Open Access License Notice

Evolution of Information Security Issues in Small Businesses

Abstract

Small businesses often display a lack of concern towards cybercrime and information security problems. A lack of concern usually results in delayed or incorrectly implemented security measures, which increases vulnerability to cybercrime. This paper presents an empirical study of 122 small business owners from the state of Hawaii with regards to their information security concerns. These results are compared with earlier studies conducted in 2000 and 2003. The results of this study showed a significant evolution of information security issues within small businesses. This research suggests that small businesses leaders need to demonstrate leadership, technical knowledge and actions to broaden their preparation against a range of information security issues and problems. The findings may be applicable to small business leaders who proactively search for a cost-effective and optimal combination of leadership styles, technologies, and policies that will mitigate the evolving threats of cybercrime and information security problems.

1. Introduction

Globalization and increased reliance on the internet has forced many organizations to rely on computer and networking technology for the storage of valuable company and personal information [13]. Many small businesses have embraced internet technologies to reach out to their customers, partners, and employees from around the world [11]. Proliferation of online activity and e-commerce has attracted the attention of existing criminal organizations and a new breed of cybercriminals [17].

Cybercriminals engage in online attacks that exploit vulnerabilities and deficiencies within the cyber defenses of organizations [35]. Because of size, resource, and skill constraints, small businesses are often ill-prepared to combat the emerging threats of cybercrime [29]. Small business owners and key employees with effective leadership styles can help prioritize actions needed to combat cybercrime and mitigate information security concerns [25]. Conversely, ineffective leadership styles can lead to passive or reactive measures against cybercrime, which can lead to business damages and losses [17]. Phishing, a deceptive strategy to gain personal information the target might not otherwise divulge, is an increasingly common form of computer attack [13].

Key similarities and differences exist between cybercrime and crime carried out by traditional means. The online nature of cybercrime allows for criminals to survey potential victims from afar and attack them when they least suspect an intrusion. Wall [38] noted that software viruses, spyware, and malware could embed themselves in the computer systems of small businesses and track their activities and transactions. Covert surveillance of a small business could lead to theft of information without the awareness [38].

Current research indicates that the information systems of small businesses in the United States are vulnerable to cybercrime [1, 4, 17, 26]. The problem is small businesses often display a lack of concern towards information security problems [17]. A lack of concern usually results in delayed or incorrectly implemented security measures, which increases vulnerability to cybercrime [3, 12].

This study examined the problem by determining whether and to what degree any relationship exists between leadership styles and the level of concern for information security problems. The study then compared the information security problems from previous studies conducted in 2000 and 2003. The general population for the study included small businesses located in the state of Hawaii. The results of this study provides small business leaders with information useful in assessing their level of concern and determining which leadership styles are the most effective in mitigating information security problems.

The remainder of the paper is structured as follow: section 2 security issues and concerns within small businesses; section 3 describes the study design in detail; section 4 presents results from the study; section 5 provides a comparison with earlier studies conducted in 2000 and 2003 and sections 6 and 7 concludes the paper with recommendations and conclusions.

2. Security issues within small businesses

Cybercrime is not only relevant to large corporations, but to the millions of small businesses in the United States [17]. According to the US Small Business Administration and the Small Business Act, a small business is an independently owned entity and not dominant in its field of operation [31]. The US Small Business Act also states that the size definition of a small business varies by industry. The Office of Advocacy, of the US SBA, defines a small business as a business having 500 or fewer employees. This study used US SBA definitions and classifications.

Small businesses play a significant role in the US economy [13]. According to the US SBA's Office of Advocacy, the US had 17,000 large businesses and approximately 25 million small ones in 2005. Small businesses generated 2.4 times more innovations than large businesses [13]. According to the US SBA, small businesses employ half of all private sector employees and pay half of the total US private payroll.

Small businesses in the US have generated 60 to 80% of net new jobs annually over the last decade and created more than 50% of nonfarm private gross domestic product [13]. Economic figures indicate the importance of small businesses to the US economy and the potential for negative economic impacts from cybercrime [10]. A coordinated cyber threat against small businesses might readily impact a significant section of the US economy [33]. Because small businesses are so important to the US economy, preparation against the evolving threat of cybercrime is important [10].

In regard to their preparations against cybercrime, small businesses can be divided into three categories [33]. According to the report on the state of small business security [33], one category consists of "mom and pop" businesses whose business computers also serve as the owners' home computers. Small businesses in the "mom and pop" category have basic anti-virus and security software in place and rarely rely on skilled professionals for security assistance. The report on the state of small business security also described a second category of small companies with a few hundred employees and a dedicated information technology (IT) staff [10]. According to the US CSI/FBI study [10], small businesses with a few hundred employees rely on the knowledge and expertise of their key IT personnel for cyber security.

The third and final category included small businesses that outsource most of their security requirements to third-party vendors [33]. According to the report on the state of small business security [33], vendors provide the level of security needed to prevent cybercrime and enable recovery from security breaches. Small businesses that outsource information security depend upon on the outside vendor's training and reliability for their security needs [10]. According to the US CSI/FBI study [10], reliance on an external vendor introduces risks but also benefits in that it removes the need of a small business to train and retain skilled IT employees to combat cybercrime.

Unlike large businesses with dedicated IT resources, small businesses often lack the skills, resources, and infrastructure to tackle cybercrime and even to conduct security assessments [17]. According to Gupta and Hammond [17], small businesses frequently fail to deploy comprehensive and effective security policies. Because of ongoing challenges, cybercriminals increasingly target small instead of large businesses for identity theft and other cybercrimes [10].

The existing literature on cybercrime and cyber security focuses on the needs of large organizations that have thousands of employees, complex security needs, and large computer systems [1]. The literature on leadership styles and information security concerns within small businesses is very limited. The literature gap may be due to the evolution of cybercrime, which initially targeted the computer systems of large corporations and government organizations [17].

As the cyber security efforts of large organizations and the government have expanded and improved, the trends of cybercrime have shifted to vulnerable targets like small businesses [38]. According to the Symantec Threat Report of 2005 [34] cybercriminals increasingly focused on identity theft and fraud for motives of financial gain. The shift in the orientation of cybercriminals over the past few years may help to explain the present literature gap regarding the impact of cybercrime on small businesses [1, 17].

3. Study design

This research study used a quantitative, descriptive, correlational methodology to investigate a possible relationship between the particular leadership styles of small business owners (independent variables) and the level of concern for information security problems (dependent variables) within small businesses in Hawaii. The study defined a "small business" as one with 500 or fewer employees, according to the United States Small Business Administration [31]. This study utilized the Multifactor Leadership Questionnaire (MLQ) instrument [7], to assess each company's leadership style (independent variable) and the Small Business Security Survey instrument [29] to determine the level of concern for information security problems within each small business (dependent variable).

For the first part of the research, a pilot study was conducted with 10 small businesses who are members of the various chambers of commerce and trade associations within Hawaii. The pilot study participants, randomly selected from the study population were small business owners who fulfilled the eligibility criteria of the study population. The randomly selected 10 businesses represented different industries, and had different number of employees. Five businesses belonged to the Chamber of Commerce of Hawaii [9] and five businesses belonged to the Small Business Hawaii (SBH) [32] trade association.

Over two weeks, an online survey was distributed to all 10 participants through email. The instructions in the email directed the participants to an online survey hosted by Zoomerang [39], a commercial provider of online surveys. The researcher followed up any survey responses needing clarification with phone calls. The pilot study sought to ensure that the participants clearly understood the survey questions; that the survey was adequate for answering the research questions; and that the online survey was user-friendly enough for participants to complete it in 10 minutes.

The second part of the current research involved an online survey of 800 small businesses who, as mentioned previously, are members of the various chambers of commerce and trade associations within Hawaii. Businesses that belong to more than one organization were included only once in the study population, in order to avoid duplication. The online survey used two previously validated, reliable and broadly used research survey instruments [7, 29].

The third part of this study involved triangulation and the random selection of 10 small businesses from the list of valid respondents to the online survey. Interviews were conducted with 10 businesses to help triangulate the results of the online survey and to confirm or dispute the findings. Triangulation helped reduce the chances for systematic error because triangulation provided a strategy for obtaining the same information through different methods [28].

3.1 Study variables

The study contained 14 dependent variables. As shown in Table 1, each represented a specific information security problem that a small business may face [29]. Using a Likert scale, the study examined the level of concern for each security problem.

Table 1. 14 Dependent Variables

Information security problem	Examples of problem in small businesses
Insider access abuse	Unauthorized login by employees
Viruses	Programs that enter through attachments in email
Power failure	Loss of data due to abrupt shutdown of computers
Software problems	Vulnerable software due to absence of patches

Data integrity	Corruption of customer list or sales data
Transaction integrity	Corruption of financial transaction with bank
Outsider access abuse	Unauthorized entry by former employees
Data secrecy	Confidentiality of payroll information
Data availability	Availability of access to time sheet data
Data theft	Theft of confidential employee information
Data sabotage	Intentional destruction of financial data
User errors	Accidental erasure of data by untrained user
Natural Disaster	Damage to computer systems from floods
Fraud	Impersonation and deceit used to elicit information

The three independent variables, as shown in Table 2, were the transformational, transactional, and passive-avoidant leadership styles as defined by Bass and Avolio [7]. The study hypothesized that effective leadership styles (the independent variables, listed in Table 2) would foster concern for information security problems (the dependent variables, listed in Table 1) within small businesses.

Table 2. Three Independent Variables

Leadership styles	Examples in small businesses
Transformational	Visionary, dynamic owner
Transactional	Leader focused on costs/benefits
Passive-avoidant	Absentee, unavailable leader

3.2 Hypothesis

The research study employed three statistical hypotheses to measure the relationship(s) among three independent variables (three leadership styles) and 14 dependent variables (information security problems). The H0 represented the null hypothesis and Ha the alternative hypothesis. The following hypotheses were tested, based on a quantitative research methodology, to answer the research questions.

Hypothesis 1

$H1_0$: There is no relationship between the transformational leadership style score and the level of concern for information security problems within small businesses.

$H1_a$: There is a relationship between the transformational leadership style score and the level of concern for information security problems within small businesses.

Hypothesis 2

$H2_0$: There is no relationship between the transactional leadership style score and the level of concern for information security problems within small businesses.

$H2_a$: There is a relationship between the transactional leadership style score and the level of concern for information security problems within small businesses.

Hypothesis 3

$H3_0$: There is no relationship between the passive-avoidant leadership style score and the level of concern for information security problems within small businesses.

$H3_a$: There is a relationship between the passive-avoidant leadership style score and the level of concern for information security problems within small businesses.

4. Study results

The theoretical framework of this research study was based on the full range leadership model of Bass and Avolio [7]. The study used the MLQ instrument that includes a Likert scale to measure three specific leadership styles (defined here as independent variables) of small business owners [7]. The MLQ instrument assesses three leadership styles by investigating nine behavioral factors. Through extensive factor analysis in 2003, Bass and Avolio [7] have identified the five behavioral factors of the transformational leadership style as follows: idealized attributes (IA), idealized behaviors (IB), inspirational motivation (IM), intellectual stimulation (IS), and individualized consideration (IC).

Through confirmatory factor analysis, Bass and Avolio also have identified two behavioral factors of transactional leadership style: contingent reward (CR) and management-by-exception (active) (MBEA). Finally, their factor analysis determined the two behavioral factors of laissez-faire or passive-avoidant leadership style: passive management-by-exception (passive) (MBEP) and laissez-faire (LF).

The findings indicated that transactional leadership style is significantly related to 11 out of 14 information security problems. This implies that the higher the level of transactional leadership style score, the higher the level of concern for 11 information security problems.

The transactional leadership factor of Management by Exception Active (MBEA) is significantly related to 10 out of 14 information security problems. This implies that the higher the practice of active management by exception, the higher the level of concern for 10 information security problems.

Seven out of 14 information security problems were related to more than one leadership factor. Using stepwise multiple regression analysis, the transformational factor of Idealized Influence Attributes (IIA) and the transactional factor Management by Exception (MBEA) were the best predictors for the seven information security problems. This implies a combination of transformation and transactional leadership styles to prepare against seven common security problems.

The findings also indicated that transformational leadership style was significantly related to the level of concern for two information security problems, and passive-avoidance leadership was related to one information security problem.

Using the Pearson product-moment correlation, there is a statistically significant ($p <= 0.05$), positive correlation between transformational leadership style score and the level of concern for two (out of 14) information security problems. These two problems are data secrecy and data availability. Thus, the null hypothesis $H1_0$ is rejected.

Likewise, there is a statistically significant ($p <= 0.05$), positive correlation between transactional leadership style score and the level of concern for 11 (out of 14) information security problems. Therefore, the null hypothesis $H2_0$ is strongly rejected.

Finally, there is a positive correlation between passive-avoidance leadership style score and the level of concern for one (out of 14) information security problems, power failure. While the null hypothesis $H3_0$ is rejected, it is not as strongly rejected as $H1_0$ and $H2_0$.

5. Evolution of security issues and concerns

The study results of 2008 (N=122) were compared to similar studies, using the same survey, conducted by Ryan [29] in 2000 and Gupta [17] in 2003. The study by Ryan covered small businesses in the United States with particular focus on businesses located in the state of Maryland. 209 responses were collected from the study by Ryan (N=209). Gupta focused on the Chamber of Commerce in the South Eastern United States and collected responses from 138 small business (N=138). Table 3 describes the changes in access to computers and networks over the years for small businesses, with sharp growth in usage over the years for all employees, contractors and family members.

Table 3. Access to Computers and Networks

	2000	2003	2008
All Full-time Employees	57.4%	49.3%	72.1%
Part-time Employees	17.2%	18.8%	38.5%
Temporary Employees	21.3%	8.7%	21.3%
Some Emp, job related	31.6%	49.3%	20.5%
Contractors	6.7%	3.6%	18%
Family members, friends	24.4%	2.2%	15.6%
Customers	6.2%	6.5%	12.3%
E-commerce partners	1.9%	0.7%	4.9%

Table 4 below displays the changes in information security policies and procedures within small businesses. The results suggest an increase in policies and procedures in most categories, especially in the areas of information security policy and procedures, and computer misuse and data destruction.

Table 4. InfoSec Policies and Procedures

	2000	2003	2008
Data Recovery Procedures	39.7%	47.1%	50%
Information Security Policy	30.6%	40.6%	49.2%
Information Security Procs	23%	32.6%	45.9%
Computer Use Policy	24.9%	42.8%	44.3%
Proprietary Data Use Policy	18.2%	26.1%	38.5%
Communication Use Policy	13.9%	25.4%	32%
Data Destruct Procedures	12.9%	21%	27%

Comp Emergency Response Plan	13.4%	18.8%	26.2%
Business Continuity Policy	21.5%	23.9%	20.5%
Comp Emergency Response Team	7.18%	13.8%	18%
Media Destruction Procedures	6.7%	9.4%	17.2%
Info Sensitivity Coding	13.4%	25.4%	11.5%

Table 5 below displays the changes in the technologies used by the survey respondents to prevent, detect, and resolve information security problems. The results indicate a sharp increase in the use of firewalls, shredders and intrusion detection systems, but a surprising decline in the use of system access control and redundant systems.

Table 5. Information Security Technologies

	2000	2003	2008
Anti-virus Software	87.1%	56.5%	95.9%
Firewalls	25.8%	42.8%	90.2%
Power Surge Protectors	70.3%	79.7%	84.4%
Data Backup Systems	75.1%	65.2%	71.3%
Shredders	44.5%	48.6%	68.9%
Encryption	25.4%	18.8%	41.8%
System Access Control	72.7%	58%	39.3%
Intrusion Detection	22.5%	25.4%	37.7%
Facility Access Control	14.4%	17.4%	26.2%
Redundant Systems	45.5%	34.8%	25.4%
Data Segmentation	28.7%	23.9%	21.3%
System Activity Monitor	15.8%	21%	20.5%
Security Eval Systems	11.5%	8.7%	13.9%
Media Degaussers	3.3%	0.7%	5.7%
Dial-back Modem	10%	8.7%	2.5%

Table 6 below displays the changes in information security issues and problems experienced by the survey respondents in two separate studies conducted in 2000 and 2008. The results indicate that data corruption and problems with viruses and malicious software remain the highest concerns for businesses.

Table 6. InfoSec Experiences

	2000	2008
Data Corrupted or Partially Lost	28.7%	19.7%
Problems with Virus/Malicious SW	20.6%	18.0%
Emps Abused Internet Privileges	6.7%	12.3%
Problems with Reliability of IS	18.2%	12.3%
Experienced IS Incident	8.6%	6.6%
Outsider Break in to IS	1.9%	5.7%
Insider Abused Info Privileges	3.3%	5.7%
Victim of Fraud	3.8%	4.1%
Lost Money due to IS problem	9.1%	3.3%
Victim of a Natural Disasters	3.3%	3.3%
Computer Equipment Stolen	2.9%	3.3%
Proprietary Data Stolen	1.0%	2.5%
Secret Information Divulged	1.9%	2.5%

6. Recommendations for small businesses

The study highlights the need to complement the benefits of transformational and transactional leadership styles with effective policies and updated technologies that mitigate information security problems. Small businesses cannot rely primarily on basic technologies such as anti-virus software, firewalls, and power surge protectors, the top three technologies in Table 6, to protect against cybercrime. Likewise, small businesses cannot rely primarily on basic data recovery procedures and information security policies and procedures for protection against cybercrime.

The first recommendation for small business leaders is to introduce a systematic and consistent system of leadership assessment within their organization. The Multifactor Leadership Questionnaire (MLQ), available from Mind Garden Inc. [23], is a valid and reliable survey instrument for assessing leadership styles within a small business. The results of this research study highlight the importance of three leadership factors that are components of transformational and transactional leadership styles. These leadership factors are Idealized Influence Attributes (IIA), Contingent Reward (CR) and Management-by-Exception Active (MBEA). Small business leaders can evaluate their scores on these three leadership factors by using the MLQ (Rater Form) with their subordinates.

The second recommendation is for small businesses to conduct an audit of their information security. A web site [27] and guide published by the US Department of Homeland Security [18] provides a detailed

checklist to conduct security assessments within small businesses. Additional detailed guides from SANS [30], NW3C [26] and ISO [20] provides a risk audit for very small businesses, with 10 or less employees, who were the primary respondents for this research study.

The US National Institute of Standards and Technology (NIST) [24], in conjunction with the US Small Business Administration (SBA) [31], Federal Trade Commission (FTC) [15] and the US Federal Bureau of Investigation (FBI) [14], conducts a series of regional workshops on IT security for small businesses. The emphasis of these workshops is practical advice that small business leaders can apply to their business to improve IT security and mitigate information security problems [24, 19]. Security technology and guidance for small businesses can be obtained from the websites of leading technology vendors such as Microsoft [22], Symantec [34], McAfee [21], Cisco [8], and ADT [2].

The third recommendation is to utilize a combination of leadership styles, technology and policy to combat specific security problems and concerns. The key is that one leadership style is not applicable to all security problems, and that technology and policy solutions need to be augmented with leadership and knowledge.

7. Conclusions

This research study is socially significant in its finding that leadership styles are statistically significant when it comes to mitigating information security issues and concerns within small businesses. Small business leaders are preoccupied with everyday business issues and concerns and often display a lack of concern towards information security problems [17]. A lack of concern usually results in delayed or incorrectly implemented security measures, which increases vulnerability to cybercrime [3, 12].

This research has demonstrated the need for effective transactional and transformation leadership styles that will enable small business leaders to prioritize their efforts to mitigate cybercrime. An optimal combination of leadership styles, security policies and technology will enable small businesses to prevent and combat cybercrime.

8. References

[1] Adamkiewicz, S. L. (2005). *The correlation betweenproductivity and the use of information security controls in small businesses.* The George Washington University, United States -- District of Columbia.

[2] ADT. (2008). Small business security and alarm systems. Retrieved January 15, 2013, from https://www.adt.com/wps/portal/adt/small_business/

[3] Andress, A. (2003). Surviving security: How to integrate people, process and technology. New York: Auerbach Publications.

[4] Baker, W. H., & Wallace, L. (2007). Is information security under control? IEEE Security & Privacy.

[5] Bass, B. M. (1985). Leadership and performance beyond expectations. New York: Free Press.

[6] Bass, B. M. (1990). Bass & Stogdill's handbook of leadership: Theory, research, and managerial applications (3rd ed.). New York: Free Press.

[7] Bass, B. M., & Avolio, B. (2004). The multifactor leadership questionnaire: Sampler set.

[8] Cisco. (2008). Small and medium business security. Retrieved January 15, 2013, from http://www.cisco.com/en/US/netsol/ns643/networking_solutions_packages_list.html

[9] CoCHawaii. (2007). The Chamber of Commerce of Hawaii. Retrieved January 15, 2013, from http://www.cochawaii.com/.

[10] CSI/FBI. (2006). Computer Crime and Security Survey XI Annual. Retrieved January 15, 2013, from http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf.

[11] Day, K. (2003). Inside the security mind: Making decisions. Upper Saddle River, NJ: Prentice Hall.

[12] DeZulueta, M. (2004). A novel neural network based system for assessing risks associated with information technology security breaches. Florida International University, United States -- Florida.

[13] Easttom, C. (2006). Computer security fundamentals. Upper Saddle River, NJ: Prentice Hall.

[14] FBI. (2005). 2005 FBI Computer Crime Survey. Retrieved January 15, 2013, from www.digitalriver.com/v2.0-img/operations/naievigi/site/media/pdf/FBIccs2005.pdf.
[15] FTC. (2008). Federal trade commission - identity theft site. Retrieved January 15, 2013, 2008, from http://www.ftc.gov/bcp/edu/microsites/idtheft//
[16] GISS. (2006). Global Information Security Survey. Retrieved January 15, 2013, from http://www.ey.com/Global/download.nsf/International/TSRS_-_GISS_2006/$file/EY_GISS2006.pdf.
[17] Gupta, A., & Hammond, R. (2005). Information systems security issues and decisions for small businesses: An empirical examination. Information Management & Computer Security, 13(4), 297.
[18] Homeland Security. (2004). Tools for small business. Retrieved January 15, 2013, from http://www.ntsbdc.org/docs/sba_homeland_security.pdf
[19] IC3. (2006). *Internet Crime Complaint Center.* Retrieved January 15, 2013, from http://www.ic3.gov/.
[20] ISO/IEC. (2005). *ISO/IEC 17799:2005 Information technology - security techniques.* Retrieved October 9, 2007, from http://www.iso.org/iso/information_security.
[21] McAfee. (2007). McAfee for small and medium business. Retrieved January 15, 2013, from http://www.mcafee.com/us/smb/index.html.
[22] Microsoft. (2007). *Security Guidance Center.* Retrieved January 15, 2013, from http://www.microsoft.com/smallbusiness/support/computer-security.mspx.
[23] MindGarden. (2008). *Multifactor Leadership Questionnaire* Retrieved January 15, 2013, from http://www.mindgarden.com/products/mlq.htm
[24] NIST. (2008). SBC computer security workshops. Retrieved January 15, 2013, from http://csrc.nist.gov/groups/SMA/sbc/workshops.html
[25] Northouse, P. G. (2004). *Leadership: Theory and practice*. Thousand Oaks, CA: Sage.
[26] NW3C. (2006). *National White Collar Crime Center.* Retrieved January 15, 2013, from http://www.nw3c.org/.
[26] O'Rourke, M. (2003). Cyberattacks prompt response to security threat. *Risk Management, 50*(1), 8.
[27] ReadyBusiness. (2008). Ready.Gov - small business readiness. Retrieved January 15, 2013, from http://www.ready.gov/business/index.html
[28] Rubin, A., & Babbie, E. (2005). *Research methods for social work* (5th ed.). Belmont, CA: Brooks/Cole - Thomson.
[29] Ryan, J. J. C. H. (2000). *Information security practices and experiences in small businesses.* The George Washington University, United States -- District of Columbia.
[30] SANS. (2003). Case study: A risk study of a very small business. Retrieved January 15, 2013, from http://www.sans.org/reading_room/whitepapers/casestudies/1243.php
[31] SBA. (2007). US Small Business Administration. *Advocacy Small Business Statistics and Research.* Retrieved October 9, 2007, from http://app1.sba.gov/faqs/faqindex.cfm?areaID=24.
[32] SBH. (2007). *Small Business Hawaii.* Retrieved January 15, 2013, from http://www.smallbusinesshawaii.com/SBHabout.html.
[33] *The state of small business security in a cyber-economy: Hearing before subcommittee on regulatory reform and oversight of the committee on small business*, US House of Representatives, 109th Congress Second Sess. (2006).
[34] Symantec. (2007). Small and mid-sized business products. Retrieved January 15, 2013, from http://www.symantec.com/smb/products/index.jsp.
[35] Szor, P. (2005). *The art of computer virus research*. Upper Saddle River, NJ: Symantec Press.
[38] Wall, D. S. (2004). Surveillant internet technologies and the growth in information capitalism: Spams and public trust in the information security. In R. E. K. Haggerty (Ed.), *The new politics of surveillance and visibility*. Toronto: University of Toronto Press.
[39] Zoomerang. (2007). *Zoomerang Online Survey Tool.* Retrieved January 15, 2013, from http://info.zoomerang.com/.