54

Behavioral Information Security Management

54.1 Introduction

Modern organizations’ critical dependencies on information assets have resulted in information security being included among the most important academic research issues within the field of information systems (IS) (Dhillon and Backhouse, 2000; Kankanhalli et al., 2003). The massive amounts of information assets being created every day require management and protection. Technical, administrative, and behavioral controls must be implemented to protect information as it is created, captured, stored, and transmitted. Information at each of these four states of information is vulnerable to security threats. Technical controls, such as firewalls, port scanning, automated backups, intrusion detection systems (IDS), and anti-malware software have introduced significant safeguards against external human perpetrators of security threats, but various human behaviors, especially those of organizational insiders, continue to pose the greatest risk to the security of IS and continue to be cited as the greatest challenge for security practitioners (Davis, 2012; Willison and Warkentin, 2013).

The four goals of the management and protection of information assets are to ensure their confidentiality, integrity, availability, and accountability throughout the organization (Siponen et al., 2006; Stanton et al., 2005; Warkentin and Johnston, 2006, 2008). An information asset’s confidentiality is maintained by controlling the methods of disclosure within and beyond the organization. The availability goal is maintained by ensuring that only those individuals authorized to access an information asset are afforded such access only when and where it is required. The maintenance of the integrity of an information asset is achieved through use of controls that restrict asset alterations or deletions. Last, the goal of accountability, more formally known as nonrepudiation, is the assurance that an electronic “paper trail” exists and precludes the denial of transaction occurrences or of the actions of any individual.
Achieving information security within an organization requires development of policies and procedures, followed by their successful implementation (Warkentin and Johnston, 2006, 2008). The information security policies (ISPs) specific to the needs of an organization are developed using the information security goals as a framework. Both formal and informal policies should be aligned with the overall organizational policies and strategies. Procedures and performance standards necessary to support the ISP must be developed and will include specification of the mechanisms and methods for implementation. Finally, the ISPs are put into practice through implementation of the procedures. Employees are informed of the ISP and achieve an appropriate level of understanding of the ISP through information security education, training, and awareness (SETA) campaigns, discussed later.

The various sources and types of threats to information security may be categorized, as shown in Figure 54.1, into internal and external threats and further subdivided into human and non-human threats (Loch et al., 1992; Willison and Warkentin, 2013). Information security and therefore information security research typically focuses on either a technical or behavioral viewpoint (Bulgurcu et al., 2010; Tsohou et al., 2008). The non-human threats that exist include potential events that may occur internally such as equipment failure or events due to external forces such as natural disasters. Human threats in the form of computer hackers or corporate spies are commonly seen in news media headlines (Willison and Siponen, 2009) and as favorites of cinematic thrillers, likely making these external threats the most well known. These external human threats can be subdivided into three categories of perpetrators, any of which may cause harm to the organization, but each fueled by a different intent.

The first category of perpetrators within the external human threat is made of individuals believed to be fueled by curiosity, boredom, and the need for notoriety. These individuals are known as script kiddies, a derogatory term for those who seek out system vulnerabilities to exploit by using software tools, or scripts, developed by others and whose antics are typically considered unsophisticated or childish (Vamosi, 2002; Wlasuk, 2012). Although there is no specific age restriction to be considered a script kid, they are typically young but are still quite capable of causing great harm. They have been known to have gained unauthorized access to networks and computer systems, built botnets, and committed web tagging, an electronic form of graffiti.

<table>
<thead>
<tr>
<th>Sources</th>
<th>Perpetrators</th>
<th>Intent</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Internal</strong></td>
<td>Human (Employees, other insiders)</td>
<td>Passive, non-volitional non-compliance (Unintentional actions, accidental data entry, forgetful oversights, uninformed violations)</td>
</tr>
<tr>
<td></td>
<td>Non-human (Hardware failure, dust, power surges, leaks)</td>
<td>Volitional (but not malicious) non-compliance (Failing to log off when leaving PC, delayed backups, not changing passwords regularly)</td>
</tr>
<tr>
<td><strong>External</strong></td>
<td>Human (Hackers, espionage)</td>
<td>Intentional, malicious (harmful) computer abuse (Sabotage, data theft or corruption, embezzlement, fraud, deliberate policy violations)</td>
</tr>
<tr>
<td></td>
<td>Non-human (Natural disasters, malware, power failures, telecomm failures)</td>
<td>Curiosity, boredom, notoriety (Script kiddies)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Financial gain (Identity thieves, organized crime)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Activism, covert operations ('Hacktivists,' government intelligence)</td>
</tr>
</tbody>
</table>

FIGURE 54.1 IS security threat vector taxonomy.
The second category of external human threat perpetrators is made of individuals fueled by the promise of financial gain. These perpetrators have become quite sophisticated and use social engineering methods such as phishing and other forms of deception and psychological techniques to commit fraudulent acts such as theft of intellectual property or of identity theft (Wright and Marett, 2010). These cybercrimes may be committed by individual humans or by members of organized crime syndicates (“Who commits the crime,” n.d.). By virtue of the capabilities of the World Wide Web and the Internet, the perpetrators of these crimes can be anywhere in the world, adding to the complexity of their identification and difficulty in punishing them if they are caught.

The last category of perpetrators within the external human threat is made of individuals whose intent is that of activism or covert operations performed by governments. The most well-known perpetrators within this category is the “hactivist” group, Anonymous, who became known to the world in early 2008 when they staged a protest against the Church of Scientology after YouTube was ordered by the church to remove an internal video they claimed was copyrighted (Schwartz, 2012). Since that date, members of Anonymous have been involved in numerous protests and attempts to expose wrongs in the world and have evolved into a culture (Norton, 2011).

Though maintenance of organizational security relies upon employee compliance with ISP, the threats from non-human sources and from humans external to the organization are primarily addressed through maintenance programs and business continuity plans that leverage technological controls such as firewalls and IDS (Cavusoglu et al., 2009), biometrics (Ballard et al., 2007), and encrypted logins (Boncella, 2002). Hardware failures (a prime non-human threat to security) are addressed through both technical and behavioral controls (Malimage and Warkentin, 2010). A great deal of time, effort, and financial resources are spent on protective efforts against these threats, yet research shows that the internal human threat may cause the most harm and be the most difficult to guard against (Doherty and Fulford, 2005; Straub and Welke, 1998; Warkentin and Johnston, 2006; Warkentin and Willison, 2009).

The internal human perpetrators category in Figure 54.1 includes those threats to information security that come from a group of individuals who already have access to the information assets of the organization and are therefore known as the “insider threat.” Research in information security (InfoSec) addresses antecedents of and issues related to individual compliance and noncompliance with and criminal violation of IS security policies and procedures. The InfoSec performed to date is the focus of this chapter. We begin with a definition of the term insider threat and a brief discussion of the employee intent continuum shown in Figure 54.1. A review of the theories, methods, and measures used by researchers in this area of study today follows, and the chapter concludes with recently identified major information security research issues and need for future study.

### 54.2 Information Security Research: The Insider Threat

Who is the insider? Organizational boundaries are dynamic, fluid, and often poorly defined. In the age of the virtual organization and inter-organizational global collaborative teams, many individuals may have access to trusted information resources. In the context of our investigation, there are two essential aspects of an insider: (1) insider access and (2) deep familiarity with organizational processes.

First, the insider must be an individual who has access to information resources not typically provided to the “outsider” (all others in the general public). These resources include systems and their data/information. While this category of individual is typically instantiated as an employee, it should be recognized that he or she may also be a contractor, a virtual partner (supply chain partner or strategic alliance partner with access to resources), or even a constituent who is a customer or other client (e.g., student, medical patient, etc.), provided they have some level of insider privileges. Essentially, the insider is an individual who can easily operate “behind the firewall” who has proper authentication
via password or other methods.* This person is thought of as a trusted member of the organization. It should also be recognized that organizations have numerous categories of trusted individuals and use “role-based security” mechanisms to afford greater or lesser control to various individuals based on their respective roles. These may be thought of as concentric circles of access, but with overlap, according to one’s need for access.

Second, insiders not only have access to and often control of systems and information, but they also are individuals who have a deep knowledge of their organizations’ critical processes because of their dynamic involvement and experiences with these processes. Though this relationship may also exist between companies and their partners, this context is best typified by the employer–employee relationship. In this context, organizational policies and procedures may have an impact on the insider. Organizations seek to hire trustworthy employees. Firms implement SETA programs to train their employees in the use of proper actions and behaviors to ensure compliance with security policies. Managers may also utilize persuasive communications, such as fear appeals (Johnston and Warkentin, 2010), to encourage compliant protective behaviors. Sanctions may also be targeted against noncompliant employees as a deterrent (D’Arcy et al., 2009). Furthermore, the policies and actions of organizational managers can have a strong impact on the psychological perceptions of the employees, as well as their subsequent thought processes that may lead to various actions. Finally, these same principles apply also to former employees, customers, and partners, who often retain insider access and process knowledge and thus can pose continued threats even after the relationship is terminated or expired. The same factors that can influence insiders, presented in our three propositions, can continue to influence former employees. A recent survey of nearly 1900 firms from all major industries and from all over the globe found that 75% of respondents revealed their concern with the possible reprisal from employees recently separated from their organization (Ernst and Young, 2009).

Though extensive evidence suggests that insiders pose the greatest risk to information security (Brenner, 2009; CSO Magazine, 2007; Ernst and Young, 2009; Loveland and Lobel, 2010; Ponemon Institute, 2010; Richardson, 2011; Smith, 2009), many firms continue to spend the lion’s share of their time, effort, and budget on perimeter security measures, such as firewalls, IDS, encryption of transmissions, anti-malware software, and content filtering, all of which aim to keep outsiders (e.g., hackers) or other external entities (e.g., malware) from penetrating the perimeter and threatening the organization’s information resources. Though a certain degree of this focus is mandated by various regulations (Warkentin et al., 2011a), this allocation of resources is not entirely justifiable.

Behaviors that may result in harm to the organization are often unintentional. Prevention of these behaviors requires that employees be provided with knowledge regarding the behavior expected of them. This requirement is typically addressed through the development and implementation of ISP (Bulgurcu et al., 2010; Karjalainen and Siponen, 2011; Siponen and Vance, 2010; Thomson and von Solms, 1998). To further ensure employee compliance, information security instruction is often performed to explain the policies and achieve an understanding by employees regarding secure behavior (Puhakainen and Siponen, 2010; Siponen, 2000; Siponen and Iivari, 2006; Warkentin and Johnston, 2006; Warkentin et al., 2011a). However, employee compliance with ISP continues to be among the top concerns of organizations (Bulgurcu et al., 2010; D’Arcy and Hovav, 2009; Dodge et al., 2007; Kaplan, 2010; Loveland and Lobel, 2010; Prince, 2009). Therefore, information security research explores the typical controls used by organizations to encourage secure behaviors, such as SETA programs (D’Arcy et al., 2009; Furnell et al., 2002; Peltier, 2005; Wilson and Hash, 2003), development of acceptable use policies (Doherty et al., 2011; Ruighaver et al., 2010), and use of deterrence programs (D’Arcy et al., 2009; Straub and Welke, 1998).

* Security practitioners utilize access methods that require “something you know” (passwords, PINs), “something you have” (badges, cards, fobs), and/or “something you are” (biometric signatures such as fingerprints). So-called two-factor authentication is deemed better than methods that employ only one of these three.
Research of this nature historically looked at employee behaviors with the assumptions being that any unsecure behaviors were the result of non-malicious actions on the part of the employees. This assumption has changed over the past few years to include intentional and malicious actions. A continuum of employee intent as illustrated in Figure 54.1 has been identified and broadened the area of information security study.

On the upper end of the continuum, employee intent is passive and, on the whole, behavior is considered secure. The majority of the original insider threat research conducted would reside on this end as it focused on errors or misunderstandings as the underlying cause of unsecure actions or breaches in security. These types of unsecure behaviors may be corrected through improved information security instruction. In the middle of the continuum are intentional (but not malicious) acts and volitional behaviors such as choosing to not log off when leaving a PC unattended or to write down a password. These types of unsecure behaviors may be addressed through persuasion, deterrence, or other forms of behavioral controls. The lower end of the continuum includes intentional behaviors such as theft, embezzlement, and other deliberate actions. These behaviors are no longer benign in their intent and are committed for malicious reasons and or personal gain and are included in the category of crimes known as cybercrime.

The remainder of this manuscript identifies some theoretical tools for exploring InfoSec, along with a very brief assessment of the methods that have been used.

### 54.3 Theories Applied to Behavioral Information Security Research

The field of IS frequently adapts theories from other fields as is also the case with information security research. The majority of the research to date draws upon a small set of behavioral theories that originated primarily in the fields of psychology, sociology, communications, and criminology. These theories are listed in Table 54.1 along with a brief description and the primary literary sources for each.

Figure 54.2, generated by a word cloud software assessment of the key articles published in the area of IS security behaviors, provides a visual representation of the theories used to investigate such behaviors.

#### 54.3.1 Deterrence Theory

Deterrence theory, commonly called general deterrence theory (GDT) though there are distinctions between general and specific deterrence that we will not address here, is identified as the theory most commonly applied in IS research (D’Arcy and Herath, 2011; Siponen et al., 2008). GDT provides the theoretical foundation necessary to explore and explain ISP compliance issues and IT abuse or misuse issues. Its foundation is the “rational choice model” of human behavior that posits that individual decisions are influenced by the fundamental motivation to apply a rational calculus of maximizing pleasure and minimizing pain. The assumption is that individuals will make behavioral choices based on the potential risks or costs and the potential gains or benefits, with the choice to act hinging on the balance between them. If the benefits are sufficiently large, a person may be willing to assume the risks or costs; but if the costs are sufficiently large, it will deter the behavior in question. Societies impose deterrence measures (costs of actions) in the form of punishments (fines or imprisonment) for illegal acts, whereas organizations impose deterrence measures against policy violations in the form of formal workplace sanctions, such as reprimands, demotions, withholding raises, or termination. These imposed costs are intended to discourage unwanted behavior. The theory states that if sanctions are in place, individuals will make a rational choice through the assessments of the likelihood of being caught (perceived sanction certainty), the harshness of the sanction or punishment (perceived sanction severity), and the speed with which the sanction may be carried out (perceived sanction celerity).
### TABLE 54.1 Theories Used in Behavioral Research in Information Systems Security

<table>
<thead>
<tr>
<th>Theory</th>
<th>Description</th>
<th>Primary Sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>General deterrence theory (GDT)</td>
<td>GDT states that individuals will weigh and balance the risks and gains associated with their actions and will consider the certainty, severity, and celerity of sanctions that exist to discourage the behavior</td>
<td>Gibbs (1975)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Straub and Welke (1998)</td>
</tr>
<tr>
<td>Rational choice theory (RCT)</td>
<td>RCT states that individuals will make behavioral choices based on balancing the risks and gains of the choices available, and the level of magnitude of the risks and the gains are calculated through subjective individual assessment</td>
<td>Paternoster and Simpson (1996)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>McCarthy (2002)</td>
</tr>
<tr>
<td>Neutralization theory (NT)</td>
<td>NT states that individuals will use neutralization techniques to justify choices to perform behaviors even when the behaviors are not secure or are against policy</td>
<td>Sykes and Matza (1957)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Klockars (1974)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Minor (1981)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Benson (1985)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cressey (1989)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Siponen and Vance (2010)</td>
</tr>
<tr>
<td>Protection motivation theory (PMT)</td>
<td>PMT states that individuals will process fear appeals (persuasive messages) by performing a threat appraisal (severity and susceptibility of a threat) and a coping appraisal (response efficacy and self-efficacy), which will result in protection motivation behaviors</td>
<td>Rogers (1975)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maddux and Rogers (1983)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Floyd et al. (2000)</td>
</tr>
<tr>
<td>Extended parallel process model (EPPM)</td>
<td>Related to PMT, the EPPM states that individuals, when presented with a high threat message, may become overwhelmed and will not develop protection motivation behaviors to respond to the threat but instead will develop avoidance behaviors and ignore or reject the threat</td>
<td>Witte (1992)</td>
</tr>
<tr>
<td>Elaboration likelihood model (ELM)</td>
<td>ELM states that individuals will process messages via a direct or peripheral route. A message processed via the direct route is more likely to result in stable and predictable outcomes whereas messages processed via the peripheral route are more likely to result in unstable and short-lived outcomes. A receiver’s lack of personal involvement in the message topic and the availability of message cues may encourage peripheral route processing</td>
<td>Petty and Cacioppo (1986b)</td>
</tr>
<tr>
<td>Information manipulation theory (IMT)</td>
<td>IMT states that when individuals participate in a conversation, a message sender may deceive the other party, the receiver, through the subtle alteration(s) of one or more of the four main components of a message, namely the quantity, quality, clarity, or relevance of the message. The receiver of the message may be deceived if he or she does not detect the alteration(s)</td>
<td>McCornack (1992)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>McCornack et al. (1992)</td>
</tr>
<tr>
<td>Interpersonal deception theory (IDT)</td>
<td>IDT suggests that a sender knowingly wishing to deceive a receiver may strategically insert false information in the course of a conversation. The receiver will judge the credibility of the message and as long as no deception is detected the conversation may continue with the deceiver interactively adjusting the message as needed to remain undetected.</td>
<td>Buller and Burgoon (1996)</td>
</tr>
<tr>
<td>Equity theory (ET)</td>
<td>ET addresses human perceptions regarding inequality in social exchanges. The application of ET within organizational settings is known as distributed justice</td>
<td>Adams (1965)</td>
</tr>
<tr>
<td>Social cognitive theory (SCT)</td>
<td>Best known as the theory behind the self-efficacy construct, SCT provides a framework by which human behaviors may be predicted and explained through relationships between individuals and the environment</td>
<td>Bandura (1977)</td>
</tr>
</tbody>
</table>
The original form of GDT included only formal sanctions that carried legal consequences such as criminal penalties or civil lawsuits (analogous to workplace punishments). Theories about informal sanctions that were introduced by later scholars included those sanctions attributed to societal norms, such as guilt, shame, embarrassment, and social influence (Vance and Siponen, 2012). When moral individuals consider a deviant act, the mere thought of disapproval by one’s peer group may deter the commission of the act, and thus informal sanctions likely play a very significant deterrence role, but they remain a largely unexplored antecedent of behavior in the InfoSec context.

The seminal work by Straub (1990) applied GDT within the field of IS and argued that the investments in information security must be balanced with the level of potential information asset risks. The focus was on the intentional human abuses and the common controls to discourage such abuses that were available at the time. The evolution of GDT and its use within IS saw the theory combined with Simon’s managerial decision-making model to create the security action cycle (Straub and Welke, 1998), which became what is now the foundation for numerous information security research studies.

The security action cycle combines the generally accepted four stages of system risk reduction and identifies strategies for each where managers may implement security controls to reduce insider computer abuse (Straub and Welke, 1998). Security controls should first focus on deterrence, discouraging employees from performing unapproved, undesirable, and noncompliant behaviors. The goal is to minimize abuse; but if deterrence fails, the organization should implement prevention measures that inhibit risky employee behaviors that may bring harm to the organization’s systems. Third, detection should be implemented in cases where employees are not deterred or prevented from behaving in an insecure manner. Last, remedies should be implemented to enable recovery from any harm that may result from an employee’s insecure behavior, as well as punishment of the employee him/herself. GDT tells us that when the risk of being caught and punished outweighs the benefit of the action, individuals will refrain from performing the risky behavior. With this in mind, managers are encouraged to stress the deterrence and prevention security control implementation stages (Shropshire et al., 2010). The security action cycle has been recently expanded by Willison and Warkentin (2013) to look further back in time at the earliest motivations for workplace computer abuse, such as perceptions of organizational injustice, neutralization factors, and expressive motivations for committing abuse.

Information security studies focusing on the deterrence and prevention stages of the security action cycle often apply GDT toward assessing the effectiveness of various methods of information security control.
security controls. These controls, termed “security countermeasures” (Straub and Welke, 1998), include both technical methods such as restricting system access through software authorization and behavioral methods such as implementation of SETA programs. While these studies find GDT to be useful overall, inconsistencies across study findings have led researchers to explore additional issues to better explain the effectiveness of security controls. For example, factors specific to an organization such as industry type, company size, and management support were explored and found to be important considerations toward security effectiveness perceptions (Kankanhalli et al., 2003).

Another study explored how the deterrent effectiveness of security countermeasures may be affected by the employees’ awareness of the countermeasures (D’Arcy et al., 2009). Awareness was found to have a significant impact particularly through the perceptions of severity and certainty of the sanctions. The level of the employee’s morality was also found to play a significant part in how sanctions are perceived (Dinev and Hu, 2007; Shropshire et al., 2012).

54.3.2 Rational Choice Theory

The most serious threats to information security assets may be classified as criminal acts. However, crimes committed within the workplace differ significantly from those upon which theories of criminology were based. The rational choice Theory (RCT) extends GDT and deterrence theory to be applied more generally toward the explanation of individual behaviors by noncriminals within the workplace (Paternoster and Simpson, 1996) and as such has been applied by IS researchers in the context of information security.

The assumption of RCT is that the choice to commit an offense requires that an individual perform an assessment of benefits and costs. When an individual determines that his or her perception of the benefits outweighs his or her perception of the costs, the choice to offend is more likely to be made. When applied to the context of employees and potential offenses committed within an organization, other factors such as business practices and culture are likely to influence the actions taken by individuals (Sabherwal and Robey, 1995). Therefore, perceived costs and benefits assessed may include those for the individual as well as for the employer. Furthermore, costs and benefits may be tangible, intangible, formal, and informal. The moral beliefs of an individual are also believed to be a strong contributing factor within RCT, with individual behaviors more strongly influenced by morality than by any fear of perceived sanctions (Paternoster and Simpson, 1996).

Although RCT’s origins suggest an appropriate fit in the area of information security, IS researchers have only recently applied it within an information security context. For example, the costs and benefits of ISP compliance and costs of ISP noncompliance were the focus of a recent study that found RCT significantly explained the effects of an employee’s beliefs regarding ISP compliance on the employee’s secure behaviors (Bulgurcu et al., 2010). The assumption that moral beliefs are a significant predictor of an individual’s behavior was supported within the context of information security (Hu et al., 2011). Along with moral beliefs, the effect of employee self-control was also explored and found that those with low self-control were more likely to commit noncompliant acts when the benefits were perceived to be higher than the perceived costs. In yet another study, once again moral beliefs were found to be significantly related to secure behavior choices, along with perceived benefits (Vance and Siponen, 2012) with higher moral beliefs positively related to ISP compliance intention and higher perceived benefits negatively related to ISP compliance intention.

54.3.3 Neutralization Theory

While GDT has been widely applied across information security studies, inconsistent results have been found and the explanation may lie with the neutralization theory (NT) (Benson, 1985; Cressey, 1989; Sykes and Matza, 1957). NT states that regardless of the values and norms to which an individual subscribes, a process to neutralize, or justify, breaking a rule may be performed when the individual desires
Behavioral Information Security Management

54.3.4 Protection Motivation Theory

The study of persuasion and its effects on individual behavior has recently gained popularity with information security researchers in the field of IS. The use of persuasive messages known as fear appeals and the resulting effects of the messages on the attitudes and behaviors of individuals first gained the interest

<table>
<thead>
<tr>
<th>Technique</th>
<th>Description</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appeal to higher loyalties</td>
<td>An act may be justified when the individual perceives that the act is required for those to whom he or she is loyal or must protect (family, friends)</td>
<td>Sykes and Matza (1957)</td>
</tr>
<tr>
<td>Condemnation of the condemners</td>
<td>An act may be justified when the individual perceives that those who condemn the act should themselves be condemned</td>
<td></td>
</tr>
<tr>
<td>Denial of injury</td>
<td>An act may be justified when the individual perceives that no one was injured by the act</td>
<td></td>
</tr>
<tr>
<td>Denial of responsibility</td>
<td>An act may be justified when the individual perceives that committing the act is beyond his or her control</td>
<td></td>
</tr>
<tr>
<td>Denial of the victim</td>
<td>An act may be justified when the individual perceives that the act is a form of retaliation or that the party being injured deserves to be injured because he or she harmed others first</td>
<td></td>
</tr>
<tr>
<td>Metaphor of the ledger</td>
<td>Individuals rationalize their misdeed by pointing to the many good deeds (or compliance) they have done in the past</td>
<td>Klockars (1974)</td>
</tr>
<tr>
<td>Defense of the necessity</td>
<td>Required actions, have no choice</td>
<td>Minor (1981)</td>
</tr>
<tr>
<td>Avoidance of greater harm</td>
<td>Various justifications</td>
<td>Garrett et al. (1989)</td>
</tr>
<tr>
<td>Comparative standards</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Legal rights</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malicious intentions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Claim of entitlement</td>
<td>Other rationalizations, some similar to earlier forms</td>
<td>Coleman (1994)</td>
</tr>
<tr>
<td>Defense of the necessity of the law</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Claim of individuality</td>
<td>Various justifications</td>
<td>Henry and Eaton (1994)</td>
</tr>
<tr>
<td>Claim of relative acceptability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Justification by comparison</td>
<td>Individuals justify committing the act because it is less harmful than other acts that could be just as easily committed</td>
<td>Cromwell and Thurman (2003)</td>
</tr>
<tr>
<td>Postponement</td>
<td>In order to commit the act, individuals put off any thoughts of wrong right or of guilt feelings about committing the act</td>
<td></td>
</tr>
</tbody>
</table>

Source: Adapted from Willison, R. and Warkentin, M., MIS Quarterly, 37, 1, 2013.

the outcome believed to be attainable by performing the action (Siponen and Vance, 2010). The use of neutralization techniques may explain why individuals behave in an unsecure manner and risk harm to organizational assets. The theory originally proposed that five neutralization techniques exist (Sykes and Matza, 1957) and included denial of responsibility, denial of injury, denial of the victim, condemnation of the condemners, and appeal to higher loyalties. A sixth technique, the metaphor of the ledger, was added about 20 years later (Klockars, 1974) and a seventh, the defense of necessity, was added soon after that (Minor, 1981). Several other neutralization techniques have been identified and are listed in Table 54.2 with the original five techniques with a brief description of selected entries.
Managing and Securing the IT Infrastructure and Systems

of researchers in the field of psychology during the 1950s (Janis and Feshbach, 1953, 1954). The numerous research projects produced findings that indicated further research was worthwhile, but the explanations of the findings lacked a cohesive theory until 1975 when the protection motivation theory (PMT) was developed (Rogers, 1975). In the years following, researchers in other fields such as communications (Witte, 1992), health care (Kline and Mattson, 2000), marketing (Dillard and Anderson, 2004), and IS security (Anderson and Agarwal, 2010; Herath and Rao, 2009; Johnston and Warkentin, 2010) continued the exploration of the ability of fear appeals to stimulate the appropriate level of fear or concern about an event and change individual attitudes or behaviors. Fear appeals have been shown to be effective in encouraging individual behaviors in the areas of health promotion, societal defense, and information security.

The PMT states that when individuals are exposed to a fear appeal, two cognitive mediating processes will ensue and protection motivation behavior will result. The cognitive mediating processes are the appraisal of the threat and the appraisal of the individual’s capacity to cope with the threat. Threat appraisal includes the constructs of perceived threat severity and perceived threat susceptibility. Coping appraisal includes the constructs of perceived response efficacy and perceived self-efficacy. For the fear appeal message to be effective, it must include appropriate details regarding the threat and the recommended response to a threat, specifically that the threat is severe and is likely to occur, and a response that works is available and can be successfully performed (Maddux and Rogers, 1983; Rogers, 1975). When exposed to a fear appeal message, individuals perform threat and coping appraisals, and the individual’s perception of the level of threat severity, threat susceptibility, response efficacy, and self-efficacy will affect the level of protection motivation behavior developed. If the threat is perceived to be serious and likely to occur, the recommended response is perceived to be effective against the threat, and the receiver believes he or she is capable of successfully performing the response, motivation toward protective behavior will result.

PMT has been applied in several contexts within the area of information security. Findings in most studies indicate use of PMT is effective toward explaining information security phenomena, but the findings have not been consistent across all contexts. For example, numerous information security threats exist with online activities such as sharing information on social networking sites, participating in blogging, and frequenting any password-secured website (Banks et al., 2010; LaRose et al., 2005, 2008; Marett et al., 2011; Zhang and McDowell, 2009). In the context of social networking, individuals’ decisions whether to share personal information were influenced most by the threat appraisal variables (Marett et al., 2011) along with social influence (Banks et al., 2010). Alternately, when considering overall online safety, the greater influence was found to be self-efficacy and response efficacy (LaRose et al., 2008). Similarly, self-efficacy and response efficacy were found to be strong influences toward online account password management intent along with a strong negative relationship between response cost and intent to implement strong passwords (Zhang and McDowell, 2009).

Other areas of information security research with PMT include explorations of general secure computing practices (Anderson and Agarwal, 2010; Ng et al., 2009; Woon et al., 2005; Workman et al., 2008) and anti-malware software use (Garung et al., 2009; Johnston and Warkentin, 2010; Lee and Larsen, 2009; Liang and Xue, 2010; Stafford and Poston, 2010). Application of PMT within these contexts has also produced varied results. For example, social influence, self-efficacy, and response efficacy were found to be the strongest influences of intent to use anti-malware software in one study (Johnston and Warkentin, 2010). Another study found that threat severity, self-efficacy, and response efficacy were significant indicators of software use, and also found that threat vulnerability and response costs produced no significant contributions (Garung et al., 2009). Particularly interesting results have been found as well, such as relationships between threat severity and self-efficacy and threat severity and response efficacy (Johnston and Warkentin, 2010), two relationships that are generally not tested in PMT-based information security research.

Another common information security threat is related to the great amounts of data being generated each day and the threat of losing the data at any time. A simple response to this threat is to perform data backups. Self-efficacy and response efficacy were found to be positively related, and threat susceptibility
and severity were found to be negatively related to performing data backups (Crossler, 2010). Another study, however, found that only threat severity, response efficacy, and self-efficacy were strong indicators of behavioral intent (Malimage and Warkentin, 2010).

PMT research in the context of information security has produced different and varied findings as compared to the prior PMT research in contexts such as health care and marketing. Constructs that are not included in prior PMT research have shown to be strong indicators of secure behavior intent within an information security context, suggesting that the PMT model may require expanding to better fit this context. For example, social influence has been found to be highly significant toward influencing security behaviors (Johnston and Warkentin, 2010; Pahnila et al., 2007a) and descriptive norms have been found to be particularly important in influencing protective behaviors against a collective threat, with subjective norms found to be influential against individual threats (Anderson and Agarwal, 2010).

### 54.3.5 Extended Parallel Process Model

At times, research has found that certain fear appeals may not produce adaptive (protection motivation) behaviors, but instead produce maladaptive behaviors. A theory developed to explain such results is the extended parallel process model (EPPM) (Vroom and von Solms, 2004; Witte, 1992). EPPM states that fear appeal theories assume message acceptance and therefore only explain behaviors that result from acceptance of the persuasive message. For example, when the threat appraisal is high and not properly balanced with a high coping appraisal, an individual may become overwhelmed by the threat and choose to reject the persuasive message and develop maladaptive avoidance behaviors rather than adaptive protection motivation behaviors. In these unbalanced cases, rather than achieving the intended outcome of the message with acceptance of the persuasion and ensuing adoption of protection motivation behaviors, the outcome may be defensive avoidance where the individual responds by avoiding the appeal by choosing to ignore the message or avoid thinking about the threat. Or it may be reactance where the individual negatively reacts to the appeal, choosing instead to behave oppositely in a phenomenon called the “boomerang effect.” In either case, individuals with insufficient coping levels, either response efficacy (“it won’t work”) or self-efficacy (“I can’t do it”), will exhibit undesirable maladaptive responses that manage the fear itself, rather than the threat. Message rejection is a common phenomenon in which a user suggests that the message is not valid and that the threat is not severe. In the context of information security threats, a user may suggest that reports about viruses are overblown and he or she should not worry about them (“head in the sand” reaction). Or the message recipient may reject the messenger, discrediting the validity of the appeal. EPPM, like PMT, also states that when presented with a fear appeal, an individual will perform two message appraisals. However, rather than the appraisals being those of threat and coping as in PMT, EPPM describes a cognitive process to determine the danger control (which includes threat and coping appraisals) and an emotional process to determine the fear control (Vroom and von Solms, 2004; Witte, 1992).

### 54.3.6 Elaboration Likelihood Model

A theory that addresses the cognitive processes that individuals perform when presented with information is the elaboration likelihood model (ELM) (Petty and Cacioppo, 1986a,b). The theory states that there are two possible routes from which individuals will choose to process a message: the central route and the peripheral route. The general goal of a persuasive message is to achieve a long-term change in the attitude or behavior of an individual. When a message is processed by way of the central route, a more predictable and stable change of attitude or behavior typically results. When processed by way of the peripheral route, however, the results tend to be unstable and short-lived. Therefore, persuasive messages will be more successful when processed via the central route.

When an individual is confronted with a message that he or she is not motivated to directly process, peripheral route processing may offer a more comfortable “path of least resistance” for them.
For example, an individual may choose the peripheral route to process a message that is too difficult to process, that is not interesting, or that is a subject with which the individual is not comfortable. A message that is processed through the peripheral route relies upon message cues that may be found within or around the message. Cues may be perceptions about the sender of the message such as his or her likability, trustworthiness, or level of authority, or the presentation of the message such as its attractiveness or form of communication media. Rather than spending the cognitive effort toward fully addressing the message, individuals may instead rely on message cues to influence the decisions regarding the message.

Messages processed via the central route will be predictably and more fully processed for maximum understanding. ELM states that to discourage peripheral route processing, a message must be developed with no unnecessary cues that may be used to encourage the peripheral route and must include features that will motivate individuals to process it through the central route. Therefore, knowledge and understanding of these two potential processing routes can aid in the development of a persuasive message to ensure that individuals process the message by way of the direct route such that there is a greater likelihood that an intended and longer-lasting outcome is achieved.

ISP instructional programs may benefit from ELM by concentrating on modeling instructional messages to encourage central route processing and avoiding potential message cues that may encourage peripheral route processing (Puhakainen and Siponen, 2010). This includes developing the programs to ensure that individuals are motivated to expend the cognitive effort to fully process the messages such that longer-lasting behavior change may occur. Concentrating on providing ISP instruction that is relevant and meaningful to individuals has been found to be successful in encouraging employee ISP compliance.

ISP compliance involves numerous information security issues. An increasingly growing threat involves techniques of social engineering used by persons wishing to gain access to systems to which they are not authorized. The social engineering techniques use deceptive communications and encourage individuals to process messages via the peripheral route (Workman, 2007, 2008). When a perpetrator uses social engineering, employees are fooled into performing an act or revealing sensitive information to the perpetrator. Most ISP instructional programs teach employees to be ethical and responsible and to protect information assets but do not prepare them to fend off techniques such as social engineering. ISP instructional programs may benefit from the inclusion of instructional methods for employees to recognize and prevent social engineering attacks.

54.3.7 Information Manipulation Theory

Originating in the field of communications, the information manipulation theory (IMT) (McCornack, 1992; McCornack et al., 1992) has recently been applied to information security research. The theory builds upon conversational theory that states individuals have expectations regarding the quantity, quality, clarity, and relevance of the information transmitted by a conversation. IMT proposes that any or all of these four expectations may be manipulated by the sender in such a way that the receiver of the message is unaware of the manipulation and the sender is then able to deceive the receiver. This can also be stated to mean that the level of deceptiveness of a message may be identified through quantifiable means through measurement of the quantity, quality, manner, and relevance of the information contained in the message.

54.3.8 Interpersonal Deception Theory

Another theory from the field of communications and one gaining interest within information security literature is the interpersonal deception theory (IDT) (Buller and Burgoon, 1996). As with IMT, IDT is built on conversational theory and involves a sender knowingly attempting to deceive receivers, but is expanded to include the receivers’ attempts to process the messages and to verify the truthfulness of the messages. IDT states that an interpersonal communication involves two or more individuals
dynamically exchanging information. The assumptions of IDT are that communicators enact both strategic and nonstrategic behaviors while encoding and decoding messages. Throughout the conversation, the credibility of the sender and of the message is judged by the receiver. The progression of the conversation is interactive and continuing. A deceiver may strategically insert false information into a conversation and then observe the reaction of the receivers to determine whether or not the deception was recognized. If the deception is not discovered, the conversation continues with the deceiver continuing to insert false information, adjusting as needed to remain undetected. As the conversation continues, familiarity increases and truth biases become stronger, resulting in a situation ripe for abuse. Such exchanges occur in face-to-face so-called social engineering security threats in which an individual tricks another party into revealing sensitive information, such as a password. These exchanges also frequently occur in the virtual space, where emails and websites (such as so-called fake AV sites) deceive individuals into disclosing protected information or into downloading malware in the guise of anti-virus software. Deception plays a large role in the behavioral threat environment, and is receiving fresh attention from scholars.

54.3.9 Equity Theory

The seminal work to advance the equity theory (ET) was conducted by Adams (1965) in which individuals’ perceptions of fairness within social exchanges were explored. The application of ET to equity perceptions by employees within organization has become known as distributive justice (Nowakowski and Conlon, 2005). For example, employee pay scales, raises, benefits, and hiring practices are all issues where employees may compare themselves to their coworkers and the potential for perceptions of inequality exists. In those instances when there are such perceptions, employees may become disgruntled and in turn behave in ways that are not beneficial to the organization. Employees are known to be the insider threat to organizations and information security, and the worst cases of employee disgruntlement may result in attempts by employees to harm the organization's information assets. A large percentage of the reported organizational computer abuses have been attributed to employee grievances, suggesting that this is a worthy area of study within information security, yet to date only a few works have addressed information security from this organizational aspect (Willison and Warkentin, 2009, 2013).

A larger domain known as organizational justice includes four constructs in total to describe the various forms of inequality perceptions that employees may develop within a workplace. With the first being distributive justice, second is procedural justice, related to inequalities an employee may perceive to exist within the organizational procedures (Leventhal, 1980; Leventhal et al., 1980). The last two are interactional justice, also known as interpersonal justice, and information justice (Greenberg, 1990, 1993). Interactional justice is related to the interactions between authority figures and their subordinates. Informational justice is related to the completeness and accuracy of the information as it is disseminated from senior members of the organization down through those more junior employees.

54.3.10 Social Cognitive Theory

The social cognitive theory (SCT) provides a framework to explain and predict individual behavior and changes to behaviors through the interaction of an individual with his or her environment (Bandura, 1977). SCT is primarily known as the theory behind the construct of self-efficacy and has been included in numerous studies in the field of IS with the most prominent being the development of the computer self-efficacy construct (Compeau and Higgins, 1995; Marakas et al., 1998). A self-efficacy construct is frequently included in studies within the information security context, most often addressing questions related to ISP compliance (Bulgurcu et al., 2010; Pahnila et al., 2007b). Studies based on the theoretical foundation of PMT (Anderson and Agarwal, 2010; Herath and Rao, 2009; Johnston and Warkentin, 2010), a theory that includes the self-efficacy construct, are perhaps the most common studies found within the context of information security to also rely on SCT.
54.4 Methods Applied to Behavioral Information Systems Security Research

The previous section described the theories used to investigate the research questions explored in the context of individual security-related behaviors, as well as some of the findings from research today. This section very briefly describes some of the methods commonly used in this domain. As expected, the methods are similar to other behavioral research about individual users within the IS context. InfoSec researchers survey individuals about their perceptions, attitudes, and beliefs, as well as their behaviors or intentions to exhibit various behaviors. Scholars have also devised creative lab and field experiments to create environments in which to measure salient constructs that relate various factors to security behavior. However, several unique characteristics about these behaviors and their motivation present unique challenges to valid data collection.

Measuring actual user behavior is the “holy grail” of IS behavioral research, and we often rely on measuring self-reported behavioral intention to act in a specific manner. In InfoSec, we often ask individuals to report their intention to act in a protective manner, to comply with organizationally mandated policies and procedures, or to violate such policies. Beyond the traditional concerns about validity threats from common method bias or social desirability bias, there are unique challenges encountered when asking an individual about committing a crime, which have been addressed by the criminology scientific community, from which we draw our inspiration. (Similar resistance is encountered when asking employees about violation of organizational policies.) One common solution is the implementation of a scenario-based factorial survey method approach, in which subjects are asked to read one or more versions of a scenario in which statements are embedded that represent various levels or values for the independent variables. The scenario character, acting in response to these antecedents, chooses to act in a deviant manner by violating a social norm, law, or organizational policy. The subject is then asked about the likelihood of doing as the scenario character did. In this way, the subject disassociates himself or herself from his or her own moral obligations to a certain extent and will provide a more valid indication of his or her behavioral intent. This method is now used widely within IS security behavior research to investigate the cognitive and affective elements of interest. In other cases, researchers have found creative ways to collect actual behaviors from server logs, from managers, and from other sources (Warkentin et al., 2011b, 2012).

54.5 Conclusions

Recent research in behavioral InfoSec has surfaced extensive knowledge about human behavior within this domain; however, many questions are left unanswered and much work remains. Scholars are beginning to explore new factors and new interpretations of the motivations and other antecedents of human behavior in this context, and more insights are gained every year. Future work in this area is informed by scholarly assessments of this domain (c.f. Willison and Warkentin, 2013 and Crossler et al., 2013) and by the real-world evidence of new threats and new psychological factors at play.

References


© 2014 by Taylor & Francis Group, LLC


© 2014 by Taylor & Francis Group, LLC

