

# Relationship between Employees Trust and Safety of Information in Small Organizations

Santosh Mutnuru<sup>1</sup>

<sup>1</sup>PhD, Eastern Michigan University, United States

Correspondence: Santosh Mutnuru, PhD, Eastern Michigan University, United States

Received: August 16, 2018

Accepted: September 12, 2018

Online Published: September 20, 2018

doi:10.5539/ibr.v11n10p34

URL: <https://doi.org/10.5539/ibr.v11n10p34>

## Abstract

This study is trying to understand employee's perspective on how a trust of an employee has on his/her employer has any significance on safety of information from internal attacks in a small organization. The relationship between the trust of an employee on his/her employer with safety of information from internal employee attacks in small organizations has not been explored well. The study was conducted on employees who worked in small organizations which maintained all of its information in digital format. About four hundred and ninety employees responded who belong to small organizations in the Midwestern US region. The influence that employees trust on his/her employer and the safety of information was explored. The research findings revealed that there is a positive correlation between the trust of employee on his/her employer and safety of information from internal attacks in small organizations.

**Keywords:** trust, information safety, employees trust, internal attacks, security, internal employee attacks

## 1. Introduction

Up until a few decades ago, almost all information was stored in a physical format which consisted of images on a substrate. By the early 1980s the personal computer revolution began to expand. Computers started to pop exponentially all around the world. Since then, companies started to rely more on computers to store and retrieve digital information. With the prices for computation capability at an all-time low, the growing menu of applications available as solutions to traditional storage problems is forcing businesses of every size to rely more on Information storage.

### 1.1 Digital Storage Has Become a Widespread Practice

The exponential growth in volume of digital information that needs to be efficiently stored for extended periods of time and the decreasing costs of disk storage, memory, and processing have motivated all the organizations to use design of low-cost, high efficiency digital storage systems (Lawrence et al. 2011). Also, most companies started to use digital data which prompted the information to grow exponentially [Lyman et al. 2003]. With the increase of data storage, a company tends to store and archive all its information.

### 1.2 Threats to Digital Information

With the proliferation of digital information management and storage, new risks have emerged. Major concerns for organizations include protecting their information within the organization's annual budget, meeting the standards of regulations, storing large amount of personally identifiable information, ensuring that the information is safe from internal and external threats.

### 1.3 Vulnerability to External and Internal Employee Attacks

From an organization perspective, digital security attacks which include outsider attacks and insider employee attacks affect every department from small organizations to large organizations, from small privately-owned businesses to nonprofit organizations (Mutnuru, 2016). To generalize, digital security attacks can happen to any organization that uses digital information. Outsider attack varies from illegal access to information and/or monetary gain. Whereas insider employee attacks have been a major issue for all organizations, sometimes even more severe than damage that was caused by outsider attacks, as seen in the WikiLeaks and NSA surveillance incidents (Silowash et al. 2012). Insider employee attacks are real and happens all the time. Symantec's 2013 Internet Security Threat Report states that small organizations are not well prepared and are cannot protect

themselves for many external attackers (Symantec, 2013). The Symantec report reveals that in 2012, half of the targeted attacks were aimed at organizations that were less than 2,500 employees. These companies are often less careful in their cyber defenses and so make themselves low-difficulty intrusion targets, particularly for criminals.

## 2. Literature Review

### 2.1 *The Role of Employee Trust*

Trust in general is conceptualized in a variety of ways and several follow them. Luhmann's (1979) conceptualization, trust represents the level of confidence that an individual has in another to act in a fair, ethical, and predictable manner. Griffin (1967) defines trust as "the reliance upon the characteristics of an object, or the occurrence of an event, or the behavior of a person in order to achieve a desired but uncertain objective in a risky situation" (Griffin, 1967, p. 105). Carnevale and Wechsler (1992) states that trust "involves faith or confidence in the intentions or actions of a person or a group, the expectation of ethical, fair, and non-threatening behavior, and concerns for the rights of others" (Carnevale and Wechsler, 1992, p. 473). Culbert and McDonough (1986) contend that "trust pertains to whether or not one individual is able to value what another is up to and demonstrate respect for him or her particularly when the individual's need and those of the person taking the action momentarily compete" (Culbert and McDonough, 1986, p. 175).

#### 2.1.1 Measuring Employee Trust

Argyris (1964) states that trust will be positively associated with openness, experimentation with new behaviors, and nonthreatening feedback on performance. This statement is very much apt when it comes to employees trust on other employees. Zand (1972) and Boss (1978) express that high levels of trust are the key factor in effective problem solving, this can be even related to problem solving as a team in an organization. Trust is a "positive force from which cooperation is derived" (K. D. Scott 1980, p.158). Savage (1982) states that the productivity methods have trust as a basis. She believes that merely creating an atmosphere of trust can positively affect productivity without new programs or expense. Matthai (1989) defines "trust is defined as the employees' feelings of confidence that, when faced with an uncertain or risky situation, the organization's words and behaviors are consistent, and are meant to be helpful" (Matthai, 1989, p. 29).

Culbert and McDonough (1986) states that "when an individual perceives that an organizational system is not trustworthy-that the system will not recognize and reward contributions the individual seeks to make-the individual seeks to reduce his or her vulnerability by emphasizing only those performance areas that can be objectively tabulated and defended" (Culbert and McDonough, 1986, p. 179).

Luhmann (1979) states that system's trust stands beyond the experiences that influence personal trust on a daily basis (Luhmann, 1979, p. 58). This dichotomization assumes that an employees' degree of trust on his or her supervisor varies when compared to the organization as a whole. Employees trust on an organization varies based on the decisions and actions of the executive group. These images of an organization as an entity are separate from those that are formed based on the immediate contact the employee has on a daily basis with his or her supervisor. The supervisor controls the flow of information in most organizations, and access to information is a key manifestation of the level of trust in an organization (Creed and Miles 1996).

Winning employees' trust is an important element for an organization's success. Trust has long been recognized as being fundamental to cooperative relationships (Blau, 1964). In particular, employee trust is an important part of the relationship between individuals and organizations. However, the main issue has previously been "trust in whom?" (Perry & Mankin, 2004). Hunt and Aldrich (1998) suggested that direct supervisors have a stronger influence than company CEOs. In turn, trust in leaders has been tied to desirable outcomes such as job satisfaction, commitment, and OCB (Dirks & Ferrin, 2002). Morrison and Robinson (1997) stated that employees who trust their immediate managers required to tell them the truth about the company, and, if they do not, the employees feel that they are treated unfairly, which then decreases their work engagement.

Cook and Wall (1980) concluded that trust among the individuals and a team in an organization is very important and significant for both short-term and long-term stability of an organization. Cohen and Prusak (2001) believe that trust is an essential fluid for all social activities, allowing people in an organization to work together, without creating unnecessary stresses and conflicts during negotiations. Thus, the influential elements that develop employees' trust for their managers are integrity, good will with managers, and professional competency; these are necessary components that determine whether supervisors can be trusted or not (Colquitt, Scott, & LePine, 2007).

#### 2.1.2 Summary of Relevant Findings

Iacono & Weisband (1997) found that trust resulted in greater efficiency in moving through project processes.

Not all research is in agreement however concerning the necessity of trust for success, as Aubert & Kelsey (2003) found that trust was not needed for a team to deliver a quality product. Aryee, Budhwar & Chen (2002) found that trust in the organization completely moderated the relationship between work attitudes of job satisfaction, turnover intentions and organizational commitment. Kanawattanachi and Yoo's (2002) research concerning trust examined trust as being both cognitively and affectively-based. Their study hypothesized correctly that cognitive-based trust would be slightly higher than affective-based trust in a team's project in an organization. Furthermore, their study determined that high-performing teams will have higher levels of both cognitive and affective-based trust than lower performing teams, and that low performance was related to affective-based trust. These findings clearly suggest that workers will trust because they want it to be in their best interest because of an emotional reaction.

### 3. Method

Existing studies have uncovered positive links between trust and organizational commitment as per Aryee, Budhwar & Chen (2002). Iacono & Weisband (1997) found that trust resulted in greater efficiency in moving through project processes. Not all research is in agreement however concerning the necessity of trust for success. Cook and Wall (1980) concluded that trust among the individuals and a team in an organization is very important and significant for both short-term and long-term stability of an organization. But none of the studies have provided if there is a relationship between trust of an employee on his/her employer and safety of information. Lack of supporting prior literature regarding the impact of employees trust on safety of information suggest the following research question.

1. *Does the level of trust an employee has on his/her employer have any relationship with the safety of information in an organization?*

#### 3.1 Sample

A cross-sectional survey approach was taken in this study and the responses were collected using convenience random sampling on employees working in small organizations that belong to Information Technology domain in the mid-western region of the U.S. The survey used a seven-point Lickert scale which were responded by respondents based on the agreement with each item on the survey (7 – Very Strongly Agree; 6 –Strongly Agree; 5 –Agree; 4 - Neither Agree or Disagree; 3 –Disagree; 2 –Strongly Disagree; 1 –Very Strongly Disagree). 17 items on the survey related to the variables in this study and 6 related to the demographic profile of respondents to the survey.

#### 3.2 Data Collection

Employee who belong to the organizations that fall under the sample were contacted, and the researcher obtained approval to distribute a survey concerning employees trust and safety of information. Data collection was done through electronic questionnaire. Each employee in an organization was asked to complete the questionnaire. These questions did not test the employee's credibility, but it just gathered information about employees trust and safety of information.

Participants were provided with a URL in the e-mail message. A participant following the URL link was automatically directed to a website hosting the survey where it was completed. Initially, e-mail was sent to all the participants and this e-mail was sent from the organization's human-resource department. The survey instrument was constructed to gather responses regarding the constructs studied in this research project as well as responses regarding the respondent's age, education level, experience, gender and industry. One hundred and sixty responses were received; only surveys that were 100 percent complete were used. Since the human resource department distributed the survey, it is hard to determine the exact response rate. However, the estimated response rate was 32 percent based on an approximate potential sample of 490 participants.

#### 3.3 Demographic Profile of Survey Respondents

An examination of the descriptive data collected in this study uncovered several interesting findings. More females took part in the survey than males. Sixty-eight women and 63 men participated in the survey.

Age groups have been divided based on the generations, and almost all generations participated equally, which helps to minimize threats to external validity. Millennials (born from 1981-2000) who participated in the survey constituted 20.37% of the responses; Generation Xers (born 1964-1980) had a response rate of 25.92%. Baby Boomers (born 1946-1964) responded at a rate of 39.81%, and the Silent Generation (born 1922-1945) had a response rate of 13.88%.

The education level of the respondents was divided based on the following: high school, some college,

bachelor's degree, master's degree, and doctorate. Threats to external validity may have been minimized since all the education levels have been represented. The highest proportion of the level of education was 27.94%, which belongs to those respondents possessing bachelor's degrees, and the lowest proportion of the level of education was doctorate degree holders, whose response rate was 6.61%.

The experience level of the respondents was divided based on the following: 0 – 4 years (entry level), 5 – 9 years (midlevel), 10 – 14 years (senior level), and greater than 15 years (expert). Threats to external validity may have been minimized since all the experience levels are represented. The highest proportion of the level of experience is 49.3%, which belongs to those with 0 – 4 years' experience, and the lowest proportion of the level of experience is the respondents whose experience falls under 10 – 15 years and was 5.9%.

Table 1. Demographic Characteristics of the Sample

Characteristics	Attribute	Frequencies
Gender	Male	63
	Female	68
Age	Millennials (born 1981-2000)	22
	Generation X (born 1965-1980)	28
	Baby Boomers (born 1946-1964)	43
	Silent Generation (born 1922-1945)	15
Education	High School	35
	Some College	24
	Bachelor's Degree	38
	Master's Degree	30
	Doctorate (Ph.D.)	9
Experience	0 - 4 years	67
	5 - 9 years	33
	10 - 14 years	8
	15+ years	28

### 3.3.1 Crosstab between Demographics and Employee Trust

Crosstab has been performed between demographics and trust of an employee on his/her employer. Demographics items such as gender, employee's education, employee's age, and employee's experience were individually involved in a crosstab operation with trust of an employee on his/her employer.

Crosstab has been performed between employee's education and trust and the results seems to be normal. Education didn't play a significant role to identify the level of trust an employee has on his/her employer. All the values of trust and employee's education are presented in Table 2.

Table 2. Crosstab between trust and employee's education

		Low Trust	Medium Trust	High Trust	Total
EDUCATION	High School	12	11	12	35
	Associate/Some College/Certificate	8	9	7	24
	Bachelor's	10	16	12	38
	Master's	11	8	11	30
	Doctorate	2	5	2	9
Total		43	49	44	136

### 3.3.2 Crosstab between Trust and Employees Age

Crosstab has been performed between employee's age and trust of an employee on his/her employer and the results seems to be interesting. Employees who were born after 1946 and before 1964 has a prominent level of trust when compared with employees who were born after 1964. All the values of employee trust and employee's age are presented in Table 3.

Table 3. Crosstab between trust and employee's age

		Low Trust	Medium Trust	High Trust	Total
GENCOHORT	Millenials	7	9	6	22
	Generation X	13	8	7	28
	Greatest Generation	9	15	19	43
	Silent Generation	4	5	6	15
Total		33	37	38	108

### 3.3.3 Crosstab between Employees Trust and Gender

Crosstab has been performed between employee's gender and trust and the results seems to be pretty normal. Gender didn't play much role with respect to trust of an employee on his/her employer. All the values of trust and employee's gender are presented in the below Table 4.

Table 4 Crosstab between trust and employee's gender

		Low Trust	Medium Trust	High Trust	Total
GENDER	Male	21	21	21	63
	Female	21	26	21	68
TOTAL		43	40	48	131

### 3.3.4 Crosstab between Trust and Employees experience

Crosstab has been performed between employee's experience and trust of an employee on his/her employer and the results seems to be quite normal. Employees who have 10 – 14 years in the same company seems to have prominent level of trust. All the values of the employee performance and employee's experience are presented in Table 5.

Table 5. Crosstab between trust and employee's experience

		Low Trust	Medium Trust	High Trust	Total
Experience	0 – 4 years	20	23	24	67
	5 – 9 years	11	10	12	33
	10 – 14 years	1	5	2	8
	> 15 years	11	11	6	28
Total		43	49	44	136

## 4. Results

Results from crosstab analysis between employees age and employees trust has shown a positive correlation between them. Employees who were born between 1946 and 1964 has shown more trust on his/her employer than compared to other age groups. Results from the crosstab analysis between employees experience and employees trust on his/her employer has shown a positive correlation between them. Employees who have experience between 10 to 14 years in an organization shown more trust on his/her employer when compared to other levels of experience within an organization.

Results indicate that level of trust that an employee has with their employer is significantly related to organizations' safety of information. Testing the relationship between the level of trust that an employee has with their employer and organizations' safety of information indicated that the model was significant (Beta = .49, F=113.941,  $p < .001$ ), predicting 46% of variance in trust (Table 6).

Table 6. Summary of Linear Regression Analysis for Predicting the level of trust that an employee has with their employer and safety of information from internal attacks

Trust	Safety of Information	
	R <sup>2</sup>	Beta
	.460	.49***
*** p<.001    ** p<.01    * p<.05    †<.1    (n = 120)	(one-tailed)	

## 5. Conclusion

Out of the several reasons why safety of information being compromised. This paper identified one of the key findings, when an employee has less trust on his/her employer then the chances of internal employee attacks are more in a small organization which leads to less safety of information. Also, employees age and employees experience within an organization play a significant role in internal employee attacks. Employees who are born after 1964 are prone for more internal employee attacks when compared with employees who are born before 1964. Employees who have more than 10 years of experience within an organization tend to have more concern on the safety of information when compared with other levels of experience within an organization. Hence it is concluded that safety of information in an organization has direct correlation between employees' trust, employees' age and employees' experience in an organization.

## 6. Discussion

Several interesting findings emerged from the analysis of linear regression models in this study. First, it was found that higher levels of trust an employee has on his/her employer had a very significant and very positive relationship with organizations' safety of information. Which means when an employee has more trust on his/her employer then the employee will protect the information and will not try to compromise the information, which means there are very less chances of internal employee attacks. It is also identified that when an employee has less trust on his/her employer then there are more chances of compromising safety of information. These employees tend to compromise the information hence leading to internal employee attacks.

Employees who were born before 1964 has a prominent level of trust when compared with employees who were born after 1964. This leads to support the use case where employees age also has significant relation with safety of information from internal attacks. Employees who were born before 1964 will not try to compromise their organizations' information. This also leads to further argument that employees' who were born after 1964 tend to compromise their employer's information leading to internal employee attacks. Employees who have over 10 years of experience in the same company seems to have prominent level of trust when compared with other employees in the organization. This leads to support the use case where employees who have more than 10 years of experience in the same organization tend to protect the information and will not try to compromise the information leading to less number of internal employee attacks.

## 7. Limitations

This study has following limitations which are described below:

1. This research only examined the employees who worked in small organizations.
2. This study collected no information about the employees' ethnicity or their languages. It would have been beneficial and interesting to find out how ethnicity and language moderate the factors of employee's trust on the safety of organization's information.
3. The ordering of the questions might have created a mindset for the respondents that expect the same questions throughout the survey.

## 8. Future Research

The research model could be tested in more diverse sample sizes with more diverse industries. Experimental studies could be conducted which examine the developed research model. By utilizing the developed research model, these future studies could examine the impact of safety of information based on employees trust on medium and large organizations. Future studies could focus on identifying other variables that safety of information could possibly influence. Future researches could create a survey that presents the questions randomly to reduce bias in the anticipation of the questions. Future studies could also focus on the level of employee engagement and level of employee performance to determine any relation to the number of successful internal and external attacks within small organizations.

## References

- Argyris, C. (1964). Integrating the individual and the organization. New York: Wiley.
- Aryee, S., Budhwar, P. S., & Chen, Z. X. (2002). Trust as a mediator of the relationship between organizational justice and work outcomes: test of a social exchange model. *J. Organiz. Behav*, 23, 267-285. <https://doi.org/10.1002/job.138>
- Association of Certified Fraud Examiners (ACFE). (2010). Fraud report.
- Ashbaugh-Skaife, H., Collins, D., Kinney, W., & LaFond, R. (2006). The Effect of Internal Control Deficiencies on Firm Risk and Cost of Equity Capital, Working paper, University of Iowa.
- Blau, P. M. (1964). Exchange and Power in Social Life. New York: Wiley.
- Cascio, W. F. (1992). Managing human resources: productivity, quality of work life, profits (3<sup>rd</sup> ed.). New York: McGraw-Hill Inc.
- Cohen, D., & Prusak, L. (2001). In good company: How social capital makes organizations work. Harvard Business Press.
- Colquitt, J. A., Scott, B. A., & LePine, J. A. 2007. Trust, trustworthiness, and trust propensity: A meta-analytic test of their unique relationships with risk taking and job performance. *Journal of Applied Psychology*, 92, 909-927. <https://doi.org/10.1037/0021-9010.92.4.909>
- Cook, J., & Wall, T. (1980). New work attitude measures of trust, organizational commitment and personal need non-fulfillment. *Journal of Occupational Psychology*, 53, 39-52. <https://doi.org/10.1111/j.2044-8325.1980.tb00005.x>
- Covin, J. G., & Slevin, D. P. (1989). Strategic management of small firms in hostile and benign environments, *Strategic Management Journal*, 10(11), 57-75. <https://doi.org/10.1002/smj.4250100107>
- Creed, D., & Miles, E. (1996), Trust in Organizations. A Conceptual Framework Linking Organizational Forms, Managerial Philosophies, and the Opportunity Costs of Control in R. M. Kramer and T. Tyler (Eds.), Trust in organizations. Frontiers of Theory and Research. Thousand Oaks: Sage Publications, London, pp. 16-38. <https://doi.org/10.4135/9781452243610.n2>
- Culbert, S., & McDonough, J. (1986). The politics of trust and organization empowerment. *Public Administration Quarterly*, 10(2), 171-188.
- Dirks, K. T., & Ferrin, D. L. (2002). Trust in leadership: Meta-analytic findings and implications for research and practice. *Journal of Applied Psychology*, 87(4), 611-628. <https://doi.org/10.1037/0021-9010.87.4.611>
- Griffin, K. (1967). The contribution of studies of source credibility to a theory of interpersonal trust in the communication process. *Psychological Bulletin*, 68, 104-120. <https://doi.org/10.1037/h0024833>
- Guide to size standards. Retrieved from <http://www.sba.gov/content/guide-size-standards>
- Higgins, K. J. (2013). Small Businesses Now Bigger Targets in Cyberattacks. Retrieved from <http://www.darkreading.com/government-vertical/small-businesses-now-bigger-targets-in-c/240153043>
- Lawrence, L. Y., Kristal, T. P., Darrell, D. E., & Long, K. G. (July 2011). Transactions on Storage (TOS). *ACM* 7(2).
- Kane, J. S. (2000). Accuracy and its determinants in distributional assessment. *Human Performance*, 13(1), 47-84. [https://doi.org/10.1207/S15327043HUP1301\\_3](https://doi.org/10.1207/S15327043HUP1301_3)
- Lyman, P., Varian, H. R., Searingen, K., Charles, P., Good, N., Jordan, L. L., & Pal, J. (2003). How much information? 2003. <http://www.sims.berkeley.edu/research/projects/how-much-info-2003/>
- Matthai, J. M. (1989). Employee perception of trust, satisfaction, and commitment as predictors of turnover intentions in a mental health setting. Dissertation Abstract International.
- Morrison, E. W., & Robinson, S. L. (1997). When employees feel betrayed: a model of how psychological contract violation develops. *Academy of Management Review*, 22, 226-256. <https://doi.org/10.5465/amr.1997.9707180265>
- Mutnuru, S. (2016). The role of internal controls on employees' engagement in small Organizations. *Journal of Business Studies Quarterly*, 7(4), 102-114.
- Mutnuru, S. (2015). Users' Perspective on the Relationship between Internal Controls and Key Constructs.

- Pressly, T. R. (2009). Combining Strategic Management and Internal Control Processes: A Recipe for Entrepreneurial Competitive Advantage. *The Entrepreneurial Executive*, 14, 49-64.
- Savage, D. (1982). Trust as a productivity management tool. *Training and Development Journal*, 36(2), 54-57.
- Silowash, G., Cappelli, D., Moore, A., Trzeciak, R., Shimeall, T., & Flynn, L. (2012). Common Sense Guide to Mitigating Insider Threats, 4th Edition (CMU/SEI-2012-TR-012). Retrieved from Software Engineering Institute, Carnegie Mellon University website: <http://www.sei.cmu.edu/library/abstracts/reports/12tr012.cfm>

### **Copyrights**

Copyright for this article is retained by the author(s), with first publication rights granted to the journal.

This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/4.0/>).