MIS Quarterly

RESEARCH ARTICLE

INSIDERS' PROTECTION OF ORGANIZATIONAL INFORMATION ASSETS: DEVELOPMENT OF A SYSTEMATICS-BASED TAXONOMY AND THEORY OF DIVERSITY FOR PROTECTION-MOTIVATED BEHAVIORS

Clay Posey
Department of Information Systems, Statistics, and Management Science, Culverhouse College of Commerce and Business
Administration, The University of Alabama, Tuscaloosa, AL 35487 U.S.A. {cposey@cba.ua.edu}

Tom L. Roberts
Department of Management and Information Systems, College of Business, Louisiana Tech University,
Ruston, LA 71272 U.S.A. {troberts@latech.edu}

Paul Benjamin Lowry
Department of Information Systems, College of Business, City University of Hong Kong,
Hong Kong PEOPLE'S REPUBLIC OF CHINA {paul.lowry.phd@gmail.com}

Rebecca J. Bennett and James F. Courtney
Department of Management and Information Systems, College of Business, Louisiana Tech University,
Ruston, LA 71272 U.S.A. {rbennett@latech.edu} {courtney@latech.edu}

Appendix A

Rationale for the Proposed Six-Step Approach to Theorizing Diversity

Proposed Methods	Basis for Why Each Step Is Requisite	Method(s) for Addressing the Step
Phase I. Discovering the new construct's domain space (i.e., the relevant associated behaviors within the environment encompassed by the proposed construct) (determine the key behaviors that best represent a construct, from the perspective of the theory-based literature, experts, and target participants for whom the construct is being defined)		
Step 1a. Behavioral elicitation through literature review	Researchers who propose new constructs must consider previous work that has examined similar or related ideas. Because new constructs likely have some conceptual overlap with others, researchers should examine earlier contributions for similarities/differences.	A thorough review of IS security literature—academic- and practitioner-based—was conducted. At this stage, we excluded intentions to engage in protective behavior because insiders' actual activities are the foundation of PMBs.
Step 1b. Behavioral elicitation through qualitative analysis of target subjects of the construct	Previous literature alone is insufficient in determining the behaviors, objects, or concepts that comprise a new construct's domain space. Researchers should also obtain information from experts with topical knowledge.	We conducted semi-structured interviews with 11 information-security professionals and 22 "traditional" insiders. This mix of respondents limits the potential for an "elite bias."

Proposed Methods	Basis for Why Each Step Is Requisite	Method(s) for Addressing the Step
Step 2. Removal of redundant/ irrelevant items using unique SME groups	Some of the elicited behaviors might need to be removed due to redundancy or irrelevance based on the new construct's formal definition. For increased validity and generalizability, researchers should not use the same set of experts to perform both assessments.	Two SMEs conducted an initial review to remove redundant PMBs. Ten different SMEs then conducted a second, more rigorous examination to determine the appropriateness of each PMB.
Phase II. Discovering the taxonomic dimensions of and the homogeneous classes within the new construct (determine the perceptual map of the target participants that best represent how they most commonly classify and process the construct's underlying behaviors)		
Step 3. Acquisition of similarity ratings	Following the initial steps to elicit relevant behaviors, researchers should ascertain how the target population views the behaviors relative to each other.	An online panel of 492 insiders from a wide variety of industries assessed the general similarities among the behaviors. These insiders also provided qualitative data about their bases for making the comparisons.
Step 4. Use of MDS to determine target subjects' dimensions of the construct	Researchers should determine the number of dimensions that the target population uses to make the above comparisons.	The MDS technique was run with various initial configurations, and the analyses confirmed a three-dimensional solution.
Step 5. Using ProFit analysis to label the dimensions	Researchers should label the discovered dimensions to form a taxonomy.	Another set of 235 insiders assessed the behaviors on the dimensions elicited from Step 3. These ratings were regressed on the positions of each behavior within the perceptual structure recovered by MDS in Step 4.
Step 6. Using cluster analysis to find classes within the taxonomy	Classes of behaviors are likely to exist within taxonomies. These classes categorize the perceptions of the target population on a more detailed level.	We performed various cluster analyses on the behaviors within the cognitive structure; 14 PMB classes emerged.

Appendix B

Property Attribute Vectors for All Three Dimensions

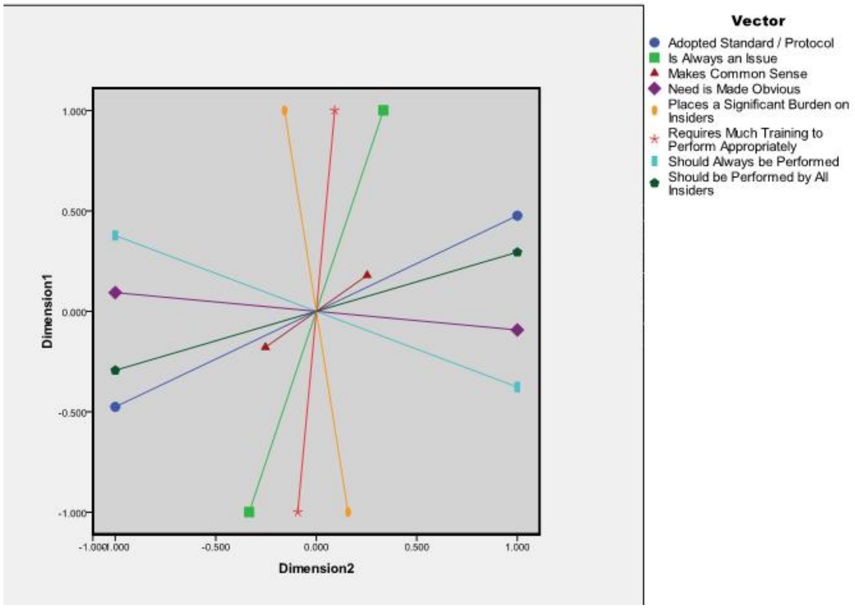

Figure B1. Property Attribute Vectors in Dimensions 1 and 2 of MDS Solution

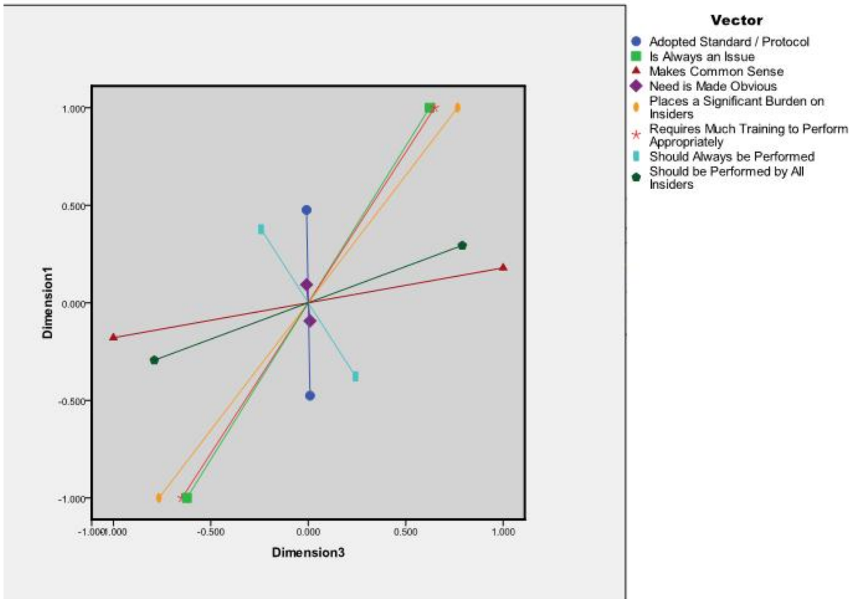

Figure B2. Property Attribute Vectors in Dimensions 1 and 3 of MDS Solution

Appendix C

Individual Behaviors Comprising Each of the 14 PMB Clusters

Table C1. Identification and Membership of Homogeneous Classes*

Class ID	Class Name	Behavior ID	Behavior Description
1	Legitimate e-mail handling	7	An OI only responds to e-mails which have a legitimate business request
		21	An OI adequately documents any changes he/she makes in the computer system
		34	An OI follows up with an individual who received an inadvertent e-mail from him/her to make sure that the individual disposed of the e-mail and its information properly
		47	An OI opens e-mail attachments only if he/she knows the e-mail's sender and was expecting the e-mail
2	Protection against unauthorized exposure	9	An OI does not allow unauthorized individuals to do his/her work for him/her
		12	If an OI needs to use a shared computer station at work but another employee is logged on, he/she logs the other employee out of the station prior to using it
		26	An OI sets his/her computer workstation's screen saver to password protect (i.e., requires a password once the screen saver detects user activity to regain access to the workstation)
		64	An OI does not verbally discuss sensitive information in areas where unauthorized persons may be located (e.g., a hallway, an elevator)
		66	An OI locks his/her workstation when leaving his/her office space so that the workstation cannot be accessed by other individuals
3	Policy-driven awareness and action	16	An OI does not forward e-mail spam to coworkers
		25	An OI stores information only according to the retention policies specified by his/her organization
		28	An OI changes his/her passwords according to his/her organization's security guidelines
		30	An OI notifies his/her coworkers of important security information he/she becomes aware of
		41	If an OI identifies something that looks out of the ordinary in his/her work environment, he/she immediately reports it to the proper organization authorities
		54	If an OI knows of shortcuts in the computer system that would be against the organization's accepted security protocol, he/she does not use them
		61	An OI does not bring a laptop from home and attach it to his/her organization's corporate network without authorization to do so
4	Appropriate data entry and management	19	An OI properly destroys and disposes of all unneeded sensitive documents
		20	An OI performs a “double check” of his/her work to make certain that the sensitive information he/she enters into the computer system is accurately coded
		53	An OI works at a steady but cautious pace to ensure that he/she performs their job tasks in a secure manner
		65	An OI backs up important data and documents on a regular basis
5	Document conversion	24	An OI does not write his/her passwords down
		40	An OI converts sensitive documents to Adobe PDF format so that none of the information in the document can be altered once it is finalized

*Organization insider has been shortened to OI

Class ID	Class Name	Behavior ID	Behavior Description
6	Secure software, e-mail, and Internet use	13	An OI does not open e-mails that he/she believes have a chance of containing a virus or other potentially malicious components
		31	An OI does not install software on his/her computer workstation unless authorized to do so
		39	An OI immediately applies software updates to his/her computer workstation when notified of the update by an authorized individual or department within his/her organization
		46	An OI pauses before responding to an e-mail to make certain that he/she is responding to a valid request
		51	An OI uses corporate e-mail for work-related activities only
		52	While at work, an OI utilizes the Internet for work-related tasks only
7	Verbal and electronic sensitive information protection	17	An OI discusses sensitive organizational information with authorized individuals only
		22	An OI does not discuss sensitive company information with the media unless authorized to do so
		37	An OI does not allow anyone to look over his/her shoulder when he/she works on sensitive documents
		44	An OI stores sensitive corporate information only on protected media or locations (e.g., a protected server)
		49	When compiling a new e-mail message, an OI double checks the list of recipients in the “To:”, “CC:”, and “BCC:” fields before he/she actually sends the e-mail to verify that only the intended recipients receive the communication
8	Wireless installation	8	An OI does not set up a wireless network access point in the corporate office without proper approval
9	Widely applicable security etiquette	3	An OI properly destroys unneeded data residing on the computer system or his/her computer workstation
		5	Prior to speaking with someone about sensitive company information, the OI makes sure the other individual(s) has legitimate access to that information
		23	An OI logs out of the computer system as soon as he/she is done using it
		29	An OI fully reads and pays close attention to security newsletters sent by his/her organization's department that is responsible for information-security matters
		55	An OI verifies an individual's identity prior to releasing sensitive information to them
		57	An OI protects his/her computer-system account information by never giving it to other individuals
10	Distinctive security etiquette	1	An OI does not write his/her system login information down
		2	An OI sets the permissions of computer files to prevent unauthorized access
		4	An OI actively attempts not to accidentally disclose sensitive company information with unauthorized individuals
		6	An OI does not put sensitive information in e-mails or other forms of electronic communication (e.g., instant messages) unless authorized to do so as required by his/her job
		10	An OI does not display sensitive documents in public (e.g., airplane or airport)
		11	An OI always properly logs into and out of computer systems at work
		27	An OI creates strong passwords (i.e., passwords having a combination of lower- and upper-case letters, numbers, and special characters)
		33	An OI does not leave active computers unattended
		36	An OI immediately reports a lost access card to the proper organization authorities
		38	An OI clears sensitive information off of his/her desk or computer before allowing someone entrance into his/her office or leaving at the end of the work day

Class ID	Class Name	Behavior ID	Behavior Description
		45	An OI locks sensitive, physical documents in a secure location when they are not in use
		56	An OI adheres to the information-security guidelines and policies adopted by his/her organization
		63	An OI does not discuss company-specific, information-security information (e.g., internal protocols, breaches) with anyone who does not need to know
11	Coworker reliance	14	An OI does not open e-mails that “just do not look right” to him/her
		18	An OI informs his/her coworker if he/she believes that the coworker is engaging in behaviors not accepted by their company's information-security guidelines and policies
		58	An OI does not allow anyone else to utilize his/her computer workstation
		62	An OI only uses secured wireless and/or wired networks approved by his/her organization for off-site network access
		67	An OI reminds his/her fellow coworkers of information-security guidelines and protocols adopted by their organization
12	Account protection	35	An OI immediately informs his/her supervisor upon his/her awareness of the physical theft of computer equipment
		42	An OI immediately informs the authorized individual or department within the organization if he/she found a potential information-security problem or loophole
		50	An OI only accesses information in the computer system that is required for his/her job
		59	An OI does not allow anyone else to utilize a computer workstation under his/her account and login information
		60	An OI does not perform work on a computer workstation with a coworker's account information or under a coworker's login session
13	Immediate reporting of suspicious activity	15	An OI quickly notifies the sender of an e-mail if that e-mail contained sensitive information that was not meant for him/her
		43	An OI immediately reports a coworker's negligent information-security behavior to the proper organization authorities
		48	If an OI receives an e-mail from someone he/she knows but the topic or content looks suspicious, he/she contacts the sender to verify that the communication attempt was valid
14	Equipment location and storage	32	An OI keeps the laptop or other electronic devices issued to them by their organization with them at all times

Appendix D

Summary of Theory of PMB Diversity

Summary of Theory of PMB Diversity

The key result of our taxonomic analysis was that we discovered that organization insiders think of PMBs in three key dimensions. We labeled the three discovered dimensions of insiders’ perceptual map of PMBs specifically as *promotion difficulty* (first dimension), *degree of criticality* (second dimension), and *degree of common sense* (third dimension). In this section, we discuss why we labeled these dimensions as such.

In terms of the first dimension, insiders separated PMBs on whether these activities were burdensome, whether they were always an issue within the individuals' organizations, and whether the activities required training. We chose to label this dimension as *promotion difficulty* because of the underlying, ongoing burden, focus, and effort required with these PMBs. Namely, PMBs classified as *high* in promotion difficulty are behaviors that insiders believe should remain a steady focus of the organization because the behaviors place more of a burden on the insiders to perform effectively. Additionally, these PMBs require more formal training to ensure the behaviors' efficacy. These PMBs also require continual emphasis within organizations and include the behaviors of double-checking work completed to ensure accuracy and backing up data on a regular basis.

Conversely, PMBs residing closer to the *low* end of the promotion difficulty dimension are those that require little-to-no formal training or continual awareness programs because the behaviors either (1) do not encumber the insider when performed and are more easily performed than those behaviors in the high classification or (2) are already being performed to such a degree that organizations need only minimal awareness efforts. Example behaviors include locking workstations before the insiders physically leave the workspace or immediately informing the proper authorities after thieves steal computing equipment.

Degree of criticality is the second dimension within the classification scheme identified by the ProFit procedures. We labeled this dimension relative to the criticalness of the PMBs according to the collective insider mindset. The dimension varies according to whether the activities are commonly accepted protocols or standards, should be performed by everyone within organizations regardless of position, should always be performed, and whether there is an obvious need for such behaviors. Insiders should perform PMBs that have a *high* degree of criticality—regardless of occupation, status, or organization. These behaviors are included as part of the adopted company protocol and are generally accepted by all insiders. Example behaviors include discussing sensitive information with authorized individuals only, logging out of a computer system as soon as an individual has completed his/her task with it, and changing passwords according to organizational guidelines.

Insiders consider PMBs with a *low* degree of criticality as having a limited scope and are less obvious than those behaviors with a high criticality. According to insiders, not everyone needs to perform these behaviors and not at all times within the organization. These characteristics are due in part to insiders' views that many of these behaviors have not been formally adopted within their organizations as protocol or as every individual's responsibility to perform. Example behaviors placed in this low classification include setting the permissions of computer files to prevent unauthorized access, keeping the electronic devices assigned to insiders by the organization with the individuals at all times, and adequately documenting any changes the individual makes in the computer system are placed within this low classification.

One notable difference in the mindset of insiders regarding behaviors in the high and low degree of criticalness types is the perceptual distance between two behaviors: *high*—reporting a coworker who deviates from those guidelines to the proper authorities; and *low*—reminding a coworker of information security guidelines. Interestingly, insiders as a collective unit believe it is critical for everyone to report an internal deviant, while only few believe that it is their responsibility to issue friendly reminders about security matters to their peers.

We best represent the third and final general dimension in the formal taxonomy as *degree of common sense*. Insiders consider behaviors that are *high common sense* as having clear logic and rationale. Many insiders referred to these activities as "knowledge commonly held by everyone." Examples of such commonsensical behaviors are working at a steady but cautious pace or immediately reporting a lost physical access card to management.

Low common sense PMBs refer to actions whose founding logic may be unclear to insiders and whose foundations go beyond normal requirements. For example, many insiders did not consider the behavior of not opening e-mails that "just do not look right" as commonsensical because they cannot assess what constitutes "legitimate business communication" adequately. Insiders thus do not believe it to be reasonable to ask them to determine what looks "right" or what looks suspicious. Insiders also collectively believe that disallowing access to the Internet for nonwork-related material and disallowing use of corporate e-mail for personal matters are irrational requests. This is a particularly salient finding as extant corporate security practice often clash with this collective mindset.

Summary of Homogeneous PMB Classes

In addition to the discovery of the cognitive taxonomy, we found that various homogeneous classes of PMBs exist. Cluster analyses identified 14 unique clusters within the MDS structure; however, a few of the clusters had only one or two members. Although all of the behaviors are PMBs, not all are similar enough for grouping with others. For example, the behaviors of *gaining approval before setting up a wireless network within the organization* and the act of *keeping the physical electronic equipment assigned to insiders by the organization with them at all times* *when away from the organization* are single-item clusters. Likewise, due to the wide array of behaviors in the perceptual space, some PMBs belong to a cluster whose other behaviors might not appear similar. In these cases, we defined clusters according to the majority of behaviors making up the composition of the clusters. Table C1 (in Appendix C) lists the individual behaviors comprising each of the clusters. We describe the 14 clusters in detail, as follows.

1. *Legitimate e-mail handling* refers to those PMBs dealing specifically with insiders' use and handling of corporate e-mail. As a communication method, insiders must handle e-mail securely to limit the detrimental effects posed by organizational security threats. Insiders' activities such as only responding to e-mails that have legitimate business requests and only opening e-mail attachments originating from known individuals belong in this cluster. Respondents continually mentioned that they have difficulty determining what specifies "legitimate" electronic communication. Some respondents mentioned "all e-mails deserve a response" due to their inability to make this determination. Other comments indicate that many insiders believe that their follow-up to an inadvertent e-mail is necessary only if that e-mail contained sensitive information, whereas other individuals believe that they "don't send information that is *THAT* private. [They] would just send it again to the correct address" (emphasis in original). Accordingly, legitimate e-mail handling activities apply to everyone and require more of an organizational focus to assist insiders in making appropriate determinations of "legitimate" communication attempts.

2. *Protection against unauthorized exposure* is composed of PMBs that specifically limit the exposure of sensitive information to unauthorized internal and external sources. PMBs in this cluster describe how insiders manipulate their personal and/or shared workstations to accomplish this goal. Behaviors such as setting a workstation's screen saver to password protect, locking a workstation before leaving one's workspace, and logging other individuals out of a shared workstation before using it belong to this cluster. To prevent unauthorized individuals from receiving sensitive organizational information, insiders must be careful to not discuss sensitive information verbally in proximity to unauthorized persons and to disallow others from doing work for which insiders are responsible. Respondents referred to these activities as "most obvious," "following good business practice," and are "always the best thing to do for everyone."

3. *Policy-driven awareness and action* behaviors are rooted in formal corporate policy. This set of PMBs includes storing information and changing passwords according to accepted internal security protocol. Further, this behavioral group also includes an insider not using *system shortcuts* (this involves choosing to skip steps in a protocol so that insiders' perceived level of performance or customer service supersedes level of protection; for example, allowing an unauthorized subordinate access to data to cut through red tape to "get a job done"). Despite being against corporate policy, individuals responded that "as long as [the shortcut] does not compromise the integrity of my work or the computer system, I will use [it]," "sometimes you need to meet a deadline," and "it depends on how effective [the shortcut] is." Other behaviors in this cluster include not e-mailing spam to coworkers and not bringing a laptop from home and attaching it to the corporate network without prior authorization.

4. *Appropriate data entry and management* is composed of PMBs related to insiders' care for data entry and data management. These behaviors include the proper disposal and destruction of all unneeded sensitive documents and the regular backing up of data and documents. Other PMBs assigned to this cluster deal directly with the accuracy of data-entry activities (e.g., double-checking one's work and working at a cautious but steady pace). Respondents mentioned that they "take pride in doing [their] job right" and that it is "always wise to have a backup in case something happens to the original documents."

5. *Document conversion* refers to insiders' converting sensitive, corporate documents to other formats to reduce potential alterations from their original content by security threats. For example, "tax-related filings," "legal documents whose wording cannot be changed," and "official corporate documents to be placed on a website" would need an added measure of protection. Most insiders perform this activity by converting a document to a PDF format. The activity of document conversion is different from many of the other behaviors because "PDFs are made to be sent to others."

6. *Secure software, e-mail, and Internet use* refers to a general set of PMBs that highlight insiders' secure use of computer software, electronic mail, and the Internet. For example, insiders should apply software updates immediately to their workstations upon receipt of notification of important updates. Insiders must also refrain from using corporate e-mail and the Internet for personal reasons while at work and must install software on workstations only if they received prior authorization to do so. However, some respondents believe "these [behaviors to be] important but often not followed" and see it as an impossibility for them to wholly conform to such restrictions. Insiders justify their actions with statements like "some personal e-mail on a limited basis can be acceptable," "everyone inevitably gets some personal e-mail once in a while," "there are some times for an organization insider to get personal business done," and the behaviors should be "allowed as long as they don't distract from getting business tasks done quickly." Employees should apply software updates "as soon as is reasonably possible but not if someone is in the middle of a project."

7. *Verbal and electronic sensitive-information protection* is the set of PMBs dealing with insiders' control of their verbal and electronic communication to limit unneeded release of sensitive information. Verbally discussing sensitive information with authorized individuals only and not discussing sensitive corporate information with the media without prior approval reside in this cluster. Individuals within organizations must also attempt to limit the exposure of electronic communication and documentation. PMBs stipulating that insiders not allow anyone to look over their shoulder while working on sensitive documents (e.g., using a laptop in a crowded area such as an airport or airplane) and double-checking all potential recipients of an e-mail before sending it decrease the chance that sensitive electronic documentation falls into the wrong hands.

8. *Wireless installation* is composed of the PMB that refers to an insider's seeking permission before setting up a wireless network access point within the organization. Overall, insiders responded that this activity would be "grounds for dismissal" if prior authorization was not given. However, most respondents stated that they would "have no idea how to set up a wireless access point" and such a request would require additional training. Others mentioned that the installation of wireless access points within the organization is the responsibility of managers or the IT group, and thus to place this responsibility on all insiders would be unreasonable because they "don't need to worry about this" along with everything else for which they are responsible.

9. *Widely applicable security etiquette* and
10. *Distinctive security etiquette* contain behaviors that are general rules of professional conduct within organizations in terms of protecting information assets. The key difference between these two sets of behavioral groups is that insiders believe that one set is critical to more positions and industries, whereas the other should be more restricted to a smaller body of individuals and/or organizations. For example, logging in and out of systems immediately upon completing job tasks and fully reading and paying attention to organizational security newsletters or other forms of communication is necessary for everyone. However, setting file permissions to restrict unauthorized access—although a good, general PMB—does not appear to be the responsibility of many insiders. Further, not all organizations issue access cards or give everyone access to important information-security information.

11. *Coworker reliance* contains PMBs related to insiders relying on each other for important information-security information and activities within organizations. These behaviors state that insiders have the ability to remind their fellow coworkers of information-security guidelines and policies or inform coworkers when they are violating organization rules.

    Despite this capability, insiders sometimes feel uneasy or hesitant about approaching one of their fellow employees if there is a chance that they could be incorrect. Some insiders mentioned that these activities require them "to take a leadership role to ensure that others adopt [policy]," which "keeps others out of trouble" even if a simple reminder of the guidelines can avert disaster; meanwhile, others leave this responsibility to management or the IT security group. Realistically, insiders must use caution in using these approaches because they do not want to appear to upset office politics and relationships.

12. *Account protection* is the set of PMBs referring to insiders' protection of their system account information, as well as the resources the individuals are able to access under their individual accounts. These behaviors include not allowing anyone else to use the insider's personal account or workstation or an insider not using another coworker's account. Moreover, insiders should be concerned with the information resources accessed when logged on under their account. However, some respondents mentioned that "if it saves time and won't affect anything, [they] will use another account." This act largely "depends on the situation" and occurs "only under certain circumstances." Others stated that "it depends on the [insider's] ethics, but if [the insider] wants to be treated the same way, [the insider] respects the coworker's privacy" and will do it if s/he receives the coworker's permission to access the system under the coworker's credentials.

13. *Immediate reporting of suspicious behavior* is the set of PMBs that specify the importance of insiders in swiftly reporting potential security dangers to appropriate authorities. Organizations rely on insiders to report suspicious physical or electronic activity to minimize potential security threats as a major line of defense. An example behavior is immediately notifying the proper internal authorities about a coworker's negligent security-related behavior.

14. *Secure equipment location and storage* is composed of PMBs specifying that insiders should always keep electronic devices (e.g., laptops, personal digital assistants) issued to them by their organization with them at all times. Although considered a worthy expectation, many insiders stated that always keeping these devices with them "just isn't sensible" because it "can be under [their] control but not with [them] at all times." This control is accomplished by devices being "locked up at home or hotel room, but they can't be beside you all of the time." Whereas all insiders are not issued portable electronic devices by their organizations, respondents mentioned individuals who make sure to carry these devices all of the time when away from their office were "obsessing with following rules."