higher overall mindfulness scores are associated with:*

- Greater physical wellbeing (e.g. faster reaction time, better health)
- Greater psychological wellbeing (e.g. more life satisfaction less need for vacation)
- Greater social wellbeing (e.g. more positive relationships, less attachment anxiety in relationships).

- Greater vocational wellbeing (e.g. higher job satisfaction, more learning, more decision-making, more creativity)

*Higher flexibility scores are associated with:*

- More cognitive empathy (perspective-taking)
- More emotional empathy (ability to recognize/feel in tune with another's emotional state and show appropriate concern)

*Higher novelty seeking scores are associated with:*

- Less negative affect
- Fewer social biases (e.g. less racist sexist, and homophobic attitudes)

*Higher novelty producing scores are associated with:*

- More positive affect
- Greater use of humor in coping

*Higher engagement scores are associated with:*

- Greater cognitive disembedding ability (e.g. identifying simpler stimuli within more complex stimuli) and greater cognitive restructuring skills (e.g. replacing irrational thoughts with realistic thoughts)
- Higher self-esteem

## Interpreting Your Score

TWO 2014 Samples:	Harvard University		General Population	
	M	SD	M	SD
Overall Score (21-147)	114.5	14.7	111.1	17.6
Flexibility (4-28)	20.4	3.6	20.2	4.0
Novelty-Seeking (6-42)	35.9	4.6	33.9	5.9
Novelty-Producing (6-42)	30.6	6.2	30.1	4.7
Engagements (5-35)	27.7	3.9	26.9	4.7

FROM THESE AND RELATED STUDIES, DATA DIVIDED INTO EQUAL THIRDS:

SCORE THIRD	BOTTOM THIRD	MIDDLE THIRD	UPPER THIRD
Overall Mindfulness	21-106	107-122	123-147
Flexibility	4-18	19-22	23-28

Novelty-Seeking	6-33	34-38	39-42
Novelty-Producing	6-27	28-34	35-42
Engagement	5-25	26-30	31-35

LOCATE YOUR SCORE ABOVE AND COMPLETE THE FOLLOWING TABLE:

Table 20.0

*Final Mindfulness Score*

Your Score	Your Third	Your Description
Overall Mindfulness Score		
Flexibility Score		
Novelty-Seeking Score		
Novelty-Producing Score		
Engagement Score		

## Appendix B

### Video Vignette Scripts

#### *Script for Video Vignette 1*

Purpose: to decipher if managers will detect spillage in a picture on social media

Spillage content: picture of Jamie at the company festival contains the confidential release date of a new version of software code.

Actors: Andrea, Jamie

Andrea: Hey, Jamie! What did you do this weekend?

Jamie: Oh, I went to a concert. Want to see pics?

Andrea: Sure!

Jamie: Oh my! I forgot about this. John took this hilarious picture of me in costume at my job's harvest festival.

Andrea: Look at your crazy hair! Hilarious!

#### *Script for Video Vignette 2*

Purpose: to decipher if managers will detect personally identifiable information (PII) on a whiteboard in the background of an online video conferencing system.

Spillage content: PII is displayed in the background of a video conference.

Actors: June, Jamie, Andrea

June: Good afternoon, this is June at Headquarters.

Jamie: Hi June.

Andrea: Hi June, hi Jamie.

June: Let's get started. Thank you for joining. We are here today to discuss the release of our next quarterly financials. I need to make sure we are all on the same page before I present them to the board. Do either of you have questions about the numbers in the attachment?

Jamie: Can you explain the difference between line 2 and column D on the spreadsheet?

June: Sure can. Line 2 shows the amount of employee commissions required to get to the projected profit on column D.

#### *Script for Video Vignette 3*

Purpose: to decipher if managers will detect personally identifiable information (PII) on a whiteboard in the background of an online video conferencing system.

Spillage content: Nothing is displayed in the background of a video conference.

Actors: June, Jamie, Andrea

June: Good afternoon, this is June at Headquarters.

Jamie: Hi June.

Andrea: Hi June, hi Jamie.

June: Let's get started. Thank you for joining. We are here today to discuss the release of our next quarterly financials. I need to make sure we are all on the same page before I present them to the board. Do either of you have questions about the numbers in the attachment?

Jamie: Can you explain the difference between line 2 and column D on the spreadsheet?

June: Sure can. Line 2 shows the amount of employee commissions required to get to the

projected profit on column D.

## Appendix C

### Video Vignette Survey

1. Have you had any social networking security training?

Yes \_\_\_ No \_\_\_

a. If so, was it provided by your employer?

Yes \_\_\_ No \_\_\_

2. How knowledgeable do you feel you are about social networking?

Very knowledgeable \_\_\_ Somewhat knowledgeable \_\_\_ Not knowledgeable \_\_\_

3. Have you ever read and consented to an employee social networking policy?

Yes \_\_\_ No \_\_\_

4. When reviewing video A, did you notice any proprietary information in it?

Yes \_\_\_ No \_\_\_

5. When reviewing video B, did you notice any proprietary information in it?

Yes \_\_\_ No \_\_\_


Appendix D  
Survey



PAGE TITLE

1. You are not required to participate in this study. In the event you do participate, you may leave this research study at any time. If you leave this research study before it is completed, there will be no penalty to you, and you will not lose any benefits to which you are entitled. If you agree to participate in this research study, place the date in the date box below.

Date / Time

MM/DD/YYYY 

\* 2. Choose your age range

- 18-26  45-53  
 27-35  63+  
 36-44

\* 3. What is your gender?

- Male  
 Female

\* 4. I like to investigate things.

Strongly disagree Strongly agree



\* 5. I generate few novel ideas.

Strongly disagree Strongly agree



\* 6. I am always open to new ways of doing things.

Strongly disagree Strongly agree



\* 7. I "get involved" in almost everything I do.

Strongly disagree Strongly agree



\* 8. I do not actively seek to learn new things.

Strongly disagree Strongly agree



\* 9. I make many novel contributions.

Strongly disagree Strongly agree



\* 10. I stay with the old tried and true way of doing things.

Strongly disagree Strongly agree



\* 11. I seldom notice what other people are up to.

Strongly disagree Strongly agree



\* 12. I avoid thought-provoking conversations.

Strongly disagree Strongly agree



\* 13. I am very creative.

Strongly disagree Strongly agree



\* 14. I can behave in many different ways for a given situation.

Strongly disagree Strongly agree



---

\* 15. I attend to the "big picture."

Strongly disagree Strongly agree



\* 16. I am very curious

Strongly disagree Strongly disagree



\* 17. I try to think of new ways of doing things.

Strongly disagree Strongly agree



\* 18. I am rarely aware of changes.

Strongly disagree Strongly agree



\* 19. I have an open mind about everything, even things that challenge my core beliefs.

Strongly disagree Strongly agree



\* 20. I like to be challenged intellectually.

Strongly disagree Strongly agree



26. **A 33.0%** Watch this video before answering the question below. Once you have watched the video, enter yes in the response box. Only watch the



video once.

- B 33.0%** Watch this video before answering the question below. Once you have watched the video, enter yes in the response box. Only watch the



video once.

C 34.0%

Watch this video before answering the question below. Once you have watched the video, enter yes in the response box. Only watch the



video once.

- Yes
- No

\* 27. When watching the video, did you notice any proprietary information, or personally identifiable information, in it?

- Yes
- No

\* 28. Have you had any social networking security training?

- Yes
- No

\* 29. Have you ever read and consented to an employer's social networking policy?

- Yes
- No

\* 30. How knowledgeable are you about social networking?

- Not knowledgeable at all
- Somewhat knowledgeable
- Very knowledgeable
- I consider myself an expert

---

## References

- Ahire, S. L., & Devaraj, S. (2001). An empirical comparison of statistical construct validation approaches. *IEEE Transactions on Engineering Management*, (48)3, 319-329.
- Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes*, (50)2, 179-211.
- Ajzen, I., & Fishbein, M. (1980). Understanding attitudes and predicting social behaviour.
- Benbasat, I., Gefen, D., & Pavlou, P. A. (2010). Introduction to the special issue on novel perspectives on trust in information systems. *MIS Quarterly*, (34)2, 367-371.
- Besmer, A., & Richter Lipford, H. (2010). *Moving beyond untagging: photo privacy in a tagged world*. Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.
- Bicen, H., & Cavus, N. (2011). Social network sites usage habits of undergraduate students: Case study of Facebook. *Procedia-Social and Behavioral Sciences*, 28, 943-947.
- Bishop, M., & Gates, C. (2008). *Defining the insider threat*. Paper presented at the Proceedings of the 4th annual workshop on Cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead.
- Bishop, S. R., Lau, M., Shapiro, S., Carlson, L., Anderson, N. D., Carmody, J., . . . Velting, D. (2004). Mindfulness: A proposed operational definition. *Clinical psychology: Science and practice*, (11)3, 230-241.
- Bodner, T. (2001). *Individual differences in mindfulness: the Langer mindfulness scale*. Paper presented at the Poster presented at the annual meeting of the American Psychological Society, Toronto, Ontario, Canada.
- Bohnert, D., & Ross, W. H. (2010). The influence of social networking web sites on the evaluation of job candidates. *Cyberpsychology, Behavior, and Social Networking*, (13)3, 341-347.
- Brown, K. W., & Ryan, R. M. (2003). The benefits of being present: mindfulness and its role in psychological well-being. *Journal of personality and social psychology*, (84)4, 822.

- Brown, V. R., & Vaughn, E. D. (2011). The writing on the (Facebook) wall: The use of social networking sites in hiring decisions. *Journal of Business and psychology*, (26)2, 219.
- Brumfield, J. (2016). Verizon's 2016 data breach investigations report finds cybercriminals are exploiting human nature. Retrieved from Verizon: <http://www.verizon.com/about/news/verizons-2016-data-breach-investigations-report-finds-cybercriminals-are-exploiting-human-0>.
- Buchheld, N., Grossman, P., & Walach, H. (2001). Measuring mindfulness in insight meditation (Vipassana) and meditation-based psychotherapy: The development of the Freiburg Mindfulness Inventory (FMI). In: JMMR.
- Burcher, N. (2010). Facebook usage statistics by country-July 2010 compared to July 2009 and July 2008. Nick burcher. *Personal thoughts on the evolution of media and advertising*, 2.
- Campbell, D. T., & Fiske, D. W. (1959). Convergent and discriminant validation by the multitrait-multimethod matrix. *Psychological bulletin*, (56)2, 81.
- Comcowich, W. 2015. The Importance of Creating a Social Media Marketing Strategy – and How to Do It. <http://www.cyberalert.com/blog/index.php/the-importance-of-creating-a-social-media-marketing-strategy-and-how-to-do-it/>. Accessed on 10 April 2018.
- Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika*, (16)3, 297-334.
- Curran, J. M., & Lennon, R. (2011). Participating in the conversation: exploring usage of social media networking sites. *Academy of Marketing Studies Journal*, (15), 21.
- Dillman, D. A., Smyth, J. D., & Christian, L. M. (2014). *Internet, phone, mail, and mixed-mode surveys: the tailored design method*: John Wiley & Sons.
- Eagly, A. H., & Chaiken, S. (1993). *The psychology of attitudes*: Harcourt Brace Jovanovich College Publishers.
- Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in human behavior*, (25)1, 153-160.
- French, A. M., & Read, A. (2013). My mom's on Facebook: an evaluation of information sharing depth in social networking. *Behaviour & Information Technology*, (32)10, 1049-1059.
- Furnell, S. (2005). Why users cannot use security. *Computers & Security*, (24)4, 274-279.



- Gordon, P. (2007). Data Leakage-Threats and Mitigation. *InfoSec Reading Room*.
- Haigh, E. A., Moore, M. T., Kashdan, T. B., & Fresco, D. M. (2011). Examination of the factor structure and concurrent validity of the Langer Mindfulness/Mindlessness Scale. *Assessment, (18)*1, 11-26.
- Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (1998). *Multivariate data analysis (5)*3, 207-219. Upper Saddle River, NJ: Prentice hall.
- Hall, K. R., Mero, N. P., & Cheramie, R. (2017). Reflecting on Performance Feedback: The Effect of Counterfactual Thinking on Individual Learning. In *Academy of Management Proceedings (Vol. 2017, No. 1, p. 15542)*. Briarcliff Manor, NY 10510: Academy of Management.
- Hamel, G., & Zanini, M. (2016). Excess Management Is Costing the US \$3 Trillion Per Year. *Harvard Business Review*.
- Holgado-Tello, F. P., Chacón-Moscoso, S., Barbero-García, I., & Vila-Abad, E. (2010). Polychoric versus Pearson correlations in exploratory and confirmatory factor analysis of ordinal variables. *Quality & Quantity, (44)*1, 153.
- Hill, R. (1998). What sample size is “enough” in internet survey research. *Interpersonal Computing and Technology: An electronic journal for the 21st century, (6)*3-4, 1-12.
- Ho, A., Maiga, A., & Aïmeur, E. (2009). *Privacy protection issues in social networking sites*. Paper presented at the Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on.
- Hoy, M. G., & Milne, G. (2010). Gender differences in privacy-related measures for young adult Facebook users. *Journal of Interactive Advertising, (10)*2, 28-45.
- Hui, L., Chow, K., Pun, K., Yiu, S.-M., Tsang, W. W., Chong, C., & Chan, H. (2004). *Risk management of corporate confidential information in digital form*. Paper presented at the Computer Software and Applications Conference, 2004. COMPSAC 2004. Proceedings of the 28th Annual International.
- Huitema, B. (2011). *The analysis of covariance and alternatives: Statistical methods for experiments, quasi-experiments, and single-case studies (Vol. 608)*: John Wiley & Sons.
- Hum, N. J., Chamberlin, P. E., Hambright, B. L., Portwood, A. C., Schat, A. C., & Bevan, J. L. (2011). A picture is worth a thousand words: A content analysis of Facebook profile photographs. *Computers in Human Behavior, (275)*, 1828-1833.

- Kane, G. C., Fichman, R. G., Gallagher, J., & Glaser, J. (2009). Community relations 2.0. *Harvard business review*, (87)11, 45-50.
- Kang, C., & Whittingham, K. (2010). Mindfulness: A dialogue between Buddhism and clinical psychology. *Mindfulness*, (1)3, 161-173.
- Kopp, E., Kaffenberger, L., & Jenkinson, N. (2017). Cyber Risk, Market Failures, and Financial Stability. In: International Monetary Fund.
- Langer, E. J. (1989). *Mindfulness*: Addison-Wesley/Addison Wesley Longman.
- Langer, E. J. (2004). Langer mindfulness scale user guide and technical manual. *Covenington, IL: IDS*.
- Langer, E. J. (2016). *The power of mindful learning*: Hachette UK.
- Langer, E. J., & Moldoveanu, M. (2000). The construct of mindfulness. *Journal of social issues*, (56)1, 1-9.
- Levinthal, D., & Rerup, C. (2006). Crossing an apparent chasm: Bridging mindful and less-mindful perspectives on organizational learning. *Organization science*, (17)4, 502-513.
- Lunney, G. H. (1970). Using analysis of variance with a dichotomous dependent variable: An empirical study. *Journal of educational measurement*, (7)4, 263-269.
- Maasberg, M., Warren, J., & Beebe, N. L. (2015). *The dark side of the insider: detecting the insider threat through examination of dark triad personality traits*. Paper presented at the System Sciences (HICSS), 2015 48th Hawaii International Conference on.
- Magklaras, G., & Furnell, S. (2005). A preliminary model of end user sophistication for insider threat prediction in IT systems. *Computers & Security*, (24)5, 371-380.
- Mikulas, W. L. (2011). Mindfulness: Significant common confusions. *Mindfulness*, (2)1, 1-7.
- Molok, N. N. A., Ahmad, A., & Chang, S. (2010). Understanding the factors of information leakage through online social networking to safeguard organizational information. In *Proceedings of the 21st Australasian Conference on Information Systems (ACIS)*.
- Neumann, P. (1999). *The challenges of insider misuse*. Paper presented at the SRI Computer Science Laboratory, Paper prepared for the Workshop on Preventing, Detecting, and Responding to Malicious Insider Misuse.

- Pallegedara, D., & Warren, M. (2016). Unauthorised Disclosure of Organisational Information through Social Media: A Policy Perspective. *IDIMC 2016*, 86.
- Parker, D. B. (1998). *Fighting computer crime: A new framework for protecting information*: John Wiley & Sons, Inc.
- Parrish, J. L., & Nicolas-Rocca, S. (2012). *Toward Better Decisions With Respect To Is Security: Integrating Mindfulness Into IS Security Training*. Paper presented at the Proceedings of the Seventh Pre-ICIS Workshop on Information Security and Privacy.
- Parrish Jr, J. L., Bailey, J. L., & Courtney, J. F. (2009). A personality based model for determining susceptibility to phishing attacks. *Little Rock: University of Arkansas*.
- Parrish Jr, J. L., Kuhn Jr, J. R., & Courtney, J. F. (2008). Mindful Administration of IS Security Policies. *AMCIS 2008 Proceedings*, 270.
- Pempek, T. A., Yermolayeva, Y. A., & Calvert, S. L. (2009). College students' social networking experiences on Facebook. *Journal of applied developmental psychology*, (30)3, 227-238.
- Phang, C.-K., Mukhtar, F., Ibrahim, N., & Mohd. Sidik, S. (2016). Mindful Attention Awareness Scale (MAAS): factorial validity and psychometric properties in a sample of medical students in Malaysia. *The Journal of Mental Health Training, Education and Practice*, (11)5, 305-316.
- Pirson, M. A., & Langer, E. (2015). *Developing the Langer mindfulness scale*. Paper presented at the Academy of Management Proceedings.
- Ponemon, L. (2009). Trends in Insider Compliance with Data Security Policies- Employees Evade and Ignore Security Policies. *Ponemon Institute*.
- Schultz, E. E. (2002). A framework for understanding and predicting insider attacks. *Computers & Security*, (21)6, 526-531.
- Sekaran, U., & Bougie, R. (2016). *Research methods for business: A skill building approach*. John Wiley & Sons.
- Sledgianowski, D., & Kulviwat, S. (2009). Using social network sites: The effects of playfulness, critical mass and trust in a hedonic context. *Journal of Computer Information Systems*, (49)4, 74-83.
- Smith, J. R. (2012). Rich media, poor media. *IEEE MultiMedia*, (19)3, 2-3.

- Stefanone, M. A., Lackaff, D., & Rosen, D. (2011). Contingencies of self-worth and social-networking-site behavior. *Cyberpsychology, Behavior, and Social Networking*, (14)1-2, 41-49.
- Steiner, P. M., Atzmüller, C., & Su, D. (2016). Designing Valid and Reliable Vignette Experiments for Survey Research: A Case Study on the Fair Gender Income Gap. *Journal of Methods and Measurement in the Social Sciences*, (7)2.
- Strano, M. M. (2008). User descriptions and interpretations of self-presentation through Facebook profile images. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, (2)2.
- Straub, D., Boudreau, M.-C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *The Communications of the Association for Information Systems*, (13)1, 63.
- Straub, D. W. (1989). Validating instruments in MIS research. *MIS quarterly*, 147-169.
- Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *International journal of medical education*, (2)53.
- Thelwall, M. (2011). Privacy and gender in the social web. In *Privacy Online*, 251-265: Springer.
- Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security*, (24)6, 472-484.
- Tongco, M. D. C. (2007). Purposive sampling as a tool for informant selection. *Ethnobotany Research and applications*, (5), 147-158.
- Walach, H., Buchheld, N., Buttenmüller, V., Kleinknecht, N., & Schmidt, S. (2006). Measuring mindfulness—the Freiburg mindfulness inventory (FMI). *Personality and Individual Differences*, (40)8, 1543-1555.
- Wall, D. S. (2013). Enemies within: Redefining the insider threat in organizational security policy. *Security journal*, (26)2, 107-124.
- Wallace, B. (2007). A mindful balance: What did the Buddha really mean by 'mindfulness'.
- Weick, K. E., & Putnam, T. (2006). Organizing for mindfulness: Eastern wisdom and Western knowledge. *Journal of management inquiry*, (15)3, 275-287.
- Wilson, R. E., Gosling, S. D., & Graham, L. T. (2012). A review of Facebook research in the social sciences. *Perspectives on psychological science*, (7)3, 203-220.

- Wright, K. B., Abendschein, B., Wombacher, K., O'Connor, M., Hoffman, M., Dempsey, M., & Shelton, A. (2014). Work-related communication technology use outside of regular work hours and work life conflict: The influence of communication technologies on perceived work life conflict, burnout, job satisfaction, and turnover intentions. *Management Communication Quarterly*, 28(4), 507-530.
- Zeadally, S., Yu, B., Jeong, D. H., & Liang, L. (2012). Detecting insider threats: Solutions and trends. *Information security journal: A global perspective*, (1)4, 183-192.
- Zingale, N. C. (2013). The phenomenology of sharing: Social media networking, asserting, and telling. *Journal of Public Affairs*, (13)3, 288-297.