Brain Betrayal: A Neuropsychological Categorization of Insider Attacks

Rachel L. Whitman
University of Georgia, rlw35713@uga.edu

Abstract
Thanks to an abundance of highly publicized data breaches, Information Security (InfoSec) is taking a larger place in organizational priorities. Despite the increased attention, the threat posed to employers by their own employees remains a frightening prospect studied mostly in a technical light. This paper presents a categorization of insider deviant behavior and misbehavior based off of the neuropsychological foundations of three main types of insiders posing a threat to an organization: accidental attackers; neurologically "hot" malcontents, and neurologically "cold" opportunists.

Disciplines
Cognitive Psychology | Industrial and Organizational Psychology | Information Security | Management Information Systems

INTRODUCTION

Information Security (InfoSec) is no longer a minor concern of organizations. In today's social media-saturated environment, data breaches can easily become large, publicized affairs that deal immense, sometimes irreparable blows to an organization's reputation (Ponemon Institute LLC, 2011). With cyberattacks coming from all sides and news outlets on the prowl for the next sensational breach, InfoSec professionals have increasingly turned their attention to the potential risks posed by an organization's own employees. Insider threat is understandably a serious issue: the damage caused by employees or associates is rated as more severe, costly, and difficult to detect than that of outsiders (Software Engineering Institute [SEI], 2013). While the majority of cyberattacks still originate from non-insiders, employee attacks are still viewed with no small amount of trepidation (SEI, 2013). Most organizations report feeling vulnerable to internally-originated incidents and 93% are planning to increase or maintain their InfoSec budgets accordingly—though roughly seven to nine percent of the median annual $750k IT budget is already allocated to security (Vormetric Data Security, 2015; Filkins & Hardy, 2016). This expansion of cybersecurity spending indicates recognition of a vulnerability, but increased internal focus potentially comes at a cost to workplace trust, organizational cohesiveness, and, ultimately, productivity.

Research attempts to explore causes and possible preventative approaches to insider threat have been gaining traction. However, as Crossler et al. note, most of these efforts tend to be geared towards the technical side of the cybersecurity field—the focus of the research appeals to the firewall-wielding, computer-savvy CISO, seemingly at the expense of the more managerial-minded Information Security professionals. Crossler and his colleagues also point to a rather undefined classification approach to insider attacks that label threat behavior as either deviant or misbehavior, and call for a clearer separation and examination of the two categories (Crossler et al., 2012). Loch, Carr, and Warkentin's Four Dimensions of Information Systems Security provides a comprehensive classification scheme for categorizing threats by analyzing threat source, agent, motivating intent, and potential results, and refinement by Willison and Warkentin has expanded the category of intent to include a continuum of motives—from unintentional to fully malicious (Lock, Carr, & Warkentin, 1992; Willison & Warkentin, 2013).

While subsequent multidimensional approaches have sought to classify threats in orthogonal manners, thus extending the modularity and applicability of Loch et al.'s original classification scheme, these approaches—thanks to their intended all-encompassing applicability—are not specific to insider threat (Jouini, Rabai, & Aissa, 2014; Jouini, Rabai, & Khedri, 2015). Due to the extremely negative emotional and financial impacts associated with the collapse of the employee-employer trust dynamic, insider threat poses a significant enough risk to warrant its own classification scheme (Reina & Reina, 2015).

By adopting a neuropsychological approach to investigating insider threat behavior, we are able to better tease apart the categories of insider deviant and misbehavior as rooted in aggression and nonaggression, respectively. We also propose a subcategorization of insider deviant behavior based on the neurological arousal levels of the aggression type displayed, resulting in our final categories of accidental attackers, hot malcontents, and cold opportunists. A common approach to uniting psychology with other management-involved fields is to pose the motivation-concerned question of *why*: why do employees fall for email scams? Why do they attack organizations? Why don't they change their password on a regular basis? We have been seeking to understand why employees attack their organizations, but perhaps it is time to ask how.

With the application of a neurologically-rooted system of categorization, we not only gain unique insight on the problem of insider threats and attacks, but we are able to surpass previously motivation-limited approaches to understanding such behavior on a psychological level. Armed with this information, Information Security professionals will be able to better understand, prepare for, and circumvent such attacks.

DANGEROUS INSIDERS

Using a traditional motive-based perspective, risks posed by employees can initially be broken down into two major groups: insiders that bear an intent to harm their organization, and those that do so accidentally. As previously mentioned, Crossler et al. classify these categories of behavior as insider deviant behavior and misbehavior, respectively (Crossler et al., 2012). The latter half, bearing no ill intent other than a possible aversion to following good security habits, requires no further categorization and such misbehaviors will be grouped together for the purpose of this approach, as most unintentionally risky behaviors can be traced to distraction or a general lack of awareness. Insiders that intend to harm their employers, however, require deeper analysis, as deviant behavior essentially amounts to acts of aggression.

It likely comes as no surprise that the neurological activity behind a lapse in attention is leagues away from that of a purposeful, aggression-based attack, but it is important to note that not all acts of aggression are cut from the same cloth. Motivation and context play a large role in determining how the body will process aggression in everyday life, and the same is true of deviant employee behavior. While both vengeance-driven sabotage and the purposeful misuse of user privileges for financial gain both seem to be intentional, deviant acts of an aggressive nature, they are displays of two very physiologically different types of human behavior. It is the difference between spitefully hurling your boss' prized decorative vase across the room, and secretly selling it on your local Free and For Sale Facebook page (whereas in this scenario, an accidental attacker might simply send the piece toppling with a stray elbow).

With these differences accounted for, we wind up with three categories of insider attacks: accidental, non-attentive, non-aggressive insiders; neurologically "hot" malcontents aiming to cause harm; and neurologically "cold" opportunists seeking to cut themselves a piece of organizational pie.

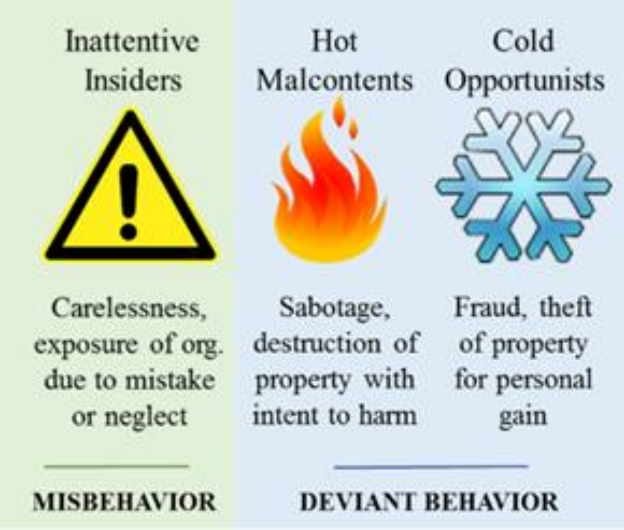

Figure 1: Proposed categories include "hot" anger and "cold" calculation in the deviant category, and inattention-based threat in the misbehavior section

Accidental Attackers

Just as the road to a familiar destination is paved with good intentions, so is the path to insider threat lined with non-malicious motives. Here defined by a lack of intent to harm an organization, unintentional insider threat can include accidental disclosure of classified information, careless treatment of physical data storage devices, and falling prey to often-obvious, sometimes-subtle phishing emails that even well-trained, cautious employees may respond to when bogged down with overwhelming amounts of correspondence (CERT Insider Threat Center [CERT], 2014). From a neurological perspective, unintentional insider threat behavior arises primarily from a lapse in attention—that is, a temporarily diverted level of consciousness. Any consequential breach of security is entirely unintended, and it is this complete lack of malice lends the title of accidental attacker to employees in this category.

Though the popularity of multitasking suggests otherwise, attention appears to be a limited resource, and employees can only spend so much before they begin to operate in the red. Though the connotations associated with words such as "careless" and "inattentive" contain negative implications, causes contributing to unintentional insider threat are varied and many, and the label of inattentive insider is not meant to be a judgment of an employee's responsibility or lack thereof. Whatever the circumstances surrounding an accidental attacker—excess amounts of stress imposed by a heavy workload, a lack of sleep, the presence of workplace distractions such as a noisy coworker—the end result is the same: a lack of attention and diminished or misdirected state of consciousness.

It may seem that the category of inattentive insiders contains mostly small workplace sins: phishing gullibility, a misplaced USB drive, or bad browsing habits. These seemingly small events stack up, though, as accidental data exposure is the most common cyber incident amongst insiders (SEI, 2013).

It is worth noting that intention once again plays an important role in distinguishing accidental threat. An intentional disregard for safe employee practices, though similar in results to a lack of attentiveness, falls under cold threat rather than inattentiveness. For example, insiders that violate guidelines for workplace behavior in order to illegally download music display a willful disregard for the expected employee behaviors. This intent to ignore codes of conduct places them under the third category—that of cold opportunists—as he or she is choosing to break the rules for the enjoyment that stands to be gained from such behavior. Inattentive insiders are categorized by their lack of attention, and willful ignorance fails to meet this qualification.

Hot Malcontents

Deriving its name from the active state of the sympathetic nervous system, "hot" insider attacks spawn from motives rooted in anger—and, by extension, aggression. One of the more overpowering human emotions, anger is able to muddy one's ability to reason, cause extreme short-sightedness, and turn an otherwise logical person into a raving lunatic (DeSteno & Piercarlo, 2011). Unlike negligence or inattentiveness, anger is characterized by intense arousal of the sympathetic nervous system—the same system that is responsible for the fear-induced fight or flight response (Carlson, 2013). While the fight or flight response is more commonly associated with fear, anger and fear share a number of biological characteristics—heart rate elevation, an increase in blood pressure, and a generally heightened state of awareness—and anger-driven insider aggression similarly runs on such responses (Ax, 1953).

Hot malcontents possess an additional neurological edge in that this category is essentially exclusively concerned with revenge-oriented insiders. While anger is certainly a dominating emotion in these instances, it has been shown that acts of vengeance activate not just the fight and flight response, but the brain's pleasure-tied reward pathways as well (de Dominique et al., 2004). The activation of these pathways make revenge more than a simple release of anger: it is a desirable, physiologically incentivized behavior. This neural intoxication makes hot malcontents a heated risk indeed.

The profile of the angry insider is well-cited archetype of the InfoSec community: an irate employee, upon discovering that they are to be demoted, fired, or otherwise cast from their spot on the organizational ladder, takes it upon themselves to alleviate their feelings of distress by relieving their former employer of valuable data or equipment. One way that hot malcontent threats differ from those of cold opportunists is that these attacks are most notably reactionary. Home Depot's Ricky Joe Mitchell, for example, caused former employer EnerVest nearly one million dollars in damages to office equipment and the company network after learning he was to be dismissed from the organization (Gallagher, 2014).

The defining characteristics of this category of insider attack are thus that they are aggressive in nature (qualifying them as deviant behavior), reactionary, and hold harming the organization as the primary goal of their behavior.

Cold Opportunists

In contrast to the heated, anger-driven nature of hot insider attacks, "cold" aggression shows much less arousal of the jittery, high-strung sympathetic nervous system. Fraud, exploitation, intellectual theft—these are all deviant behaviors that display aggression towards an organization, but they lack the neurological fire that behaviors of hot malcontents possess. Similar to acts of predation, insider attacks in this category instead fall under the jurisdiction of the calmer, more analysis-friendly parasympathetic nervous system.

This "rest and digest" division of the autonomic nervous system—which governs the unconscious activities that keep us alive and running—is responsible for some of the least aggressive activities known to humankind, such as sleep (Carlson, 2013). In certain situations, however, it can serve as a platform from which acts of aggression may be carried out. The most notable of these examples, predation, is generally defined as occurring when a member of one species engages in aggressive or violent behavior against a member of another species (Carlson, 2013). In the context of human behavior, we may presume to expand this definition to include not only activities such as hunting, but circumstances in which individuals seek to better their stations in life at the expense of others. In the absence of the adrenaline-soaked mindset that accompanies the fight or flight response, the focus is less on immediate survival (or vengeance, in the case of our hot malcontents) and more on personal advancement. Since the mind is not overwhelmed with emotion and is more capable of logical, long-term planning, attacks in this category can be highly complex, orchestrated events that pose massive risk towards an organization.

As the name suggests, cold opportunists are proactive rather than reactive: instead of negatively responding to an unfavorable HR decision, they act out of self-interest to take exploit their current situation, often financially. In the case of William G. Sullivan, Senior Database Administrator for Certegy Check Services, the potential gain in monetary advantages was enough to motivate Certegy Check Service's Senior Database Administrator to download and sell the personal records of eight and a half million customers—a breach of monumental scale (Kendall, 2007). Unlike hot malcontents, cold opportunists are not inherently against their employer; they are merely for themselves.

It is in this category that we may see the greatest variety of threat, as while financial incentives are the largest motivator of intentionally threatening insiders, espionage is steadily on the rise, and intellectual property theft is tied with accidental data exposure as the leading insider cyber incident (Verizon, 2016; SEI, 2013). Any ideological attacks conducted on an organization by an insider would similarly fall under the umbrella of cold opportunism, so long as they are proactive in nature. The defining qualifications of the cold opportunist branch of deviant insider behaviors are as follows: that the attack be an aggressive assault on an organization or its assets, that it be proactive in nature, and that it possess a self-serving intent on the part of the threat agent.

TRUST AND TRAITORS

When considering the multitude of ways in which employees pose serious risk to an organization, employees might ironically seem to be too risky for an organization to employ. The age-old and often-debated tug-of-war between the feasible and the ideal requires little discussion, but it is worth nothing the positive effects that trust in the workplace often beget. We spend much time focusing on the multitude of ways in which employees cannot be trusted, and for good reason. It is clear that our society is moving forward into an increasingly uncertain state. Between highly publicized security breaches like that of Target and Home Depot, and public information leaks that are only increasing in frequency, the concept of trust may come across as foolish notion.

However, trust does not exist in a workplace for the sole purpose of being broken: it serves to enhance performance and has a massive potential to help the organization. If an employer can foster and maintain an environment of trust in the workplace, not only will it reap the benefits of a harmonious, united workforce—it will have a leg up on the competition.

These benefits are both intuitive and well-documented. Increased levels of organizational trust lead to increased participation and engagement in employee work, and an environment in which workers are trusted to be able to competently fulfill their duties can lead to higher retention of talented individuals—whose expertise the organization stands to greatly benefit from (Reina & Reina, 2015). The Leader-Member Exchange Theory (LMX) from the Industrial/Organizational Psychological schools of thought revolves entirely around the formation of strong relationships between superiors and subordinates, and studies have found that high levels of trust in this dynamic are associated with positive work performance (Chen, Lam, & Zhong, 2012). Trust is a cornerstone of human interaction, one that cannot be struck from the workplace.

A Need for Control

As technology has grown smaller, portable, and even wearable, it has increased the spread of the workplace. Employees often have work laptops, USB drives with sensitive information, or their professional emails accessible even when not on the premises. While this expansion of the workplace indicates the diminishing separation of work and home—often at the expense of the domicile—it also poses a problem for information security professionals. Namely, that employees are both taking technology home and bringing their own personal devices to work.

The rise of supplying and utilizing personal technology in a productive environment is not limited to industry (Elementary schools even have programs such as BYLD that encourage students to "Bring Your Learning Device" and incorporate cell phones into curriculum), but it is causing some anxiety for IT decision makers. According to a 2015 survey by Vormetric, the vast majority of these professionals are concerned with their lack of control over mobile devices in the workplace. This worry, unfounded or not, is drawing attention when things like high-volume data storage remain pressingly vulnerable (Vormetric Data Security, 2015).

Though the increased attention pointed toward mobile devices indicates an elevated desire for control in an environment with innumerable variables, increasing security presence could have unintended negative effects. It is documented that while individuals who are not confident of their skill sets both benefit from and appreciate close monitoring, those who are skilled tend to resent such close attention—not only that, but their performance actually decreases in response (Aiello & Kolb, 1995). Though insiders pose some of the greatest threats to organizations, holding them under constant scrutiny would likely decrease both morale and performance, and in a worst-case-scenario could actually serve to drive away skilled employees.

The resulting conundrum is a classic one for InfoSec professionals. On one hand, the need for a balance for reasonable security measures. On the other, the need for effective workplace trust—especially since employee performance is correlated with their supervisor's perception of their ability (Dockery & Steiner, 1990). Both are necessary for maximum organizational efficiency, and it might seem that the answer lies in some variation of "too hot, too cold, just right." This is certainly a viable approach, and as every organization is a unique entity, it is up to the CISO to gauge what levels of security are appropriate for the situation. At the end of the day, cyber security is in the business of keeping the organization protected so that it may perform its business with confidence.

However, since we've gone to the trouble of classifying types of insider threat according to their physiology and categories of aggression, we can further extend our understanding into supplying general courses of action to prevent such occurrences. We've asked *how* instead of *why*, and answering this question is the first step in understanding *how not*.

IMPLICATIONS

Since our three categories of insider threat are essentially divided based on their types of aggression (or lack thereof), we will analyze the implications accordingly. Despite the differing complex forces of human behavior at play, the three categories of insider threat can be combated with a similar psychological approach. In all regards, it boils down to a matter of perception crafting.

The human brain is already in the business of synthesizing reality. It is capable of transducing and translating wavelengths of light into vivid, recognizable colors, it turns the compression and rarefaction of air into comprehensible language, and it regularly takes rhythmic utterances and extracts from them meaningful information. The brain has often been portrayed as nature's greatest supercomputer, but its remarkable processing power can be attributed in part to the fact that it takes shortcuts—as evidenced by the lengthy list of human biases to be found. Confirmation biases, stereotyping, hindsight bias—these often be the result of the brain attempting to "fill in the gaps" in an effort to save time and keep us alive. And because we only ever perceive what our brains feed us, we fall prey to these biases time and time again. Perception governs our world. Whether it is used knowingly, accidentally, or seldom at all, it is one of the greatest tools in the InfoSec toolbox.

Averting Accidents

"Accidents happen," certainly, but when working for a business that wants results twice as good in half the time, it hardly makes for an acceptable excuse when an employee falls for a phony email and winds up infecting half the network with a virus. Luckily, a lack of attention is easily and intuitively addressed through education, training, and no small amount of promotional merchandise. Training programs have been documented to reduce the risk of unintentional insider threat (UIT), and creating a culture of mindfulness within the workplace will help draw attention to good browsing habits (CERT, 2014). If a lack of attention or awareness is the main cause of unintentional insider threat, the immediate goal should be to draw attention to the problematic behaviors.

To further deter UIT, employees must perceive their careless activity as harmful to the organization, and, by extension, themselves. Reframing the organization's interests as being the individual worker's is a long-held, upstanding approach to encouraging desired behaviors. While fully harnessing a person's incredibly powerful intrinsic motivation ("I want this") remains out of reach, it is another matter entirely to attempt to convince someone that a behavior is in their best interest ("I should want this"). Doing so is hailed as one of the most effective ways to influence behavior (Carnegie, 1936), and InfoSec professionals can harness this approach in several ways. For example, promoting the idea that good employees practice good security incentivizes desirable habits in individuals who want to be exemplary workers. Framing desired organizational behaviors as beneficial to employees turns the activities from chores into self-rewarding habits.

While awareness posters and other promotional material reminding employees of acceptable organizational behaviors is certainly a step in the right direction, it loses its value if it is posted and then allowed to fallow. New additions to an environment tend to draw the eye, but once the mind has accepted an item (a poster, in this case) as part of the surrounding landscape, it is expected to be there, and thus is paid little attention, as the brain can and often does safely assume it will continue to occupy that space. Promotional material should therefore be cycled through on a regular basis, in order to keep the message of conscientiousness fresh in the minds of employees. With carefully-designed materials and a pointed effort to improve awareness, our accidental attackers stand a much better chance of recognizing and avoiding risky employee misbehavior.

Cooling Tempers

To prevent "hot malcontents" from figuratively (or perhaps literally) setting fire to an organization's assets, the goal is to expand the perception of belonging to the organization.

Since the aggression behind these types of insider attacks is fueled by the same mechanisms that react when an individual is faced with a threat to safety (the fight or flight-based sympathetic nervous system), the counteraction to best prevent such behavior would be to avoid triggering the system in the first place. Completely avoiding such arousal is beyond the scope of our ability, however, and as such we must again turn to crafting perception.

We tend to view antagonists as being either against us or for themselves, and it is in an organization's best interests to avoid the former. If an employee perceives that the organization is out to get them, he or she is probably much more likely to take news of their firing/demotion/layoff negatively than if the organization is simply struggling to survive. Framing any potentially upsetting firing decisions in the light of the organization trying to remain afloat may help in this regard. However, employers should hesitate before adopting an overly formal letter of discontinued employment, as this might be seen as a complete disregard for an employee's contributions to the company (Reina & Reina, 2015). Courtesy and appreciation are paramount in these tense situations. If there is no way to avoid conflict, though, it is advised that a close eye be kept on any vulnerable assets.

Luckily, patterns of aggression can often be traced throughout an individual's life, and an organization that conducts background checks on potential employees would do well to take any indications of such behavior into account. Rogue network administrator Terry Childs of San Francisco infamy, for example, spent time in prison for aggravated assault years before he seized control over the city's FiberWAN network (Venezia, 2008).

Deterring Opportunists

It must first be noted that there are some individuals who will resist deterrence by even the most proactive of organizational measures. However, several patters of risk behavior can be applied to insider threat scenarios, allowing for a better understanding of what factors might succeed in staving off cold opportunists. In the context of risks made for personal gain, perception is both a powerful player and a useful tool, especially considering the more complex and logically conceived behaviors in this category.

Psychologists David DeSteno and Piercarlo Valdesolo describe the manner in which violence against others is justified: through a dehumanization of the opposing force and a breaking down of the ways in which an individual can relate to their newfound enemy (DeSteno & Valdesolo, 2011). The enemy becomes "other," making them unlike ourselves and thus leaving no place for empathy, which is reserved for those whom we can relate to. This disconnect enables individuals to commit behaviors that would otherwise require a state of extreme emotional arousal to engage in. An individual can literally think themselves out of committing a morally reprehensible act—and do so quite often. This is a pattern that sees repetition throughout much of history, from colonial slavery to the Holocaust, and it is a longstanding testament to the power of perception.

Part of this is because of how perception mediates the relationship between risk behavior and outside environmental influences. Individuals who perceive their circumstances as undesirable repeatedly tend to underestimate the risks of their decisions (Sitkin & Pablo, 1992). To rephrase in the context of cyber security, an unhappy employee who has more to gain by abusing their access for fraudulent purposes is more likely to view the risks of engaging in such behavior as less than they actually are, thus increasing the chances of an insider incident. One approach to combating this would again be to pay careful attention to fostering a strong, united workplace. The majority of activities that break workplace trust are small incidents that accumulate over time, so an effort to ensure that emails are responded to promptly, appropriate employees are consulted for their opinions, and staplers are not stolen can help dissipate some of the damage done to trust in the workplace (Reina & Reina, 2015).

Visibly flaunting the organization's InfoSec department could also potentially help deter cold opportunists by promoting the perception of the organization's systems as well-guarded. Since attacks in this category are made without the hotheaded sympathetic arousal of Hot Malcontents, reason plays a much larger role in the decision to attempt to turn against one's employer. If the organization frequently advertises the fact that their assets are carefully maintained, the risks of being caught may very well outweigh the potential advantages to be gained from fraud or thievery. Subtly flaunting the strength of an organization's security can have other benefits, too—a CISO can cultivate an image through normal, awareness-promoting activities within the business. Practicing good security therefore doesn't only increase within-organizational awareness, it can deter insiders and help create a better working environment as well.

CONCLUSIONS

While neuropsychology and other brain-related subjects may still seem like a distant, laboratory-limited field of study, it is currently rapidly expanding. This era has been dubbed "The Century of the Brain" by many a scientist, and understanding how neurophysiological pathways influence and play into the behaviors we encounter every day can give twenty-first century businesses an edge. Though the field of applied neuropsychology could stand more attention, the secrets of human behavior are nevertheless being slowly unraveled, and it is up to the InfoSec professionals of the future to weave these new understandings into our organizations.

As it applies to insider threat, neuropsychology can help further define and classify employee misbehavior and insider deviant behavior into physiologically-rooted categories. While accidental attackers unintentionally expose their organization through any number of careless misbehaviors, deviant behaviors house the more malevolent, aggression-related attacks. Neurologically hot malcontents react to negative events with the intent to destroy organizational property, while the category of cold opportunists allows for a separation of aggressive events in which the employee holds his or her personal interests as the highest priority rather than the destruction of the organization.

Armed with a better understanding of how employees are psychologically able to pose a threat to their employer, CISOs may take another step on the long road toward a broader utilization of modern understandings of human behavior. Psychology and management are tightly intertwined. This will only become truer as our knowledge of both fields expands.

ACKNOWLEDGMENTS

Many thanks to Dr. Whitman for his helpfulness, and to the KSU Conference on Cybersecurity Education, Research and Practice for the opportunity to submit undergraduate research.

REFERENCES

Aiello, J. R., & Kolb, K. J. (1995). Electronic performance monitoring & social context: Impact on productivity & stress. *Journal of Applied Psychology, 80*(3), 339-353.

Ax, A. F. (1953). The physiological differentiation between fear and anger in humans. *Psychosomatic Medicine, 15*(5), 433-442.

Carlson, N. R. (2013). Emotion. In *Physiology of Behavior* (347-400). Edinburgh Gate, Harlow: Pearson.

Carnegie, D. (1936). *How to win friends and influence people*. D. Carnegie and A. R. Pell. New York, NY: Pocket Books.

CERT Insider Threat Center (2014). Unintentional insider threats: Social engineering. Technical Report. CERT Division.

Chen, Z., Lam, W., & Zhong, J. (2012). Effects of perceptions on LMX and work performance: Effects of supervisors' perception of subordinates' emotional intelligence and subordinates' perception of trust in the supervisor on LMX and, consequently, performance. *Asia Pacific Journal of Management, 29*(3), 597-616.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2012). Future directions for behavioral information security research. *Elsevier Computers & Security, 32*, 90-101.

de Dominique J. F. Q., Fischbacher, U., Treyer, V., Schellhammer, M., Schnyder, U., Buck, A., & Fehr, E. (2004). The neural basis of altruistic punishment. *Science, 305*(5688), 1254-1258.

DeSteno, D., & Piercarlo V. (2011). *Out of character*. New York, NY: Crown Publishers.

Dockery, T. M., & Steiner, D. D. (1990). The role of the initial interaction in leader-member exchange. *Group and Organization Studies, 15*, 395–413.

Filkins, B., & Hardy, G. M., (2016). *IT security spending trends.* Technical Report: SANS Institute.

Gallagher, S. (2014, September). Home Depot's former security architect had history of techno-sabotage. *Ars Technica*.

Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014). Classificatiopn of security threats in information systems. *Procedia Computer Science, 32*, 489-496.

Jouini, M., Rabai, L. B. A., & Khedri, R. (2015). A multidimensional approach towards a quantitative assessment of security threats. *Procedia Computer Science, 52*, 507-514.

Kendall, S. (2007, November). Admin to plead guilty in theft of 8.5M records from database. *CSO Online*.

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly, 16*(2), 173-186.

Ponemon Institute LLC (2011). *Reputation impact of a data breach*. Executive Summary: Experian Data Breach Resolution.

Reina, D., & Reina, M. (2015). *Trust and betrayal in the workplace* (3rd ed.). Oakland, CA: Berrett-Koehler Publishers, Inc.

Sitkin, S. B., & Pablo, A. L. (1992). Reconceptualizing the determinants of risk behaviour. *Academy of Management Review, 17*(1), 9-38.

Software Engineering Institute (2013). *US state of cybercrime survey: How bad is the insider threat?* PowerPoint slides: Carnegie Mellon University.

Venezia, P. (2008, July). Why San Francisco's network admin went rogue. *InfoWorld*.

Verizon (2016). *Data breach investigations report*. Technical Report.

Vormetric Data Security (2015). *Vormetric insider threat report: Trends and future directions in data security global edition.* Technical Report.

Willison, R. & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly, 37*(1), 1-20.