Managers' and Senior Executives' Perceptions of Frequency and Type of Employee-Perpetrated Information Sabotage and Their Attitudes toward It - The Results of a Pilot Study

John C. Hafer
University of Nebraska at Omaha

George Gresham
Jacksonville University

ABSTRACT

A pilot study investigating information sabotage found most responding managers and senior executives polled feel that most forms of sabotage are considered as grounds for termination. Respondents know sabotage occurs in their companies and many personally know someone who has committed sabotage. One in five respondents reported having been a victim, half know employees who have been victimized and a third know of other managers and customers who have been victimized. Findings are discussed. Firm size was not related to occurrence, attitudes or victimization rate.

Introduction and Purpose

In the spring of 2009, Hafer and Gresham (2009) published a theoretical article on the antecedents of information sabotage and suggested, "It would seem that investigating the perpetration of sabotage offers only limited possibilities…but researching people's knowledge of its occurrence and their attitudes towards it…could offer substantial opportunities to add to the literature base about sabotage in general and information sabotage specifically." Since information sabotage could be a covert, non-physical and difficult-to-trace act, and, since there may be no immediate, apparent and visible victim, people's attitudes toward it and its perpetrators may be very different when compared with a physically destructive, overt act where there is a readily apparent and possibly well-known victim. In the former case, people may be much more tolerant and forgiving of a saboteur who purposely delays or misdirects information as opposed to a saboteur who steals from the company or destroys its hardware or systems. Although both actions could have the same ultimate outcome on the business, covert actions like misdirecting or delaying information might be seen as a "soft misdemeanor," while physically overt acts might be perceived as purposefully destructive and felonious. This form of a "soft misdemeanor" might be tolerated as something everyone does once in a while. However, purposeful destruction of company property, files or systems would require retribution. These two scenarios are analogous to taking a pencil from work, a soft misdemeanor, as opposed to destroying sensitive computer files or stealing a computer from work, something done with intent to do harm and premeditated, (Hafer & Gresham, 2009, pp. 241-2). "In the current high-technology workplace, the opportunity,

frequency, and impact of employee sabotage is expected to increase, making the need to understand sabotage increasingly important to an organization's success," (Skarlicki, van Jaarsveld, & Walker, 2008, p. 1335).

The purpose of this article is to report the results of an empirical pilot study using data from a convenience sample of managers' and senior executives' investigating their perceptions of the occurrence of employee-perpetrated information sabotage, their attitudes towards different acts of sabotage and finally, their knowledge of victimization by information saboteurs. In addition to reporting the findings, the data will be tested to determine if there is any significant differences in these areas that might be traceable to firm size. Implications and generalizations will be discussed.

Background on Information Sabotage

"Sabotage is the act of hampering, deliberating subverting, or hurting the efforts of another. It is most often an issue in the context of military law, when a person attempts to thwart a war effort, or in employment law, or when disgruntled employees destroy employer's property. Cyber-industrial sabotage activities, such as hacking, usually relate to industrial secrets that have commercial value to competitors. In some countries, computer sabotage may be regarded as a breach of civil law rather than criminal law, but there are laws clearly defining cyber-crime as a criminal offense," (http://definitions.uslegal.com/S/SABOTAGE). Information sabotage is being defined here as the maliciously purposeful and covert, or overt, attempt by employees to intentionally and with premeditation hinder, harm or prevent the acquisition, dissemination and response to market/customer/company information (Hafer & Gresham, 2009). The defining factor separating sabotage from simple mistakes, negligence or errors is malicious intent. Direct, deliberate and physically destructive harm is obvious and needs no explanation. Indirect harm can come from damage to a company's image, reputation, or relationships with upstream vendors or downstream channel members or final customers.

Information sabotage is an ongoing threat effecting companies of all types. As reported in hreonline.com: "At Omega Engineering, a computer-systems administrator crashed Omega's companywide server and stole vital backup files. Production ground to a halt. Despite the best efforts of a team of data recovery experts, Omega lost about $10 million and countless files. At Walt Disney, an employee tampered with video release versions of the animated film 'The Rescuers', and embedded an obscene photograph in two frames. Disney responded by recalling 3.4 million videos. A Lockheed Martin employee was fired for sabotage after a mass e-mail sent to 60,000 of his co-workers crashed the company's system for six hours. It took a team of Microsoft crisis experts and several hundred thousand dollars for the company to recover. At Forbes, their New York operations were shut down for two days after a former employee crashed five of the company's eight servers. Vital information on the affected servers was lost. The employee lashed out after being fired from a temporary position," (Forman & Watkins, 2009).

Sabotage is a form of workplace aggression, itself defined over 30 years ago by Spector (1978) as "… any behavior intended to hurt the organization … [which] could be overt or covert" (p. 821). It may be unplanned or premeditated (Anderson & Bushman, 2002), verbal or physical, direct or indirect, active or passive (Buss, 1961; Baron & Neuman, 1996). Non-physical violence can be psychological violence (Chappell & De Martino, 2005). Smith and Rupp (2002) summarized the profile of saboteurs of a company's information system as "…predominately introverts. They generally experience social and personal frustrations. They often display loose ethical boundaries and disregard the notion of the word "private." They have a lack of empathy. They believe they are owed special recognition and would seek revenge if they did not receive it" (p. 180).

"The motivation to commit sabotage has been widely discussed in the literature. Crino (1994) identified twelve motivations for sabotage: (1) to make a statement, (2) to prevent or encourage corporate change, (3) to establish personal worth, (4) to gain an edge over co-workers, (5) to gain revenge, (6) to have an impact in a large bureaucracy, (7) to satisfy a need to destroy, (8) to seek thrills, (9) to avoid responsibility for failure, (10) to avoid work, (11) for personal gain, and (12) to vent personal anger created by non-work problems. Skarlicki et al. (2008) said sabotage is retaliation for perceived injustice and that it serves as a method of equity restoration or "getting even" (see Burton, Mitchell, & Lee, 2005; Ambrose, Seabright, & Schminke, 2002; Skarlicki & Folger, 1997; Skarlicki, Folger, & Tesluk, 1999). Stewart (2007) offered the notion that situational and personal factors interact in the sabotage decision. Breach of the employee-employer psychological contract has been suggested as an explanation for sabotage/retaliatory behavior (Bellou, 2007; Edwards & Karau, 2007; DelCampo, 2007a, 2007b; Burton et al., 2005; Robinson & Rousseau, 1994; Rousseau, 2001; Rousseau & Tijoriwala, 1998, 1999; Zhao, Wayne, Glibkowski, & Bravo, 2007)," Hafer & Gresham, 2009 (pp. 241-2).

There are eight types of workplace aggression based on Buss' (1961) categorization and later used by Baron and Neuman (1996), which are presented in Table 1 below. These types are based on the traditional notion of sabotage involving two people or a person and physical surroundings. Applying this scheme to information sabotage, the "verbal" aspect of this construction would relate to "information," i.e., the contents of files. Passive would represent something like redirecting files and physical would represent some sort of actual physical destruction of files, equipment or network components. The term "direct" and "indirect" would be a traceable act in the case of the former and something as covert as simply delaying or mis-directing information in the case of the latter; something that could be misidentified as an accident or coding error.

The forms of sabotage are diverse. Giacalone and Knouse (1990) identified forty methods of sabotage, but specifically identified information sabotage as information tactics whose culprit would be difficult to identify or tactics that capitalized on company weaknesses in areas that were difficult to control, e.g., the spreading of rumors; the altering or deletion of data and placing false orders. Information sabotage is also failing to transmit information needed by the target (Baron and Neuman, 1996, p. 164). It can be the deliberate destruction of the work environment, inaction, waste and purposeful

malicious activities that could bring about organizational changes, policy changes, effect sales or profits, or effect customer relations (Skarlicki et al., 1999; Neuman & Baron, 1998; Skarlicki & Folger 1997).

Table 1
Examples of Eight Types of Workplace Aggression

Type of aggression	Examples
Verbal-passive-indirect	Failing to deny false rumors about the target. Failing to transmit information needed by the target
Verbal-passive-direct	Failing to return phone calls. Giving someone "the silent treatment."
Verbal-active-indirect	Spreading false rumors about the target. Belittling someone's opinions to others.
Verbal-active-direct	Insults; yelling, shouting; flaunting status or authority; acting in a condescending, superior manner.
Physical-passive-indirect	Causing others to delay action on matters of importance to the target. Failing to take steps that would protect the target's welfare or safety.
Physical-passive-direct	Purposely leaving a work area when target enters. Reducing others' opportunities to express themselves
Physical-active-indirect	Theft or destruction of property belonging to the target. Needlessly consuming resources needed by the target.
Physical-active-direct	Physical attack, destruction directly on a target.

Source: Baron & Neuman (1996)

The costs related to information sabotage are estimates at best due to its often covert nature and the inability to directly trace a loss to anyone or any specific type of sabotage. Overt sabotage losses, such as those coming from the physical destruction of equipment, systems, software, etc., are traceable, but insidious forms of sabotage, such as misrouting information, are difficult if not impossible to accurately measure or estimate the losses. A literature search on the costs associated with sabotage to information systems uncovered statistics from as far back as 1997, and a 2000 study suggests millions of dollars are lost each year to computer, network, database and software sabotage. The 1997 Computer Crime and Security Survey was conducted by CSI (Rapalus, P., 1997) and composed of questions submitted by the Federal Bureau of Investigation (FBI) International Computer Crime Squad's San Francisco office. The survey was sent to security practitioners in a variety of U.S. corporations, government agencies, financial institutions and universities. Responses were obtained from 563 organizations. Excerpts from these two surveys highlight the extent of the reportable and identifiable losses. From the 1997 survey, 75% of respondents reported financial losses due to various computer security breaches ranging from financial fraud, theft of proprietary information and sabotage. Of those reporting financial losse (Rapalus, P., 1997):

- 16% cited losses due to unauthorized access by insiders
- 14% cited losses due to theft of proprietary information
- 12% cited losses due to financial fraud

- 11% cited losses due to sabotage of data or networks
- 8% cited losses due to system penetration from outside.
- 26 respondents reported $4,285,850 in losses due to sabotage of data or networks.

From the 2000 survey, 61 respondents quantified losses due to sabotage of data or networks for a total of $27,148,000. The total financial losses due to sabotage for the previous years combined totaled only $10,848,850 (Rapalus, P., 2000).

The 2008 CSI Computer Crime and Security Survey suggested losses to responding companies averaged $288,618 per respondent reporting (*n* = 144), with losses from theft/loss of proprietary or customer data ranging from $240,000 to $268,000 per respondent (Richardson, 2008). If these loss estimates are reliable and representative of all the firms contacted (*n* = 5000), the extrapolated loss figure would run to $1.4 billion (Richardson, 2008). The 2010 report claimed 25 percent of respondents said more than 60 percent of financial losses came from insiders, not external hacks (Richardson, 2010). Eighty-eight percent of IT administrators, if laid off the next day, said they would steal valuable and sensitive company information (Anonymous, 2008). As businesses have become more dependent on technology, especially computers and the Internet, methods of sabotage and what is defined as sabotage have grown, as have the costs of sabotage to businesses stemming from either direct losses of revenue or costs associated with prevention, detection and/or repair.

The Survey

Nineteen forms of information sabotage were identified and served as the basis of the survey. The questions were compiled and modified based on the forms of information sabotage originally published by Giacalone and Knouse (1990) and Richardson (2008), and several questions were added or modified with the assistance of corporate IT security professionals from BlueCross BlueShield Insurance Co. and First Data Recourses who were instrumental in creating the final version of the survey for this research.

The specific acts of sabotage studied represent both passive and aggressive forms and forms which are either covert or overt. The specific acts encompassed the eight forms of sabotage identified by Baron and Neuman (1996) in Table 1. The specific acts identified in the survey are shown in Table 2 along with which aggression category they fit.

The survey investigated two aspects of information sabotage. The first was the respondents' attitude regarding each act of information sabotage with respect to how serious an offense the respondent perceives it to be as reflected by the type of managerial action that should be taken in response to the specific act of sabotage, which is in line with Ajzen and Fishbein's (2005) theory of planned behavior, the idea that attitudes predict subsequent behavior.

Table 2
Specific Acts of Sabotage Investigated and Workplace Aggression Category

1.	Maliciously alters files	Physical-Active-Indirect|Verbal-Active-Direct
2.	Malicious hacking	Physical-Active-Direct|Physical-Active-Indirect
3.	Deliberately deletes files	Physical-Active-Direct
4.	Purposely delays transfer of information	Verbal-Passive-Direct
5.	Physically damages software, hardware or a network	Physical-Acitve-Direct
6.	Purposely alters security measures	Physical-Acitve-Indirect
7.	Purposely provides inaccurate information to the requestor	Verbal-Active-Indirect
8.	Steals proprietary information	Verbal-Passive-Direct
9.	Purposely misdirects information	Verbal-Passive-Indirect
10.	Purposely provides misinformation; either provides a better outlook or a worse outlook for a company	Verbal-Passive-Indirect
11.	Creates misinformation about a co-worker or manager	Verbal-Active-Indirect
12.	Hijacks electronic communications to alter the content in an unfavorable manner for the sender of the information	Verbal-Passive-Direct
13.	Gathers information in a low and slow manner; collecting critical information unnoticed	Verbal-Passive-Indirect
14.	Holds information hostage, i.e., passwords to critical systems	Verbal-Active-Direct
15.	Alters or erases backup data, making recovery impossible	Verbal-Active-Direct
16.	Alters system and application logs to cover-up one's activities	Verbal-Passive-Direct
17.	Alters network routing to enable "man-in-the-middle" attacks and/or information capture	Verbal-Active-Direct
18.	Public release of proprietary data	Physical-Passive-Direct
19.	Takes critical systems or services off-line, a denial of service	Physical-Passive-Indirect

In this section of the survey, each of the nineteen forms of sabotage was preceded with the statement "An employee of your company does the following form of information sabotage: _____ so as to harm a targeted person, department, customer, program or organizational change. Complete the following statement: "I would consider this to be a _____." Respondents chose from four foils: "Minor Offense – Warning is

sufficient," "Moderate Offense – Disciplinary action required," "Major Offense – Termination should result," and "This offense is NOT worthy of any action."

The second section of the survey asked participants about their knowledge, suspicion or perception of employees' specific participation in each of the nineteen forms. Asking about specific knowledge that sabotage has occurred seems apparent on its face. Asking about the respondents' perception of occurrence relates to the "Phenomenal Principle" (Robinson, 1994, p. 32): "If our manager perceives and as such believes that such a thing *is happening*, then s/he must also be aware of a situation *where that has happened*." Stating it somewhat differently, "if s/he had absolutely no awareness that such motivations could take place, and then s/he could not, by definition, create such a perceptual scenario. To arrive at such a perception, s/he is aware that such motivations are possible and is aware of them." Whether s/he has experienced these motivations first-hand or vicariously, s/he must be aware of them to arrive at her perception.

Respondents were given the foils of "I know one of my people has done this," "I am confident that at least one of my people has seriously considered doing this," "I'm sure at least one of my people might seriously consider this," and finally "I'm sure none of my people have ever considered doing this." The third foil, "…might seriously consider this," evokes some degree of probability on the respondent's part. While not asking for a specific probability estimate, it does suggest if the respondent marks this choice that s/he perceives there is a reasonable chance of it happening. From the responses, it is possible to array the nineteen options from "most probable" to "least probable" by counting the number of times that option was selected for that specific act…in essence how many votes that specific act received reflects the number of people that believe it could reasonably happen. Finally, respondents were asked about their knowledge of victimization, either themselves being victims or asking if they knew of individuals or customers who have been victims. Several demographic questions about gender, age, firm size (as measured by number of employees) and job title concluded the survey.

The Sample

This pilot study solicited responses from a convenience sample of all alumni from the Executive Masters of Business Administration (EMBA) program at one of the author's university. By definition, EMBA students must have attained middle management positions and have had 5+ years of management experience to have been admitted to the program.

A single, not pre-notified mailing of 517 surveys was sent to the names on the list, 60 bad address envelopes were returned yielding a net of 457 potential respondents. Of that number 72 usable surveys (16%) were returned and formed the data base for the findings for this article. Forty-two percent were females, fifty-eight percent males. Four percent were under 30 years of age, 32% were 32-45 years old, 58% were 46-64 and 6% were over 65. Most were managers/senior executives of companies employing 1000+ employees (63.1%), 21.5% employed less than 100 people, 7.7% employed between 100 and 500 employees and the balance employed between 500 and 1000.

Over 90% of the respondents had the title of manager, director, VP, CEO, CIO, CFO, owner, Sr. VP, President, etc.

Findings

The results of the questions focusing on respondent's attitudes toward the nineteen specific acts indicate that for a majority of those presented, the respondents felt each act of sabotage was a major offense and should result in termination or significant managerial disciplinary actions. The findings for each act are shown in Table 3. Rated by a majority of the respondents as a minor or moderate offense requiring either a warning or disciplinary actions were:

"Purposely delays transfer of information" - 73.2%.
"Purposely misdirects information" – 60%
"Creates misinformation about a coworker or manager" – 61.1%
"Gathers information in a slow manner…" – 69%
"Holds information hostage, i.e., passwords to critical systems" – 54.2%

The worst offenses appear to involve direct overt destructive activity, as opposed to an indirect activity, meaning they involve stealing, hacking, directly altering, hijacking, erasing or physically damaging. The least offensive acts of sabotage share the common factors of being indirect attacks of a more passive nature; delaying, slow to gather, creating misinformation or inaccurate information and misdirecting information. These could all be excused away by the perpetrator as being simple errors or mistakes. They could be excused away by claiming a work overload that resulted in not enough time or resources to do the job in a timely manner. These manager/executive respondents may have ranked the items on the bottom of the array (least offensive) as they did with the thought in mind that it is reasonable to assume this subtle form of sabotage might not be sabotage at all, while those ranked at the top of the array, things like stealing, hacking, hijacking, erasing, altering logs and physically damaging software, hardware or network components cannot reasonably be assumed to have been done accidentally. Thus we might speculate that the respondents may be giving the perpetrator of these least offensive acts the benefit of the doubt.

Simply looking at the numbers in the array, we could infer that the items at the top of the list are viewed as being as much as four times worse than the items at the bottom of the list. In summary, there is definitely a hierarchy evident. All forms of sabotage are not viewed as equally offensive as one might believe using the strict moral/philosophical distinction of right is right and wrong is wrong; one act of sabotage is as morally wrong as any other. Clearly some acts of sabotage are seen as much more significant and as such punishable than others.

Table 3
Form of Sabotage and Appropriate Disciplinary Action

In an attempt to harm…, an employee of your company does the following form of information sabotage, _____, so as to harm a targeted person, department, customer, program or organizational change. Complete the following statement: "I would consider this to be a _____.	**I Think This is a Minor Offense** – Warning Is Sufficient	**I Think This is a Moderate Offense –** Disciplinary Action Req'd.	**I Think This is a Major Offense** – Termination Should Result	**I Think This Offense is NOT Worthy of Any Action**
1. Maliciously alters files		14.1%	84.5%	1.4%
2. Malicious hacking		5.6	93.1	1.4
3. Deliberately deletes files		26.8	71.8	1.4
4. Purposely delays transfer of information	15.5%	57.7	25.4	1.4
5. Physically damages software, hardware or a network		19.4	79.2	1.4
6. Purposely alters security measures	2.8	18.1	77.8	1.4
7. Purposely provides inaccurate information to the requestor.	5.6	44.4	47.2	2.8
8. Steals proprietary information		2.8	95.8	1.4
9. Purposely misdirects information	2.9	57.1	38.6	1.4
10. Purposely provides misinformation; either provides a better outlook or a worse outlook for a company	7.0	31.0	59.2	2.8
11. Creates misinformation about a co-worker or manager	11.1	50.0	37.5	1.4
12. Hijacks electronic communications to alter the content in an unfavorable manner for the sender of the information	1.4	15.3	81.9	1.4
13. Gathers information in a low and slow manner; collecting critical information unnoticed	18.3	50.7	29.6	1.4
14. Holds information hostage, i.e., passwords to critical systems	11.1	43.1	44.4	
15. Alters or erases backup data making recovery impossible	1.4	15.3	81.9	1.4
16. Alters system and application logs to cover up one's activities	1.4	16.7	80.6	1.4
17. Alters network routing to enable "man-in-the-middle" attacks and/or information capture	1.4	18.3	77.5	2.8
18. Public release of proprietary data	2.9	14.3	81.4	1.4
19. Takes critical systems or services off-line, a denial of service	1.4	32.9	64.3	1.4

Rearranging the array listing the nineteen acts in order of most to least offensive Table 3 rearranges to the following array ranked by highest percentage (worst offense) to lowest:

8.	Steals proprietary information	95.8
2.	Malicious hacking	93.1
1.	Maliciously alters files	84.5
12.	Hijacks electronic communications to alter the content in an unfavorable manner for the sender of the information	81.9
15.	Alters or erases backup data making recovery impossible	81.9
18.	Public release of proprietary data	81.4
16.	Alters system and application logs to cover up one's activities	80.6
5.	Physically damages software, hardware or a network	79.2
6.	Purposely alters security measures	77.8
17.	Alters network routing to enable "man-in-the-middle" attacks and/or information capture	77.5
3.	Deliberately deletes files	71.8
19.	Takes critical systems or services off-line; a denial of service	64.3
10.	Purposely provides misinformation; either provides a better outlook or a worse outlook for a company	59.2
7.	Purposely provides inaccurate information to the requestor.	47.2
14.	Holds information hostage, i.e., passwords to critical systems	44.4
9.	Purposely misdirects information	38.6
11.	Creates misinformation about a co-worker or manager	37.5
13.	Gathers information in a low and slow manner; collecting critical information unnoticed	29.6
4.	Purposely delays transfer of information	25.4

The second section of the survey dealt with the respondent's belief that the forms of sabotage either had been, or could probably be, committed by one of her/his employees. The findings are shown in Table 4. As with the previous data, the overwhelming majority of the respondents believe that for many of the nineteen forms of sabotage listed, none of their employees have considered doing any of them. By arraying this information in a similar fashion to the previous set of data, the form of sabotage that almost one in three respondents did identify as having knowledge of its occurrence was creating "misinformation about a co-worker" (31.1% of the respondents), a form of sabotage that most managers rated as either a minor or moderate offense in the previous table. The next most known offenses showed a precipitous drop from the 31.1% of the respondents identifying "misinformation about a co-worker." The next most identified methods of sabotage were "gathering information…slowly" (18%) followed by creating "misinformation" (17.7%) and maliciously altering files (16.4%) - see Table 5.

These are all non-physical and generally passive in nature. The items at the bottom of the array, altering systems, hijacking content with the intent to alter it, erasing filed and

altering networks were the least known acts of sabotage. This is not to say that they are the least to occur, which we cannot speculate on; rather, these are the least known by these respondents which could speak to their invisibility, difficulty in tracking, etc.

Table 4
Incidence of and Estimation of Occurrence of Different forms of Sabotage

Specific act of information sabotage: _____ so as to harm a targeted person, department, customer, program or organizational change.		I know one of my people has done this.	I'm confident that at least one of my people has seriously considered doing this.	I'm sure at least one of my people might seriously consider this if the circumstances were right.	I'm sure none of my people have ever considered doing this regardless of the circumstances.
1.	Maliciously altering files	16.4%	8.2%	23.0%	52.5%
2.	Malicious hacking	10.0	6.7	25.0	58.3
3.	Deliberately deleting files	10.0	10.0	35.0	45.0
4.	Purposely delaying transfer of information	11.7	20.0	28.3	40.0
5.	Physically damaging software, hardware or a network	8.2	9.8	14.8	67.2
6.	Purposely altering security measures	9.8	9.8	21.3	59.0
7.	Purposely provided inaccurate information to the requestor	13.1	23.0	29.5	34.4
8.	Stealing proprietary information	11.3	14.5	27.4	46.8
9.	Purposely misdirects information	10.0	18.3	35.0	36.7
10.	Misinformation; either providing a better outlook or a worse outlook for a company	17.7	14.5	29.0	38.7
11.	Misinformation about a co-worker	31.1	23.0	24.6	21.3
12.	Hijack electronic communications to alter the content in an unfavorable manner for the sender of the information	4.9	6.6	16.4	72.1
13.	Gathering information in a low and slow manner; collecting critical information unnoticed	18.0	13.1	28.9	41.0
14.	Hold information hostage, i.e., passwords to critical systems	8.2	16.4	18.0	57.4
15.	Alter or erase backup data making recovery impossible	3.3	8.2	19.7	68.9
16.	Alter system and application logs to cover up one's activities	8.1	14.5	21.0	56.5
17.	Alter network routing to enable "man-in-the-middle" attacks and/or information capture	3.3	9.8	16.4	70.5
18.	Public release of proprietary data	9.7	11.3	21.0	58.1
19.	Taking critical systems or services off-line; a denial of service	3.4	10.2	8.5	78.0

Table 5
Results Ranked by Survey Foil: "I know this has been done."

11.	Misinformation about a co-worker	31.1%
13.	Gathering information in a low and slow manner; collecting critical information unnoticed	18.0%
10.	Misinformation; either providing a better outlook or a worse outlook for a company	17.7%
1.	Maliciously altering files	16.4%
7.	Purposely provided inaccurate information to the requestor	13.1%
4.	Purposely delaying transfer of information	11.7%
8.	Stealing proprietary information	11.3%
2.	Malicious hacking	10.0%
3.	Deliberately deleting files	10.0%
9.	Purposely misdirects information	10.0%
6.	Purposely altering security measures	9.8%
18.	Public release of proprietary data	9.7%
5.	Physically damaging software, hardware or a network	8.2%
14.	Hold information hostage, i.e., passwords to critical systems	8.2%
16.	Alter system and application logs to cover-up one's activities	8.1%
12.	Hijack electronic communications to alter the content in an unfavorable manner for the sender of the information	4.9%
19.	Taking critical systems or services off-line; a denial of service	3.4%
15.	Alter or erase backup data making recovery impossible	3.3%
17.	Alter network routing to enable "man-in-the-middle" attacks and/or information capture	3.3%

If that same data is arrayed based on the response "at least one of my people might seriously consider this" it suggests in some sense the relative probability of the occurrence of the event as perceived by these managers and executives. That data has been displayed in Table 6.

This rearrangement and examination of the percentages associated with each act suggests that almost half the items listed are believed by approximately 25% or more of the respondents to be seriously possible occurrences. In the cases of "deliberately deleting files" and "purposely misdirecting information," slightly over one in three respondents felt there was a serious chance that one or more of her/his employees would consider doing this if the circumstances were right. Nine of the acts listed had between a 15%-24% ranking and only one "denial of service" had a less than 10% ranking.

Table 6
Most Probable Form of Sabotage as Ranked by Survey Foil: "Might seriously consider…"

3.	Deliberately deleting files	35.0%
9.	Purposely misdirects information	35.0%
7.	Purposely provided inaccurate information to the requestor	29.5%
10.	Misinformation; either providing a better outlook or a worse outlook for a company	29.0%
13.	Gathering information in a low and slow manner; collecting critical information unnoticed	28.9%
4.	Purposely delaying transfer of information	28.3%
8.	Stealing proprietary information	27.4%
2.	Malicious hacking	25.0%
11.	Misinformation about a co-worker	24.6%
1.	Maliciously altering files	23.0%
6.	Purposely altering security measures	21.3%
18.	Public release of proprietary data	21.0%
16.	Alter system and application logs to cover up one's activities	21.0%
15.	Alter or erase backup data making recovery impossible	19.7%
14.	Hold information hostage, i.e., passwords to critical systems	18.0%
12.	Hijack electronic communications to alter the content in an unfavorable manner for the sender of the information	16.4%
17.	Alter network routing to enable "man-in-the-middle" attacks and/or information capture	16.4%
5.	Physically damaging software, hardware or a network	14.8%
19.	Taking critical systems or services off-line; a denial of service	8.5%

What is common about all the items listed at roughly 30% or more is that 1) they are all information, rather than equipment related, i.e., data focused in nature (deleting files, misdirecting information, providing inaccurate information, etc.) and 2) they are all very difficult to separate from common mistakes or errors. Perpetrators could claim, as was discussed in the earlier analysis, that the sabotage not really sabotage, but simple things like coding errors, legitimate mistakes, or simply delays due to time constraints. Traceable, identifiable, and deliberate acts such as hacking, stealing, altering systems, physically destroying systems, etc., appear to be thought of as seriously possible by at least one in five of the respondents.

Finally, respondents were asked about their personal knowledge of someone in the company (as opposed to being limited to people who report to them) who has intentionally committed one/some form of sabotage listed, and there were several questions about victimization. The results are shown in Table 7.

Table 7
Knowledge of Occurrence of Information Sabotage Activities

	% Yes	% No
Survey Statement:		
I have personally known someone who has intentionally committed one/some form(s) of information sabotage identified in the list.	31.0	69.0
I know for a fact one/some form(s) of information sabotage has happened here but I don't personally know anyone who has done it.	29.6	70.4
I have heard from fellow employees that it happens here but I don't personally know it is has occurred.	23.2	76.8
I think some form(s) of it happens here but I am not sure.	42.0	58.0
I have been a victim of one/some form(s) of information sabotage.	22.9	77.1
I know of other employees who have been victims.	45.1	54.9
I know of managers who have been victims.	38.6	61.4
I know of customers who have been victims.	36.2	63.8

Cross-tabulation analysis tested the hypothesis that there would be no difference in attitude toward sabotage and company size, and no difference in a second cross tabulation on knowledge of occurrence rates and company size. Acceptance would mean firm size is not an issue, i.e., large firms through the smallest of firms are not immune to information sabotage attempts. Not accepting would suggest that with this sample, at least, sabotage might be more prevalent in firms of a particular size, large vs. small for example. The cross tabulations in both tests produced no significant Chi-square values ($p<.05$) leading to acceptance of the null hypothesis in each test. Given that this is a pilot study and the sample size needs be larger before any substantive generalizations can be made, these cross tabulations and their subsequent Chi-square statistics do not provide a base upon which a supportable generalization. However, they do suggest there is at this point no reason to believe that the managers/senior executives of smaller companies feel any different about information sabotage and its probability of occurrence, than do those of large companies.

Discussion

The findings from this pilot study suggest information sabotage, in one or several forms, is not a unique occurrence; it appears to be ubiquitous. Regardless of firm size, each of the nineteen forms of sabotage presented in this survey has occurred in all the respondent's firms. Most of the forms listed were identified as major or at least moderate offenses worthy of at least disciplinary action, but many respondents felt each form of sabotage was a major offense that should result in termination. Every form of sabotage had at least one respondent indicating that s/he knows for a fact that one or more of her/his employees has been guilty of its commission. Taking critical systems off line and enabling "man in the middle" attacks were the forms least known to occur

(approximately 3% responding), while spreading misinformation about a co-worker was the most frequent form known to occur (31%). With respect to the most probable type of sabotage the respondent felt their people might do, deleting files, mis-directing information and purposely providing inaccurate information were felt to have about a one in three chance of occurring.

The most intriguing findings came from the questions about personally knowing someone who has committed information sabotage and the findings regarding victimization. Almost one in three respondents personally knows a saboteur, and slightly more than one in five respondents has been a victim. Almost half the respondents know of other employees who have been victimized. Slightly fewer than 40% know of other managers who have been victims. The most revealing statistic generated from this sample is that slightly over 36% of the respondents know of customers who have been victims. This indicates a saboteur is just as likely to take out her/his retaliatory behavior on an employee, manager or customer. These numbers are much larger than anticipated, which is symptomatic of a much larger and more deeply imbedded problem than anticipated at the start of this research. From these data gathered for this pilot study, it appears the problem of information sabotage deserves significantly more attention. If this sample reflects the reality of the larger business community, then information sabotage is a major problem with high incidence rates and high rates of victimization.

The findings presented here indicate that the forms of sabotage that are the least traceable, most passive and most indirect would be expected to be the most frequently occurring. This is not unexpected, since a person planning on engaging in some form of sabotage would want to create as much difficulty for the target as possible while maintaining the lowest profile possible.

The respondents appear to be fairly consistent in the attitude toward the forms of sabotage with respect to the forms being major offense, moderate offense, and minor offense or of no consequence. Further research on the attitudes of managers and senior executives on ethical issues relating to sabotage would appear to be justified. This research has provided insights into the apparent ubiquitous nature of information sabotage and further study on a larger sample appears to be warranted before generalizations can be substantiated.

References

Ambrose, M. L., Seabright, M. A., & Schminke, M. (2002). Sabotage in the workplace: the role of organizational injustice. *Organizational Behavior and Human Decision Process, 8*(1), 947-965.

Anderson, C. A., & Bushman, B. J. (2002). Human aggression. *Annual Review of Psychology, 53*(1), 27-52.

Anonymous, (2008). Beware the security threat posed by newly-redundant IT staff. *Banking Technology,* September, 15.

Ajzen, I., & Fishbein, M. (2005). The influence of attitudes on behavior. In D. Albarracín, B. T. Johnson, & M. P. Zanna (Eds.), The handbook of attitudes (pp. 173-221). Mahwah, NJ: Erlbaum.

Baron, R. A., & Neuman, J. H. (1996). Workplace violence and workplace aggression: evidence on their relative frequency and potential causes. *Aggressive Behavior, 22*(3)*,* 161-173.

Bellou, V. (2007). Shaping psychological contracts in public and private sectors: a human resources management perspective. *International Public Management Journal, 10*(4), 327-349.

Burton, J. P., Mitchell, T. R., & Lee, T. W. (2005). The role of self-esteem and social influences in aggressive reactions to interactional justice. *Journal of Business and Psychology, 20*(1), 131-170.

Buss, A. H. (1961). *The psychology of aggression.* New York: Wiley.

Chappell, D., & De Martino, V. (2005). *Violence at work.* Geneva: International Labor Office.

Crino, M. D. (1994). Employee sabotage: a random or preventable phenomenon? *Journal of Managerial Issues, 6*(3), 311-330.

DelCampo, R. G. (2007a). Understanding the psychological contract: a direction for the future. *Management Research News, 30*(6), 432-440.

DelCampo, R. G. (2007b). Psychological contract violation: an individual difference perspective. *International Journal of Management, 24*(1) 43-52.

Edwards, J. C., & Karau, S. J. (2007). Psychological contract or social contract? Development of the employment contracts scale. *Journal of Leadership and Organizational Studies, 13*(3), 67-78.

Forman, A. S. & Watkins, E. E. (2009). Here are 10 cases of sabotage that harmed -- or attempted to harm -- some high-profile companies. *Human Resource Executive Online*, July 1. Retrieved from http://www.hreonline.com/HRE/story.jsp?storyId=225549614&query=sabotage.

Giacalone, R. A., & Knouse, S. B. (1990). Justifying wrongful employee behavior: the role of personality in organizational sabotage. *Journal of Business Ethics, 9*(1), 55-61.

Hafer, J. C., & Gresham, G. G. (2009). Possible explanations for information sabotage: Potential research models. *Journal of Management, Spirituality & Religion, 6*(3), 233-245.

Neuman, J. H. & Baron, R. A. (1998). Workplace violence and workplace aggression: evidence concerning specific forms, potential causes and preferred targets. *Journal of Management, 24*(3), 391–419.

Rapalus, P. (1997). *1997 Computer Crime and Security Survey,* San Francisco, California: Computer Security Institute.

Rapalus, P. (2000). *Issues and Trends: 2000 CSI/FBI Computer Crime and Security Survey*, San Francisco, CA: Computer Security Institute. March 22, 2000 (press release).

Richardson, R. (2008). *2008 CSI Computer Crime & Security Survey.* San Francisco, CA: Computer Security Institute.

Richardson, R. (2010). *2010 CSI Computer Crime & Security Survey.* San Francisco, CA: Computer Security Institute.

Robinson, H. (1994). *Perception.* London: Routledge.

Robinson, S. L. & Rousseau, D. M. (1994). Violating the psychological contract: not the exception but the norm. *Journal of Organizational Behavior, 15*(3), 245-259.

Rousseau, D. M. (2001). Schema, promise, and mutuality: the building blocks of the psychological contract. *Journal of Occupational and Organizational Psychology*, *7*(4), 511-541.

Rousseau, D. M., & Tijoriwala, S. A. (1998). Assessing psychological contracts: issues, alternatives and measures. *Journal of Organizational Behavior, 19*(S1), 679-695.

Rousseau, D. M., & Tijoriwala, S. A. (1999). What's a good reason to change? Motivated reasoning and social accounts in promoting organizational change. *Journal of Applied Psychology, 84*(4), 514-528.

Skarlicki, D. P. & Folger, R. (1997). Retaliation in the workplace: the role of distributive, procedural and interactional justice. *Journal of Applied Psychology, 82*(3), 434-443.

Skarlicki, D. P., Folger, R., & Tesluk, P. (1999). Personality as a moderator in the relationship between fairness and retaliation. *Academy of Management Journal, 42*(1), 100-108.

Skarlicki, D. P., van Jaarsveld, D. D., & Walker, D. D. (2008). Getting even for customer mistreatment: the role of moral identity in the relationship between customer interpersonal injustice and employee sabotage. *Journal of Applied Psychology, 93*(6), 1335-1347.

Smith, A. D. & Rupp, W. T. (2002). Issues in cyber security: understanding the potential risks associated with hackers/crackers. *Information Management and Computer Security, 10*(4), 178-183.

Spector, P. E. (1978). Organizational frustration: A model and review of the literature. *Personnel Psychology, 31*(4), 815-829.

Stewart, S. M. (2007). An integrative framework of workplace stress and aggression. *The Business Review, 8*(1), 223-233.

Zhao, H., Wayne, S. J., Glibkowski, B. C., & Bravo, J. (2007). The impact of psychological contract breach on work-related outcomes: a meta-analysis. *Personnel Psychology*, *60*(3), 647-680.

