LEADERSHIP STYLES AND INFORMATION SECURITY IN SMALL BUSINESSES:
RESULTS OF AN EMPIRICAL INVESTIGATION

by

Debasis Bhattacharya

© 2008 by DEBASIS BHATTACHARYA
ALL RIGHTS RESERVED
TABLE OF CONTENTS

LIST OF TABLES ........................................................................................................ iv
LIST OF FIGURES ......................................................................................................... v

Introduction .................................................................................................................. 1

Background of the Problem ......................................................................................... 2

Statement of the Problem ............................................................................................. 4

Dependent and Independent Variables ......................................................................... 5

Research Design .......................................................................................................... 7

Results of Research Questions and Hypothesis ......................................................... 8

Research Question 1 and Hypothesis 1 ................................................................... 8
Research Question 2 and Hypothesis 2 ................................................................... 14
Research Question 3 and Hypothesis 3 ................................................................... 18

Implications ............................................................................................................... 21

Implications for Global Leadership ...................................................................... 21
Implications for Small Business Leaders .............................................................. 23

Recommendations ..................................................................................................... 25

Recommendation 1: Leadership Styles Assessment .............................................. 25
Recommendation 2: Information Security Assessment ......................................... 27
Recommendation 3: Application of Cybercrime Leadership ............................. 28

Recommendations for Future Research ................................................................. 32

Conclusions ................................................................................................................. 34

REFERENCES ............................................................................................................. 35

APPENDIX A: FREQUENCY TABLES ............................................................. 40
APPENDIX B: CHI-SQUARE TESTS ........................................................... 43
APPENDIX C: PEARSON’S CORRELATIONS............................................ 46
APPENDIX D: MULTIPLE REGRESSION ANALYSIS ............................... 50
APPENDIX E: SMALL BUSINESS SECURITY CHECKLIST ..................... 54
APPENDIX F: RESOURCES FOR CYBERCRIME VICTIMS .................... 58
LIST OF TABLES

Table 1 14 Dependent Variables ................................................................. 5
Table 2 Three Independent Variables .......................................................... 6
Table 3 Pearson's Correlations - Transformational Leadership Style .......... 9
Table 4 Pearson's Correlations - Transformational Leadership Factors ...... 11
Table 5 Multiple Regression Analysis - Predictors of Data Secrecy .......... 12
Table 6 Multiple Regression Analysis - Predictions of Data Availability .... 13
Table 7 Pearson's Correlations - Transactional Leadership Style .......... 15
Table 8 Pearson's Correlations - Transactional Leadership Factors .......... 17
Table 9 Pearson's Correlations - Passive-Avoidance Leadership Style .... 19
Table 10 Pearson's Correlations – Passive-Avoidance Leadership Factors .... 20
Table 11 Cybercrime Leadership using Leadership Style Score ................. 29
Table 12 Example of Cybercrime Leadership .............................................. 30
Table 13 Cybercrime Leadership, Technology and Policy ....................... 31
LIST OF FIGURES

Figure 1. Leadership Augmentation Model for Cybercrime............................. 22

Figure 2. Cybercrime Leadership Framework Overview for Small Business ... 23

Figure 3. Cybercrime Leadership Framework Details for Small Business ...... 24

Figure 4. Assessment of Key Leadership Factors ............................................ 26

Figure 5. Computation of Leadership Style Scores......................................... 27

Figure 6. Basic Information Security Assessment (Easttom, 2006)................... 28
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 (Easttom, 2006). Many small businesses have embraced internet technologies to reach out to their customers, partners, and employees from around the world (Day, 2003). Proliferation of online activity and e-commerce has attracted the attention of existing criminal organizations and a new breed of cybercriminals (Gupta & Hammond, 2005).

Cybercriminals engage in online attacks that exploit vulnerabilities and deficiencies within the cyber defenses of organizations (Szor, 2005). Because of size, resource, and skill constraints, small businesses are often ill-prepared to combat the emerging threats of cybercrime (Ryan, 2000). Small business owners and key employees with effective leadership styles can help prioritize actions needed to combat cybercrime and mitigate information security concerns (Northouse, 2004). Conversely, ineffective leadership styles can lead to passive or reactive measures against cybercrime, which can lead to business damages and losses (Gupta & Hammond, 2005).

The first purpose of this quantitative, descriptive, correlational research study was to investigate leadership styles and assess the level of concern towards information security problems within small businesses that belong to various chambers of commerce or trade associations within the state of Hawaii. The second purpose of this study was to determine the degree of a possible relationship between leadership styles and the level of concern towards information security problems within small businesses.
Background of the Problem

Studies identified several major categories of cybercrime that affect small businesses in the United States (Anat & John, 2003; Easttom, 2006; Reid, 2003). Spam (unsolicited email) crowds company inboxes and carries with it the threat of malicious attachments and viruses that can cause further damage (Reid). Small businesses contend with viruses, executable programs that can replicate themselves speedily and stealthily on many computers (Easttom). Virus detection software can protect against cybercrime, yet computers without the necessary software are susceptible to virus attacks (Campbell, 2004). According to the US CSI/FBI Survey (2006) virus attacks constituted the single biggest threat of financial loss to United States (US) businesses. Denial of Service attacks intend to overwhelm the computer networks of a target business (Anat & John). For example, cyber extortionists may launch a DoS attack on a network that provides email service to many thousands of small businesses (Lepofsky, 2006).

Phishing, a deceptive strategy to gain personal information the target might not otherwise divulge, is an increasingly common form of computer attack (Easttom, 2006). According to Easttom, incidents of phishing are rising more rapidly than other forms of cyber attacks. In a phishing attack, the victim unsuspectingly provides banking, financial, or personal information to a website that impersonates a real one. For example, a fake website from a bank controlled by cyber criminals may trick unsuspecting small businesses into disclosing key online banking information. Loss of information usually leads to identity theft and allows the cyber criminals to obtain new credit cards or transfer funds out of illegally accessed bank accounts (Diller-Haas, 2004). Over the first six months of 2006, the security software vendor Symantec’s Probe Network (Symantec, 2007) detected 157,477 unique phishing messages total—an average of 865 unique phishing messages per day. According to Symantec (2007), the phishing results
represented an 81% increase over the messages detected in the last half of 2005, and a 61%
increase over those detected in the first half of 2005.

Bot (short for robot) networks are threats against business organizations and home users
(Easttom, 2006). According to Easttom, a bot program installs itself on a system, thus enabling a
cybercriminal to have remote control of the computer. Bot-controlled computers, assembled into
a bot network, can spawn large-scale attacks against a target victim (Day, 2003). Symantec
(2007) reported that the United States had over one quarter of all the world’s bot-infected
computers between July and December of 2005. Bot-infected computers, many of which belong
to small businesses in the United States, may someday provide a foundation for cyber terrorism
(Foltz, 2004).

Cybercrimes against small businesses can be perpetrated by ex-employees who still have
secure access to company computer systems (Furnell et al., 2006). Employees or workers may be
the weakest link in the security infrastructure of a business (Hall, 2003). According to Hall,
malicious activities on the part of employees or ex-employees can significantly disrupt small
business activities. Competitors and rivals as well can use methods such as bot-nets to damage
the operations and reputation of a small business (Knight, 2004).

Small business owners are often entrepreneurs who set the company vision, demonstrate
problem-solving and decision-making capabilities, take risks, and launch strategic initiatives
(Fernald et al., 2005). According to one study of 194 small businesses (O'Regan et al., 2005),
effective leadership styles is likely to lead to better business performance. O’Regan et al. claimed
that small businesses that emphasize any specific leadership style show better performance than
businesses with weak or uncertain leadership styles.
According to the available literature on small businesses, leadership, and information security, no previous research focuses on the possible relationship between leadership styles and information security problems. This study intended to fill this void. This study assessed the leadership styles of small business leaders and the influence leadership styles exerted upon information security experiences and problems. This research study offers three potential benefits: (a) an assessment of the prevalent small business leadership styles in the state of Hawaii; (b) a more precise identification of the specific leadership styles that best mitigate information security threats and problems; and (c) guidance for small business owners on the most effective leadership styles against information security threats.

Using the Multifactor Leadership Questionnaire (MLQ) survey from Bass and Avolio (2004) and the Small Business Security Survey (Ryan, 2000), this study examined the leadership styles within a sample of small businesses that belong to various chambers of commerce (CoCHawaii, 2007) or trade associations (SBH, 2007) within the state of Hawaii.

Statement of the Problem


The problem is small businesses often display a lack of concern towards information security problems (Gupta & Hammond, 2005). A lack of concern usually results in delayed or
incorrectly implemented security measures, which increases vulnerability to cybercrime (Andress, 2003; DeZulueta, 2004). In an empirical study of 1000 small businesses in the Lynchburg, Virginia area, Gupta and Hammond suggested that ineffective leadership styles might influence the lack of concern towards information security problems. The authors noted limited empirical evidence regarding the effect of leadership styles and the level of concern towards information security problems.

This quantitative, descriptive, correlational study examined the problem by determining whether and to what degree any relationship exists between leadership styles (independent variables) and the level of concern for information security problems (dependent variables). 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.

Dependent and Independent Variables

There are 14 dependent variables. As shown in Table 1, each represented a specific information security problem that a small business may face (Ryan, 2000). Using a Likert scale, the study examined the level of concern for each security problem.

Table 1

14 Dependent Variables

<table>
<thead>
<tr>
<th>Information security problem</th>
<th>Examples of problem in small businesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insider access abuse</td>
<td>Unauthorized login by employees</td>
</tr>
<tr>
<td>Viruses</td>
<td>Programs that enter through attachments in email</td>
</tr>
<tr>
<td>Power failure</td>
<td>Loss of data due to abrupt shutdown of computers</td>
</tr>
</tbody>
</table>
Information security problem  Examples of problem in small businesses

<table>
<thead>
<tr>
<th>Software problems</th>
<th>Vulnerable software due to absence of patches</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data integrity</td>
<td>Corruption of customer list or sales data</td>
</tr>
<tr>
<td>Transaction integrity</td>
<td>Corruption of financial transaction with bank</td>
</tr>
<tr>
<td>Outsider access abuse</td>
<td>Unauthorized entry by former employees</td>
</tr>
<tr>
<td>Data secrecy</td>
<td>Confidentiality of payroll information</td>
</tr>
<tr>
<td>Data availability</td>
<td>Availability of access to time sheet data</td>
</tr>
<tr>
<td>Data theft</td>
<td>Theft of confidential employee information</td>
</tr>
<tr>
<td>Data sabotage</td>
<td>Intentional destruction of financial data</td>
</tr>
<tr>
<td>User errors</td>
<td>Accidental erasure of data by untrained user</td>
</tr>
<tr>
<td>Natural Disaster</td>
<td>Damage to computer systems from floods</td>
</tr>
<tr>
<td>Fraud</td>
<td>Impersonation and deceit used to elicit information</td>
</tr>
</tbody>
</table>

The three independent variables, as shown in Table 2, were the transformational, transactional, and passive-avoidant leadership styles as defined by Bass and Avolio (2004). 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

<table>
<thead>
<tr>
<th>Leadership styles</th>
<th>Examples in small businesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transformational leadership</td>
<td>Visionary, dynamic owner</td>
</tr>
<tr>
<td>Transactional leadership</td>
<td>Leader focused on costs and benefits</td>
</tr>
<tr>
<td>Passive-avoidant leadership</td>
<td>Absentee, unavailable leader</td>
</tr>
</tbody>
</table>
Research 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 (SBA, 2007). This study utilized the Multifactor Leadership Questionnaire (MLQ) instrument (Bass & Avolio, 2004), to assess each company’s leadership style (independent variable) and the Small Business Security Survey instrument (Ryan, 2000) 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 and five businesses belonged to the Small Business Hawaii 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 (2007), 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 (Bass & Avolio, 2004; Ryan, 2000).

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 (Rubin & Babbie, 2005).

Results of Research Questions and Hypothesis

Research Question 1 and Hypothesis 1

R₁: What is the relationship between the transformational leadership style and the level of concern for information security problems within small businesses?

H₁₀: There is no relationship between the transformational leadership style score and the level of concern for information security problems within small businesses.

H₁ₐ: There is a relationship between the transformational leadership style score and the level of concern for information security problems within small businesses.
To answer Research Question 1 and test Hypothesis 1, Pearson’s product-moment correlation coefficients were generated to examine the possible relationship between transformational leadership style (independent variable) and information security concerns (dependent variables). The research study considered 14 separate information security concerns as dependent variables. The results, shown in Table 3, indicate a positive relationship ($p \leq 0.05$) between transformation leadership style and two (out of 14) information security concerns (Data Secrecy and Data Availability). The entire results of Pearson’s product-moment correlations are displayed in Appendix C.

Table 3

**Pearson's Correlations - Transformational Leadership Style**

<table>
<thead>
<tr>
<th></th>
<th>Transformational Leadership</th>
</tr>
</thead>
<tbody>
<tr>
<td>N=122</td>
<td></td>
</tr>
<tr>
<td>Data Secrecy</td>
<td>Pearson Correlation 0.18b ($r^2 = 0.03$)</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed) 0.05</td>
</tr>
<tr>
<td>Data Availability</td>
<td>Pearson Correlation 0.24a ($r^2 = 0.06$)</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed) 0.01</td>
</tr>
</tbody>
</table>

Note: aSignificant at the 0.01 level. bSignificant at the 0.05 level.

The results indicate that small businesses leaders who practice transformation leadership styles display high levels of concern for problems regarding data secrecy and data availability. The independent variable (transformational leadership style) explains less than 3% (coefficient of determination, $r^2 = 0.03$) of the variance for data secrecy and 6% ($r^2 = 0.06$) of the variance for data availability. More than 94% of the variance in data secrecy and data availability is unaccounted for and could be related to extraneous variables. Thus, although transformational leadership style has a statistically significant relationship with two information security concerns, this relationship is considered weak.

The independent variable Transformational Leadership Styles consists of five factors of leadership. To answer Research Question 1 in additional detail, Pearson’s product-moment
correlation coefficients were generated to examine the possible relationship between five transformational leadership factors (independent variables) and 14 information security concerns (dependent variables). The results, shown in Table 4, indicated a positive relationship \( (p < 0.05) \) between four factors of transformation leadership and six information security concerns. The entire results of Pearson’s product-moment correlations are displayed in Appendix C.

This indicates that small business leaders who practice specific factors of transformational leadership display high levels of concern regarding specific information security problems. For example, the Idealized Influence Attribute (IIA) had a statistically significant relationship \( (p < 0.05) \) with concern for the six security problems of insider access abuse, data integrity, data secrecy, data availability, data theft and data sabotage. Idealized attributes behavior (IIB) and inspirational motivation (IM) had a statistically significant relationship \( (p < 0.05) \) with the level of concern for the security problems of data availability and data secrecy respectively.

However, except in the case of IIA and Data Availability (where \( r^2 = 13\% \)) the independent variables (factors of transformational leadership) in Table 4 explain less than 5% of the variance for the specific information problem. More than 95% of the variance is unaccounted for and could be related to extraneous variables. In the case of IIA and Data Availability, the independent variable explains 13% of the variance in Data Availability problems. Thus, although four factors in transformational leadership (IIA, IIB, IM and IC) have a statistically significant relationship with the level of concern for six information security problems, this relationship is considered weak.
Table 4

*Pearson's Correlations - Transformational Leadership Factors*

<table>
<thead>
<tr>
<th></th>
<th>N=122</th>
<th>IIA</th>
<th>IIB</th>
<th>IM</th>
<th>IC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insider Access Abuse</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pearson Correlation</td>
<td>0.22a</td>
<td>0.02</td>
<td>0.00</td>
<td>-0.11</td>
<td></td>
</tr>
<tr>
<td>Sig. (2-tailed)</td>
<td>0.01</td>
<td>0.83</td>
<td>0.99</td>
<td>0.22</td>
<td></td>
</tr>
<tr>
<td>Data Integrity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pearson Correlation</td>
<td>0.22b</td>
<td>0.14</td>
<td>0.15</td>
<td>0.08</td>
<td></td>
</tr>
<tr>
<td>Sig. (2-tailed)</td>
<td>0.02</td>
<td>0.13</td>
<td>0.11</td>
<td>0.36</td>
<td></td>
</tr>
<tr>
<td>Data Secrecy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pearson Correlation</td>
<td>0.21b</td>
<td>0.11</td>
<td>0.18b</td>
<td>0.10</td>
<td></td>
</tr>
<tr>
<td>Sig. (2-tailed)</td>
<td>0.02</td>
<td>0.23</td>
<td>0.04</td>
<td>0.30</td>
<td></td>
</tr>
<tr>
<td>Data Availability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pearson Correlation</td>
<td>0.36a ($r^2 = 0.13$)</td>
<td>0.18b</td>
<td>0.13</td>
<td>0.21b</td>
<td></td>
</tr>
<tr>
<td>Sig. (2-tailed)</td>
<td>0.00</td>
<td>0.04</td>
<td>0.15</td>
<td>0.02</td>
<td></td>
</tr>
<tr>
<td>Data Theft</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pearson Correlation</td>
<td>0.19b</td>
<td>0.11</td>
<td>0.03</td>
<td>0.02</td>
<td></td>
</tr>
<tr>
<td>Sig. (2-tailed)</td>
<td>0.03</td>
<td>0.25</td>
<td>0.74</td>
<td>0.76</td>
<td></td>
</tr>
<tr>
<td>Data Sabotage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pearson Correlation</td>
<td>0.20b</td>
<td>0.13</td>
<td>0.03</td>
<td>-0.01</td>
<td></td>
</tr>
<tr>
<td>Sig. (2-tailed)</td>
<td>0.03</td>
<td>0.15</td>
<td>0.72</td>
<td>0.93</td>
<td></td>
</tr>
</tbody>
</table>

Note: *Significant at the 0.01 level. **Significant at the 0.05 level.

According to Abu-Bader (2006), while bivariate statistics examine the overall relationship between one dependent variable and one independent variable, multivariate statistics examine the relationships among multiple independent variables and one (or more) dependent variable. The Pearson’s product-moment correlation is an example of bivariate statistics, while multiple regression analysis is an example of multivariate analysis. As noted in Table 4, more than one leadership factor had a statistically significant relationship with the information security problems of data secrecy and data availability. Both IIA and IM leadership factors were statistically significantly related to data secrecy problems, while IIA, IIB, and IC factors were statistically significantly related to data availability problems.

Stepwise multiple regression analysis was conducted to predict the specific outcome or criterion (specific information security problem) based on multiple, significant leadership factors. Independent variables were entered into the regression model only if their correlation with the criterion (dependent variable) was statistically significant at alpha of 0.05 or less. Table
Table 5 displays the summary results with multiple correlation coefficient \((R)\), multiple \(R \) square, unstandardized coefficient \(B\), standard error of unstandardized coefficient, standardized regression coefficient \((\beta)\), \(t\) value and level of significance \((p)\) for each regression coefficient. The results display the one-way ANOVA \(F\) ratio and the overall level of significance for each regression model.

A stepwise multiple regression analysis was conducted to estimate a model that best predicts level of concerns for data secrecy. The results of the stepwise analysis, shown in Table 5, reveals one of the two leadership factors (IIA, but not IM) as a statistically significant predictor of concern for data secrecy \((F = 5.28, p < 0.05)\). With a beta of 0.21 \((p < 0.05)\), the transformational leadership factor of idealized influence attributes (IIA) emerged as the strongest predictor of the level of concern for data secrecy problems, accounting for 4\% of the variance in the level of concern.

Table 5

<table>
<thead>
<tr>
<th>Factor</th>
<th>(R)</th>
<th>(R^2)</th>
<th>Unstd. Coeff (B)</th>
<th>Std. Err.</th>
<th>Std. Coeff (\beta)</th>
<th>(t)</th>
<th>(p)</th>
<th>(F) ratio</th>
<th>Sig.</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Constant)</td>
<td></td>
<td></td>
<td>1.73</td>
<td>0.64</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.01</td>
</tr>
<tr>
<td>IIA</td>
<td>0.21(^a)</td>
<td>0.04</td>
<td>0.47</td>
<td>0.21(^b)</td>
<td>0.21(^b)</td>
<td>2.30</td>
<td>0.02</td>
<td>5.28(^b)</td>
<td>0.02(^a)</td>
</tr>
</tbody>
</table>

\(^a\)Predictors: (Constant), Idealized Influence Attributes (IIA). \(^b\)Criterion: Data Secrecy.

These results indicate that the higher the level of Idealized Influence attributes (IIA) within small business, the higher the level of concern for Data Secrecy issues and problems. Overall, the regression model explained only 4\% of the variance in the concern for data secrecy \((R = 0.21)\), indicating a weak relationship between Idealized Influence Attributes (IIA) and concerns for data secrecy. The unstandardized regression equation for data security concerns is as follows:
\[ Y = a + b_1X_1 + b_2X_2 \ldots + b_iX_i, \]
where \( Y \) is the score for the dependent variable, \( b \) is the unstandardized regression coefficient and \( X \) is the score for the independent variable. Based on the above formula and results, the regression equation is:

**Data Secrecy Raw Score = 1.73 + (0.47 x Idealized Influence Attribute Score)**

For example, if a small business scored a rating of 3 (Fairly Often) on Idealized Attributes, then we could predict the level of concern for data secrecy to be as follows:

**Data Secrecy Score = 1.73 + (0.47 x 3) = 3.14 or Moderate level of concern.**

A stepwise multiple regression analysis was conducted to estimate a model that best predicts level of concern for data availability among small businesses. The results of the stepwise analysis, shown below in Table 6, revealed that one of the three statistically significant leadership factors (IIA, but not IIB and IC) emerged as a statistically significant prediction of the level of concern for data availability problems \( (F = 17.67, p < 0.05) \).

**Table 6**

*Multiple Regression Analysis - Predictions of Data Availability*

<table>
<thead>
<tr>
<th>Factor</th>
<th>( R )</th>
<th>( R^2 )</th>
<th>Unstd. Coeff. B</th>
<th>Std. Err.</th>
<th>Std. Coeff. ( \beta )</th>
<th>( t )</th>
<th>( p )</th>
<th>ANOVA F ratio</th>
<th>Sig.</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Constant)</td>
<td>1.07</td>
<td>0.57</td>
<td>-</td>
<td>1.89</td>
<td>0.06</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IIA</td>
<td>0.36(^a)</td>
<td>0.13</td>
<td>0.77</td>
<td>0.18</td>
<td>0.36(^b)</td>
<td>4.20</td>
<td>0.00</td>
<td>17.67(^b)</td>
<td>0.00(^a)</td>
</tr>
</tbody>
</table>

*Note:* \(^a\)Predictors: (Constant), Idealized Influence Attributes (IIA). \(^b\)Criterion: Data Availability.

With a standardized beta \( \beta \) of 0.36 \( (p < 0.05) \), the transformational leadership factor of idealized influence attributes (IIA) emerged as the strongest predictor of the level of concern for data availability problems, accounting for 13% of the variance in the level of concern for data availability problems. These results indicate that the higher the level of Idealized Influence attributes (IIA) within small business, the higher the level of concern and preparation for data availability problems. Overall, the regression model explained 13% of the variance in the...
concern for data secrecy ($R = 0.36$), indicating a weak relationship between Idealized Influence Attributes (IIA) and concerns for data availability. The unstandardized regression equation for data security concerns is as follows:

$$\text{Data Availability Score} = 1.07 + (0.77 \times \text{Idealized Influence Attribute Score})$$

For example, if a small business scored a rating of 3 (Fairly Often) on Idealized Attributes, then we could predict the level of concern for data availability as follows:

$$\text{Data Availability Score} = 1.07 + (0.77 \times 3) = 3.38$$ or Moderate level of concern.

Because one factor of transformational leadership (IIA) was statistically significant in the multiple regression analysis ($p < 0.05$) in predicting the level of concern for two information security problems (data secrecy and data availability), the null hypothesis that no statistically significant relationship exists between the transformational leadership style and the level of concern for information security problems within small businesses is rejected.

**Research Question 2 and Hypothesis 2**

**R$_2$:** What is the relationship between the transactional leadership style and the level of concern for information security problems within small businesses?

**H$_{20}$:** There is no relationship between the transactional leadership style score and the level of concern for information security problems within small businesses.

**H$_{2a}$:** There is a relationship between the transactional leadership style score and the level of concern for information security problems within small businesses.

To answer Research Question 2 and test Hypothesis 2, Pearson’s product-moment correlation coefficients were generated to examine the possible relationship between transactional leadership style (independent variable) and information security concerns (dependent variables). The research study considered 14 separate information security concerns
as dependent variables. The results, shown in Table 7, indicated a positive relationship \((p < 0.05)\) between transactional leadership style and 11 (out of 14) information security concerns. The entire results of Pearson’s product-moment correlations are displayed in Appendix C.

This indicates that small business leaders who practice transactional leadership display higher levels of concern for problems regarding insider access abuse, viruses, data integrity, outsider access abuse, data secrecy, data availability, data theft, data sabotage, user errors, natural disasters, and fraud. The independent variable (transactional leadership style) explains less than 9\% (coefficient of determination, \(r^2 \leq 0.09\)) of the variance of the level of concern for 10 information security problems. These 10 problems include insider access abuse, viruses, data integrity, outsider access abuse, data secrecy, data availability, data theft, data sabotage, user errors, and fraud.

Transactional leadership style explains 11\% \((r^2 = 0.11)\) of the variance of the level of concern for natural disasters. More than 89\% of the variance for the level of concern for natural disasters is unaccounted for and could be related to extraneous variables. Although transformational leadership style has a statistically significant relationship with the level of concern for 11 information security problems \((p < 0.05)\), these relationships are considered weak.

Table 7

<table>
<thead>
<tr>
<th></th>
<th>Pearson Correlation</th>
<th>Pearson Correlation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>(r^2 = 0.06)</td>
</tr>
<tr>
<td>Insider Access Abuse</td>
<td>0.24^a</td>
<td></td>
</tr>
<tr>
<td>Sig. (2-tailed)</td>
<td>0.01</td>
<td></td>
</tr>
<tr>
<td>Viruses</td>
<td>0.26^a</td>
<td></td>
</tr>
<tr>
<td>Sig. (2-tailed)</td>
<td>0.00</td>
<td></td>
</tr>
<tr>
<td>Data Integrity</td>
<td>0.26^a</td>
<td></td>
</tr>
<tr>
<td>Sig. (2-tailed)</td>
<td>0.00</td>
<td></td>
</tr>
</tbody>
</table>
The independent variable transactional leadership style consists of two factors of leadership. To answer Research Question 2 in additional detail, Pearson’s product-moment correlation coefficients were generated to examine the possible relationship between two transactional leadership factors (independent variable) and the level of concern for 14 information security problems (dependent variables). The results, shown in Table 8, indicated a positive relationship ($p < 0.05$) between two factors of transactional leadership and the level of concern for 11 information security problems. The entire results of Pearson’s product-moment correlations are displayed in Appendix C.

This indicates that small business leaders who practice specific factors of transactional leadership display high levels of concern for specific information security problems. For

<table>
<thead>
<tr>
<th></th>
<th>Transactional Leadership</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Outsider Access Abuse</td>
<td>Pearson Correlation</td>
<td>0.23^a</td>
<td>$r^2 = 0.05$</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.01</td>
<td></td>
</tr>
<tr>
<td>Data Secrecy</td>
<td>Pearson Correlation</td>
<td>0.18^b</td>
<td>$r^2 = 0.05$</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.05</td>
<td></td>
</tr>
<tr>
<td>Data Availability</td>
<td>Pearson Correlation</td>
<td>0.3^a</td>
<td>$r^2 = 0.09$</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.00</td>
<td></td>
</tr>
<tr>
<td>Data Theft</td>
<td>Pearson Correlation</td>
<td>0.26^a</td>
<td>$r^2 = 0.07$</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.00</td>
<td></td>
</tr>
<tr>
<td>Data Sabotage</td>
<td>Pearson Correlation</td>
<td>0.28^a</td>
<td>$r^2 = 0.08$</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.00</td>
<td></td>
</tr>
<tr>
<td>User Errors</td>
<td>Pearson Correlation</td>
<td>0.29^a</td>
<td>$r^2 = 0.08$</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.00</td>
<td></td>
</tr>
<tr>
<td>Natural Disasters</td>
<td>Pearson Correlation</td>
<td>0.33^a</td>
<td>$r^2 = 0.11$</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.00</td>
<td></td>
</tr>
<tr>
<td>Fraud</td>
<td>Pearson Correlation</td>
<td>0.19^b</td>
<td>$r^2 = 0.04$</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.04</td>
<td></td>
</tr>
</tbody>
</table>

*Note: ^aSignificant at the 0.01 level. ^bSignificant at the 0.05 level.*
example, the Management by Exception Active (MBEA) had a statistically significant relationship ($p < 0.05$) with the level of concern for 10 security problems of insider access abuse, data integrity, outsider access abuse, data secrecy, data availability, data theft, data sabotage, user errors, natural disasters and fraud. Contingent Reward (CR) had a statistically significant relationship with the level of concern from viruses. The independent variables (factors of transactional leadership) explain less than 10% for the variance of the level of concern for the specific information problem listed in Table 8.

More than 90% of the variance is unaccounted for and could be related to extraneous variables. In the case of MBEA and data sabotage, the independent variable explains 10% of the variance in the level of concern from data sabotage. In the case of CR and viruses, the independent variable explains 5% of the variance in the level of concerns from viruses. Thus, although two factors in transactional leadership (CR and MBEA) have a statistically significant relationship with the level of concern for 11 information security problems ($p < 0.05$), this relationship is considered weak.

Table 8

*Pearson's Correlations - Transactional Leadership Factors*

<table>
<thead>
<tr>
<th></th>
<th>CR</th>
<th>MBEA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insider Access Abuse</td>
<td>Pearson Correlation 0.00</td>
<td>0.27$^a$ ($r^2 = 0.07$)</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed) 0.98</td>
<td>0.00</td>
</tr>
<tr>
<td>Viruses</td>
<td>Pearson Correlation 0.23$^a$ ($r^2 = 0.05$)</td>
<td>0.12</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed) 0.01</td>
<td>0.20</td>
</tr>
<tr>
<td>Power Failure</td>
<td>Pearson Correlation -0.05</td>
<td>0.23$^a$ ($r^2 = 0.05$)</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed) 0.59</td>
<td>0.01</td>
</tr>
<tr>
<td>Data Integrity</td>
<td>Pearson Correlation 0.15</td>
<td>0.22$^b$ ($r^2 = 0.05$)</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed) 0.10</td>
<td>0.02</td>
</tr>
</tbody>
</table>
N=122, except for CR N=121

<table>
<thead>
<tr>
<th>Outsider Access Abuse</th>
<th>Pearson Correlation</th>
<th>CR</th>
<th>MBEA</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.58</td>
<td>0.02</td>
</tr>
<tr>
<td>Data Availability</td>
<td>Pearson Correlation</td>
<td>0.14</td>
<td>0.24^a (r^2 = 0.06)</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.13</td>
<td>0.01</td>
</tr>
<tr>
<td>Data Theft</td>
<td>Pearson Correlation</td>
<td>-0.01</td>
<td>0.30^a (r^2 = 0.09)</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.94</td>
<td>0.00</td>
</tr>
<tr>
<td>Data Sabotage</td>
<td>Pearson Correlation</td>
<td>0.01</td>
<td>0.31^a (r^2 = 0.10)</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.93</td>
<td>0.00</td>
</tr>
<tr>
<td>User Errors</td>
<td>Pearson Correlation</td>
<td>0.03</td>
<td>0.30^a (r^2 = 0.09)</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.72</td>
<td>0.00</td>
</tr>
<tr>
<td>Natural Disasters</td>
<td>Pearson Correlation</td>
<td>0.11</td>
<td>0.29^a (r^2 = 0.08)</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.22</td>
<td>0.00</td>
</tr>
<tr>
<td>Fraud</td>
<td>Pearson Correlation</td>
<td>-0.06</td>
<td>0.25^a (r^2 = 0.06)</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.54</td>
<td>0.01</td>
</tr>
</tbody>
</table>

*Note: ^Significant at the 0.01 level. "Significant at the 0.05 level.*

Since no more than one leadership factor was significantly related to each of the 11 security concerns in Table 8, multiple regression analysis was not required. Because two factors of transactional leadership (CR and MBEA) were statistically significantly related (p < 0.05) to 11 information security concerns, the null hypothesis that no statistical significant relationship exists between the transactional leadership style and the level of concern for information security problems within small businesses is rejected.

**Research Question 3 and Hypothesis 3**

R3: What is the relationship between the passive-avoidant leadership style and the level of concern for information security problems within small businesses?

H3o: There is no relationship between the passive-avoidant leadership style score and the level of concern for information security problems within small businesses.
H3a: There is a relationship between the passive-avoidant leadership style score and the level of concern for information security problems within small businesses.

To answer Research Question 3 and test Hypothesis 3, Pearson’s product-moment correlation coefficients were generated to examine the possible relationship between passive-avoidance leadership style (independent variable) and information security concerns (dependent variables). The results, shown in Table 9 below, indicated a positive relationship (\( p < 0.05 \)) between passive-avoidance leadership style and one (out of 14) information security problems. The entire results of Pearson’s product-moment correlations are displayed in Appendix C.

This indicates that small business leaders who practice passive-avoidance behavior have high levels of concern about power failure. The independent variable (passive-avoidance leadership style) explains less than 4% (coefficient of determination, \( r^2 \leq 0.04 \)) of the variance for the level of concern about power failures. More than 96% of the variance is unaccounted for and could be related to extraneous variables. Thus, although passive-avoidance leadership style has a statistical significant relationship with the level of concern for one information security problem (\( p < 0.05 \)), this relationship is considered weak.

Table 9

<table>
<thead>
<tr>
<th>Passive-Avoidance Leadership</th>
<th>Pearson Correlation</th>
<th>Sig. (2-tailed)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Failure</td>
<td>0.19( ^\circ ) (( r^2 = 0.04 ))</td>
<td>0.03</td>
</tr>
</tbody>
</table>

Note: \(^\circ\)Significant at the 0.05 level.

The independent variable passive-avoidance leadership style consists of two factors of leadership. To answer Research Question 3 in additional detail, Pearson’s product-moment correlation coefficients were generated to examine the possible relationship between two
passive-avoidance leadership factors (independent variable) and the level of concern for 14 information security problems (dependent variables). The results, shown in Table 10, indicated a positive relationship ($p < 0.05$) between one factor of passive-avoidance leadership (MBEP) and the level of concern for one information security problem. The entire results of Pearson’s product-moment correlations are displayed in Appendix C.

This indicates that small business leaders who practice passive management by exception behavior (MBEP) have a high level of concern for power failure. For example, the Management by Exception Passive (MBEP) style had a statistical significant relationship ($p < 0.05$) with the level of concern for power failure. However, the independent variable (MBEP) explains less than 5% of the variance for the level of concern, as presented in Table 10. More than 95% of the variance is unaccounted for and could be related to extraneous variables. Thus, although one factor in transactional leadership (MBEP) has a statistically significant relationship with the level of concern for one information security problem ($p < 0.05$), this relationship is considered weak.

Table 10

$\textbf{Pearson's Correlations – Passive-Avoidance Leadership Factors}$

<table>
<thead>
<tr>
<th></th>
<th>MBEP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Failure</td>
<td>Pearson Correlation $0.23^a$ ($r^2 = 0.05$)</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
</tr>
</tbody>
</table>

$^a$Significant at the 0.01 level.

Since no more than one leadership factor was significantly related to the level of concern for one security problem in Table 10, multiple regression analysis was not required. Because one factor of passive-avoidance leadership (MBEP) was statistically significantly related ($p < 0.05$) to the level of concern for one information security problem, the null hypothesis that no
statistically significant relationship exists between the passive-avoidance leadership style and the level of concern for information security problems within small businesses is rejected.

Implications

The review of the literature indicated that the information systems of small businesses in the United States are vulnerable to cybercrime (Adamkiewicz, 2005; Baker & Wallace, 2007; Gupta & Hammond, 2005; O'Rourke, 2003). Computer security breaches disrupt businesses, causing annual revenue losses of over $200 million in the United States (Norah, 2004). Yet small businesses often display a lack of concern towards information security problems (Gupta & Hammond, 2005). The results of this study indicate that a combination of transformational and transactional leadership styles within small businesses correlates with the ability to mitigate information security problems. The results also emphasize that passive leadership styles provide few benefits to small businesses against the growing threats from cybercrime.

Implications for Global Leadership

Bass and Avolio (2004) defined transformational leadership as a “process of influence in which leaders change their associates’ awareness of what is important, and move them to see themselves and the opportunities and challenges in a new way” (p. 96). According to Bass and Avolio, transformational leadership strives to achieve the highest level of performance and job satisfaction from the followers. Bass (1990) noted that transactional leadership involves an exchange between the leader and followers in which the leader rewards or disciplines followers in exchange for their actions. Bass and Avolio (2004) described transactional leadership as “behaviors associated with constructive and corrective transactions” (p. 97). Transactional leaders define clear performance expectations from their followers and expect achievement of specific goals in exchange for rewards.
These study findings support the model (Bass, 1985) that transformational leadership augments transactional leadership in predicting effects on employees. Bass and Avolio (2004) supported the model with evidence and noted that transactional leadership provides a basis for effective leadership, but a “greater amount of Extra Effort, Effectiveness, and Satisfaction is possible from employees by augmenting transactional with transformational leadership” (p. 22). Figure 1 displays a graphical view of the leadership augmentation model to promote cybercrime vigilance within small businesses.

![Leadership Augmentation Model for Cybercrime](source)

Figure 1. Leadership Augmentation Model for Cybercrime

Source: Developed by researcher Debasis Bhattacharya, University of Phoenix

The results of the study support the model of augmenting transactional leadership styles with transformational leadership styles. While effective transactional leadership is the predominant leadership style for mitigating cybercrime, transformational leadership augments the benefits to small businesses. The results of the study highlight the need for both transformational and transactional leadership styles within small businesses to address information security problems.
Implications for Small Business Leaders

The study also 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 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. A combination of leadership, policy, and technologies provides a small business with an effective security framework to maintain vigilance against cybercrime (see Figure 2).

Figure 2. Cybercrime Leadership Framework Overview for Small Business
Source: Developed by researcher Debasis Bhattacharya, University of Phoenix

The second table in Appendix D identifies the combination of leadership, security policy, and security technology that best prepares a small business for a specific security problem. Figure 3 below provides details on the specific policies and procedures, technology, and leadership factors required by small businesses to mitigate information security problems. All policies and procedures, as well the technologies identified in Figure 3, need to be effectively deployed by the small business. The leadership styles include a combination of transactional and
transformational leadership. Transactional leadership factors of Contingent Reward and Active Management by Exception need to be augmented with transformational leadership factor of Idealized Influence Attributes.

Figure 3. Cybercrime Leadership Framework Details for Small Business

Source: Developed by researcher, Debasis Bhattacharya, University of Phoenix

Bass and Avolio (2004) cautioned against the limitations of transactional leadership. The authors noted that some leaders practice less than active management by exception, and turn to “contingent negative reinforcement to avoid transactional relationships” with employees (p. 23). There are occasions when transactional leaders fail to deliver the necessary rewards and consequently tarnish their reputations (Bass & Avolio). The implications of these risks for small business are significant as small business leaders cannot optimize their defenses against cybercrime and information security problems without transactional leadership styles that are credible and effective. Small business leaders also need to augment transactional leadership with genuine transformational leadership and effective deployment of policies and technology.
Recommendations

Three recommendations are proposed to address information security concerns within small businesses. The recommendations are based on the findings of the research study, implications, conclusions, and personal observations that align with the established theories of transformational leadership (Bass & Avolio, 2004) and information security (Ryan, 2000). The recommendations address the study problem that small businesses often display a lack of concern towards information security (Gupta & Hammond, 2005). A lack of concern usually results in delayed or incorrectly implemented security measures, which increases vulnerability to cybercrime (Andress, 2003; DeZulueta, 2004). These recommendations will enable small business owners and entrepreneurs to understand which combination of leadership styles, policies, and technologies best protects information security.

Recommendation 1: Leadership Styles Assessment

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. (2008), 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. Figure 4 provides a graphical display of the three leadership factors.
Figure 4. Assessment of Key Leadership Factors

The average score of the Contingent Reward (CR) and Management-by-Exception (MBEA) computes the aggregated transactional leadership scores for the small business. The score for the Idealized Influence Attributes (IIA) provides one dimension of transformational leadership. Other factors for transformational leadership include Idealized Influence Behavior (IIB), Inspirational Motivation (IM), Intellectual Stimulation (IS) and Individual Consideration (IC). The average of the scores for the five factors--IIA, IIB, IM, IS and IC--computes the aggregated transformational leadership score for the small business. Figure 5 displays the factors that compute the overall scores.
Figure 5. Computation of Leadership Style Scores

Recommendation 2: Information Security Assessment

The second recommendation is for small businesses to conduct an audit of their information security. A website (ReadyBusiness, 2008) and guide published by the US Department of Homeland Security (2004) provides a detailed checklist to conduct security assessments within small businesses. Another detailed guide from SANS (2003) provides a risk audit for very small businesses, with 10 or less employees, who were the primary respondents for this research study. Appendix E provides a detailed information security checklist for small business owners and leaders. Appendix F provides a detailed list of online and other resources available to businesses who are victims of cybercrime.

The US National Institute of Standards and Technology (NIST), in conjunction with the US Small Business Administration (SBA) and the US Federal Bureau of Investigation (FBI), 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 (NIST, 2008). Security technology and guidance for small businesses can be obtained from the websites of leading technology vendors such as Microsoft (2007), Symantec (2008), McAfee (2007), Cisco (2008), and ADT (2008).

Self-help books on computer security can provide small business leaders with a cost-effective but basic approach to assess the risks and vulnerabilities of the organization, and create a basic audit of information security needs (Day, 2003; Easttom, 2006). Based on the security checklist provided by Easttom, Figure 6 displays the various components of a basic information security assessment that small businesses can conduct on their own or with the assistance of an external security professional. Easttom provides guidance to small businesses to train internal or hire external professionals who can sustain an effective computer emergency response team.

![Figure 6. Basic Information Security Assessment (Easttom, 2006)](image)

**Recommendation 3: Application of Cybercrime Leadership**

The third recommendation is to use the feedback from the leadership assessment survey (MLQ) to compute the level of concern for an information security problem. This level of
concern identifies the importance that a small business needs to place on the specific information security problem. To compute the level of concern, as shown in Table 11, the leader needs to use the leadership score and the regression equation.

Table 11

*Cybercrime Leadership using Leadership Style Score*

<table>
<thead>
<tr>
<th>Security Problem</th>
<th>Compute Leadership Score from MLQ (Scale of 0-4)</th>
<th>Compute Level of Concern using Unstandardized Regression Equation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insider Access</td>
<td>Transactional Score</td>
<td>0.75 + (0.62 x Transactional Score)</td>
</tr>
<tr>
<td>Viruses</td>
<td>Transactional Score</td>
<td>2.26 + (0.58 x Transactional Score)</td>
</tr>
<tr>
<td>Data Integrity</td>
<td>Transactional Score</td>
<td>1.35 + (0.77 x Transactional Score)</td>
</tr>
<tr>
<td>Outsider Access</td>
<td>Transactional Score</td>
<td>1.44 + (0.62 x Transactional Score)</td>
</tr>
<tr>
<td>Data Secrecy</td>
<td>Transformational Score</td>
<td>1.77 + (0.47 x Transformational Score)</td>
</tr>
<tr>
<td>Data Availability</td>
<td>Transactional Score</td>
<td>1.34 + (0.85 x Transactional Score)</td>
</tr>
<tr>
<td>Data Theft</td>
<td>Transactional Score</td>
<td>1.18 + (0.75 x Transactional Score)</td>
</tr>
<tr>
<td>Data Sabotage</td>
<td>Transactional Score</td>
<td>0.84 + (0.80 x Transactional Score)</td>
</tr>
<tr>
<td>User Errors</td>
<td>Transactional Score</td>
<td>1.38 + (0.67 x Transactional Score)</td>
</tr>
<tr>
<td>Natural Disaster</td>
<td>Transactional Score</td>
<td>0.81 + (0.82 x Transactional Score)</td>
</tr>
<tr>
<td>Fraud</td>
<td>Transactional Score</td>
<td>1.49 + (0.53 x Transactional Score)</td>
</tr>
</tbody>
</table>

For example, assuming that the transformational score is 3.0 and the transactional score is 2.5; Figure 10 displays the desired level of concern necessary for an information security problem. The regression equation is based on study data from Appendix D. The results imply that small businesses should display moderate-to-high levels of concern for viruses, data
availability, and data integrity. Lower levels of concerns are appropriate for insider access abuse, fraud, data sabotage, and natural disasters.

Table 12

Example of Cybercrime Leadership

<table>
<thead>
<tr>
<th>Security Problem</th>
<th>Leadership Score from MLQ (Scale of 0-4)</th>
<th>Level of Concern using Unstandardized Regression Equation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insider Access Abuse</td>
<td>Transactional Score = 2.5</td>
<td>0.75 + (0.62 x 2.5) = 2.30 (low)</td>
</tr>
<tr>
<td>Viruses</td>
<td>Transactional Score = 2.5</td>
<td>2.26 + (0.58 x 2.5) = 3.71 (moderate)</td>
</tr>
<tr>
<td>Data Integrity</td>
<td>Transactional Score = 2.5</td>
<td>1.35 + (0.77 x 2.5) = 3.28</td>
</tr>
<tr>
<td>Outsider Access</td>
<td>Transactional Score = 2.5</td>
<td>1.44 + (0.62 x 2.5) = 2.99</td>
</tr>
<tr>
<td>Data Secrecy</td>
<td>Transformational Score = 3</td>
<td>1.77 + (0.47 x 3) = 3.18</td>
</tr>
<tr>
<td>Data Availability</td>
<td>Transactional Score = 2.5</td>
<td>1.34 + (0.85 x 2.5) = 3.47</td>
</tr>
<tr>
<td>Data Theft</td>
<td>Transactional Score = 2.5</td>
<td>1.18 + (0.75 x 2.5) = 3.06</td>
</tr>
<tr>
<td>Data Sabotage</td>
<td>Transactional Score = 2.5</td>
<td>0.84 + (0.80 x 2.5) = 2.84</td>
</tr>
<tr>
<td>User Errors</td>
<td>Transactional Score = 2.5</td>
<td>1.38 + (0.67 x 2.5) = 3.06</td>
</tr>
<tr>
<td>Natural Disaster</td>
<td>Transactional Score = 2.5</td>
<td>0.81 + (0.82 x 2.5) = 2.86</td>
</tr>
<tr>
<td>Fraud</td>
<td>Transactional Score = 2.5</td>
<td>1.49 + (0.53 x 2.5) = 2.82</td>
</tr>
</tbody>
</table>

The Cybercrime Leadership Framework provides small businesses with a quantifiable estimate of the level of concern needed to mitigate information security problems. Table 13 identifies technologies and policies based on results in Appendix D.
Table 13

*Cybercrime Leadership, Technology and Policy*

<table>
<thead>
<tr>
<th>Security Problem</th>
<th>Recommended Leadership Style</th>
<th>Recommended Technology and Policy to Augment Leadership Style</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insider Access Abuse</td>
<td>Transactional</td>
<td>Computer Emergency Response Team, Encryption Technology</td>
</tr>
<tr>
<td>Viruses</td>
<td>Transactional</td>
<td>Anti-virus software, Computer Emergency Response Plan</td>
</tr>
<tr>
<td>Data Integrity</td>
<td>Transactional</td>
<td>Intrusion Detection Systems, Computer Use and Misuse Policy</td>
</tr>
<tr>
<td>Outsider Access Abuse</td>
<td>Transactional</td>
<td>Intrusion Detection Systems</td>
</tr>
<tr>
<td>Data Secrecy</td>
<td>Transformational</td>
<td>Information Security Policy, System Activity Monitors, Anti-virus software</td>
</tr>
<tr>
<td>Data Availability</td>
<td>Transactional</td>
<td>Computer Use and Misuse Policy</td>
</tr>
<tr>
<td>Data Theft</td>
<td>Transactional</td>
<td>Computer Emergency Response Team, Anti-virus software, System Activity Monitors</td>
</tr>
<tr>
<td>Data Sabotage</td>
<td>Transactional</td>
<td>Computer Emergency Response Team, Intrusion Detection Systems</td>
</tr>
<tr>
<td>User Errors</td>
<td>Transactional</td>
<td>Computer Emergency Response Team, Anti-virus software</td>
</tr>
<tr>
<td>Natural Disaster</td>
<td>Transactional</td>
<td>Computer Emergency Response Plan</td>
</tr>
<tr>
<td>Fraud</td>
<td>Transactional</td>
<td>Computer Emergency Response Team</td>
</tr>
</tbody>
</table>
Recommendations for Future Research

The findings of this research study disclose a statistically significant relationship between transactional leadership style and several information security problems. Based on the findings, an adoption of the transactional leadership factor of Management by Exception Active (MBEA) can enable small businesses to better prepare against the majority (10 out of 14) of information security problems. As mentioned previously, these 10 problems are insider access abuse, data integrity, outsider access abuse, data secrecy, data availability, data theft, data sabotage, user errors, natural disasters, and fraud.

The study also 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 only on basic technologies such as anti-virus software, firewalls, and power surge protectors to protect against cybercrime. Likewise, small businesses cannot rely merely on basic policies and procedures for protection against cybercrime. A combination of leadership, policy, and technologies provides a small business with a vigilant and effective security framework.

Based on these findings, five suggestions are offered for further research. The first suggestion is to conduct additional studies in several small and large states in the United States, and broaden the sample population. This expansion may result in findings that are based on experiences of small business in various situations that are not relevant to the state of Hawaii. Additional research may be conducted in overseas countries that contain small businesses with profiles similar to those of small businesses in the United States. This global exposure will provide researchers with insight into global security problems and issues.
A second suggestion is to conduct a mixed-method quantitative-qualitative study designed to, in addition to giving survey statements, ask open ended questions about information security and concerns. Open-ended questions could elicit information regarding new and emerging security issues and feedback that are not covered by the questions in a survey instrument. Qualitative feedback could help facilitate specific action plans and strategies to mitigate new and emerging information security problems.

A third suggestion is to conduct similar studies on an ongoing basis for the next decade. Given the evolving nature of cybercrime and information security, the attitudes and exposures of small businesses vary over time. As such, regular studies conducted over a long period of time will provide researchers with details on trends and new issues. The results from these studies will provide researchers with a comprehensive evaluation of the growth and evolution of cybercrime and the abilities to combat it.

A fourth suggestion is to conduct a similar study in small, medium, and large organizations. This broadened study would provide researchers with information to compare and contrast security issues and concerns across an industry or region. The results of this study may allow organizations to adopt leadership styles, technologies and policies that are relevant to any organization, whatever its size.

A final suggestion is to update the list of independent and dependent variables to ensure that they cover the current leadership styles and information security concerns. As leadership styles evolve and the nature of cybercrime changes, the list of independent and dependent variables will need to be updated. The specific elements of leadership and security problems listed in the survey instruments for this study may become obsolete or irrelevant in a few years. As a result, the questionnaire needs to be updated.
Conclusions

The research 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 (Gupta & Hammond, 2005). A lack of concern usually results in delayed or incorrectly implemented security measures, which increases vulnerability to cybercrime (Andress, 2003; DeZulueta, 2004). 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 business leaders to mitigate information security problems without disrupting their core business functions.
REFERENCES


APPENDIX A: FREQUENCY TABLES
### Frequency Table of Intervening Variable: Business Area

<table>
<thead>
<tr>
<th>Business Area</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Professional, Scientific, and Technical Services</td>
<td>44</td>
<td>36.1</td>
</tr>
<tr>
<td>Other</td>
<td>16</td>
<td>13.1</td>
</tr>
<tr>
<td>Educational Services</td>
<td>9</td>
<td>7.4</td>
</tr>
<tr>
<td>Finance and Insurance</td>
<td>8</td>
<td>6.6</td>
</tr>
<tr>
<td>Retail Trade</td>
<td>7</td>
<td>5.7</td>
</tr>
<tr>
<td>Real Estate, Rental, and Leasing</td>
<td>6</td>
<td>4.9</td>
</tr>
<tr>
<td>Arts, Entertainment, and Recreation</td>
<td>5</td>
<td>4.1</td>
</tr>
<tr>
<td>Construction</td>
<td>5</td>
<td>4.1</td>
</tr>
<tr>
<td>Management of Companies and Enterprises</td>
<td>4</td>
<td>3.3</td>
</tr>
<tr>
<td>Agriculture</td>
<td>3</td>
<td>2.5</td>
</tr>
<tr>
<td>Information</td>
<td>3</td>
<td>2.5</td>
</tr>
<tr>
<td>Transportation and Warehousing</td>
<td>3</td>
<td>2.5</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>2</td>
<td>1.6</td>
</tr>
<tr>
<td>Publishing, Broadcasting, ISPs, Telcos and Recording</td>
<td>2</td>
<td>1.6</td>
</tr>
<tr>
<td>Wholesale Trade</td>
<td>2</td>
<td>1.6</td>
</tr>
<tr>
<td>Accommodation and Food Services</td>
<td>1</td>
<td>0.8</td>
</tr>
<tr>
<td>Utilities</td>
<td>1</td>
<td>0.8</td>
</tr>
<tr>
<td>Waste Management and Remediation Services</td>
<td>1</td>
<td>0.8</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>122</strong></td>
<td><strong>100.0</strong></td>
</tr>
</tbody>
</table>

### Frequency Table of Intervening Variable: Number of Employees

<table>
<thead>
<tr>
<th>Range</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 to 100</td>
<td>85</td>
<td>69.7</td>
</tr>
<tr>
<td>201 to 500</td>
<td>11</td>
<td>9.0</td>
</tr>
<tr>
<td>21 to 50</td>
<td>10</td>
<td>8.2</td>
</tr>
<tr>
<td>101 to 200</td>
<td>6</td>
<td>4.9</td>
</tr>
<tr>
<td>11 to 20</td>
<td>6</td>
<td>4.9</td>
</tr>
<tr>
<td>51 to 100</td>
<td>4</td>
<td>3.3</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>122</strong></td>
<td><strong>100.0</strong></td>
</tr>
</tbody>
</table>
### Frequency Table of Intervening Variable: Annual Revenues

<table>
<thead>
<tr>
<th>Range</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 to $500,000</td>
<td>70</td>
<td>57.4</td>
</tr>
<tr>
<td>More than $5 million</td>
<td>28</td>
<td>23.0</td>
</tr>
<tr>
<td>$500,001 to $1 million</td>
<td>13</td>
<td>10.7</td>
</tr>
<tr>
<td>$1 million to $5 million</td>
<td>11</td>
<td>9.0</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>122</strong></td>
<td><strong>100.0</strong></td>
</tr>
</tbody>
</table>

### Frequency Table of Intervening Variable: Number of Computers

<table>
<thead>
<tr>
<th>Range</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 to 5</td>
<td>67</td>
<td>54.9</td>
</tr>
<tr>
<td>11 to 20</td>
<td>14</td>
<td>11.5</td>
</tr>
<tr>
<td>More than 100</td>
<td>14</td>
<td>11.5</td>
</tr>
<tr>
<td>6 to 10</td>
<td>13</td>
<td>10.7</td>
</tr>
<tr>
<td>21 to 50</td>
<td>8</td>
<td>6.6</td>
</tr>
<tr>
<td>51 to 100</td>
<td>6</td>
<td>4.9</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>122</strong></td>
<td><strong>100.0</strong></td>
</tr>
</tbody>
</table>
APPENDIX B: CHI-SQUARE TESTS
Chi-Square Test of Leadership Styles by Business Area (Intervening Variable #1)

<table>
<thead>
<tr>
<th>Value</th>
<th>df</th>
<th>Asymp. Sig. (2-sided)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pearson Chi-Square</td>
<td>676.28</td>
<td>632</td>
</tr>
<tr>
<td>N of Valid Cases</td>
<td>122.00</td>
<td></td>
</tr>
</tbody>
</table>

Chi-Square Test of Leadership Styles by Number of Employees (Intervening Variable #2)

<table>
<thead>
<tr>
<th>Value</th>
<th>df</th>
<th>Asymp. Sig. (2-sided)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pearson Chi-Square</td>
<td>494.89</td>
<td>480</td>
</tr>
<tr>
<td>N of Valid Cases</td>
<td>122.00</td>
<td></td>
</tr>
</tbody>
</table>

Chi-Square Test of Leadership Styles by Annual Revenue (Intervening Variable #3)

<table>
<thead>
<tr>
<th>Value</th>
<th>df</th>
<th>Asymp. Sig. (2-sided)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pearson Chi-Square</td>
<td>298.27</td>
<td>288</td>
</tr>
<tr>
<td>N of Valid Cases</td>
<td>122.00</td>
<td></td>
</tr>
</tbody>
</table>

Chi-Square Test of Leadership Styles by Number of Computers (Intervening Variable #4)

<table>
<thead>
<tr>
<th>Value</th>
<th>df</th>
<th>Asymp. Sig. (2-sided)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pearson Chi-Square</td>
<td>478.06</td>
<td>480</td>
</tr>
<tr>
<td>N of Valid Cases</td>
<td>122.00</td>
<td></td>
</tr>
</tbody>
</table>

Note: The Chi-Square p values for all four intervening variable were greater than 0.05 \( (p > 0.5) \), and indicated no statistically significant relationship with leadership styles. As a result, there was no need to examine the strength of relationship through the Phi and Cramer’s V tests.
### Chi-Square Test of Leadership Styles by LAN Connectivity (Intervening Variable #5a)

<table>
<thead>
<tr>
<th>Value</th>
<th>df</th>
<th>Asymp. Sig. (2-sided)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pearson Chi-Square</td>
<td>100.66</td>
<td>96</td>
</tr>
<tr>
<td>N of Valid Cases</td>
<td>122.00</td>
<td></td>
</tr>
</tbody>
</table>

### Chi-Square Test of Leadership Styles by Internet Connectivity (Intervening Variable #5b)

<table>
<thead>
<tr>
<th>Value</th>
<th>df</th>
<th>Asymp. Sig. (2-sided)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pearson Chi-Square</td>
<td>69.61</td>
<td>96</td>
</tr>
<tr>
<td>N of Valid Cases</td>
<td>122.00</td>
<td></td>
</tr>
</tbody>
</table>

### Chi-Square Test of Leadership Styles by Intranet Connectivity (Intervening Variable #5c)

<table>
<thead>
<tr>
<th>Value</th>
<th>df</th>
<th>Asymp. Sig. (2-sided)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pearson Chi-Square</td>
<td>96.75</td>
<td>96</td>
</tr>
<tr>
<td>N of Valid Cases</td>
<td>122.00</td>
<td></td>
</tr>
</tbody>
</table>

### Chi-Square Test of Leadership Styles by Web Connectivity (Intervening Variable #5d)

<table>
<thead>
<tr>
<th>Value</th>
<th>df</th>
<th>Asymp. Sig. (2-sided)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pearson Chi-Square</td>
<td>98.00</td>
<td>96</td>
</tr>
<tr>
<td>N of Valid Cases</td>
<td>122.00</td>
<td></td>
</tr>
</tbody>
</table>

### Chi-Square Test of Leadership Styles by Extranet Connectivity (Intervening Variable #5e)

<table>
<thead>
<tr>
<th>Value</th>
<th>df</th>
<th>Asymp. Sig. (2-sided)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pearson Chi-Square</td>
<td>103.76</td>
<td>96</td>
</tr>
<tr>
<td>N of Valid Cases</td>
<td>122.00</td>
<td></td>
</tr>
</tbody>
</table>

### Chi-Square Test of Leadership Styles by E-Commerce Connectivity (Intervening Variable #5f)

<table>
<thead>
<tr>
<th>Value</th>
<th>df</th>
<th>Asymp. Sig. (2-sided)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pearson Chi-Square</td>
<td>107.34</td>
<td>96</td>
</tr>
<tr>
<td>N of Valid Cases</td>
<td>122.00</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** All Chi-Square p values ($p > 0.05$) indicated no statistically significant relationship between elements of connectivity and leadership styles. As a result, there was no need to examine the strength of relationship through the Phi and Cramer’s V tests.
APPENDIX C: PEARSON’S CORRELATIONS
### Pearson's Correlations - Transformational Leadership Style and Five Factors

<table>
<thead>
<tr>
<th>N=122</th>
<th>Transf</th>
<th>IIA</th>
<th>IIB</th>
<th>IM</th>
<th>IS</th>
<th>IC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insider Access Abuse</td>
<td>Correlation</td>
<td>0.02</td>
<td><strong>0.22</strong>&lt;sup&gt;a&lt;/sup&gt;</td>
<td>0.02</td>
<td>0.00</td>
<td>-0.04</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.81</td>
<td><strong>0.01</strong></td>
<td>0.83</td>
<td>0.99</td>
<td>0.69</td>
</tr>
<tr>
<td>Viruses</td>
<td>Correlation</td>
<td>0.13</td>
<td>0.15</td>
<td>0.07</td>
<td>0.16</td>
<td>0.12</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.15</td>
<td>0.10</td>
<td>0.44</td>
<td>0.09</td>
<td>0.20</td>
</tr>
<tr>
<td>Power Failure</td>
<td>Correlation</td>
<td>-0.10</td>
<td>-0.08</td>
<td>-0.08</td>
<td>-0.11</td>
<td>-0.11</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.28</td>
<td>0.38</td>
<td>0.37</td>
<td>0.23</td>
<td>0.24</td>
</tr>
<tr>
<td>Software Problems</td>
<td>Correlation</td>
<td>0.03</td>
<td>0.02</td>
<td>0.07</td>
<td>0.06</td>
<td>-0.03</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.74</td>
<td>0.79</td>
<td>0.46</td>
<td>0.55</td>
<td>0.79</td>
</tr>
<tr>
<td>Data Integrity</td>
<td>Correlation</td>
<td>0.16</td>
<td><strong>0.22</strong>&lt;sup&gt;b&lt;/sup&gt;</td>
<td>0.14</td>
<td>0.15</td>
<td>0.05</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.09</td>
<td><strong>0.02</strong></td>
<td>0.13</td>
<td>0.11</td>
<td>0.58</td>
</tr>
<tr>
<td>Transaction Integrity</td>
<td>Correlation</td>
<td>0.07</td>
<td>0.01</td>
<td>0.06</td>
<td>0.11</td>
<td>0.02</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.47</td>
<td>0.94</td>
<td>0.53</td>
<td>0.22</td>
<td>0.82</td>
</tr>
<tr>
<td>Outsider Access Abuse</td>
<td>Correlation</td>
<td>0.06</td>
<td>0.12</td>
<td>0.07</td>
<td>0.05</td>
<td>0.01</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.52</td>
<td>0.19</td>
<td>0.44</td>
<td>0.60</td>
<td>0.94</td>
</tr>
<tr>
<td>Data Secrecy</td>
<td>Correlation</td>
<td><strong>0.18</strong>&lt;sup&gt;b&lt;/sup&gt;</td>
<td><strong>0.21</strong>&lt;sup&gt;b&lt;/sup&gt;</td>
<td>0.11</td>
<td><strong>0.18</strong>&lt;sup&gt;b&lt;/sup&gt;</td>
<td>0.13</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td><strong>0.05</strong></td>
<td><strong>0.02</strong></td>
<td>0.23</td>
<td><strong>0.04</strong></td>
<td>0.15</td>
</tr>
<tr>
<td>Data Availability</td>
<td>Correlation</td>
<td><strong>0.24</strong>&lt;sup&gt;a&lt;/sup&gt;</td>
<td><strong>0.36</strong>&lt;sup&gt;a&lt;/sup&gt;</td>
<td><strong>0.18</strong>&lt;sup&gt;b&lt;/sup&gt;</td>
<td>0.13</td>
<td>0.12</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td><strong>0.01</strong></td>
<td><strong>0.00</strong></td>
<td><strong>0.04</strong></td>
<td>0.15</td>
<td>0.20</td>
</tr>
<tr>
<td>Data Theft</td>
<td>Correlation</td>
<td>0.09</td>
<td><strong>0.19</strong>&lt;sup&gt;b&lt;/sup&gt;</td>
<td>0.11</td>
<td>0.03</td>
<td>0.02</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.32</td>
<td><strong>0.03</strong></td>
<td>0.25</td>
<td>0.74</td>
<td>0.80</td>
</tr>
<tr>
<td>Data Sabotage</td>
<td>Correlation</td>
<td>0.10</td>
<td><strong>0.20</strong>&lt;sup&gt;b&lt;/sup&gt;</td>
<td>0.13</td>
<td>0.03</td>
<td>0.06</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.26</td>
<td><strong>0.03</strong></td>
<td>0.15</td>
<td>0.72</td>
<td>0.50</td>
</tr>
<tr>
<td>User Errors</td>
<td>Correlation</td>
<td>-0.01</td>
<td>0.12</td>
<td>-0.01</td>
<td>-0.05</td>
<td>-0.01</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.91</td>
<td>0.19</td>
<td>0.88</td>
<td>0.56</td>
<td>0.88</td>
</tr>
<tr>
<td>Natural Disasters</td>
<td>Correlation</td>
<td>0.10</td>
<td>0.14</td>
<td>0.10</td>
<td>0.09</td>
<td>0.05</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.28</td>
<td>0.13</td>
<td>0.29</td>
<td>0.31</td>
<td>0.61</td>
</tr>
<tr>
<td>Fraud</td>
<td>Correlation</td>
<td>0.01</td>
<td>0.03</td>
<td>0.00</td>
<td>0.00</td>
<td>-0.03</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.88</td>
<td>0.71</td>
<td>0.97</td>
<td>0.98</td>
<td>0.74</td>
</tr>
</tbody>
</table>

**Note:**<sup>a</sup>Significant at the 0.01 level. <sup>b</sup>Significant at the 0.05 level. IIA & B - Idealized Influence Attributes and Behavior, IM – Inspirational Motivation, IS – Intellectual Stimulation, IC – Individual Consideration
<table>
<thead>
<tr>
<th></th>
<th>Correlation</th>
<th>CR</th>
<th>MBEA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Insider Access Abuse</strong></td>
<td>Pearson Correlation</td>
<td>0.24</td>
<td>0.27</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.01</td>
<td>0.98</td>
</tr>
<tr>
<td><strong>Viruses</strong></td>
<td>Pearson Correlation</td>
<td>0.26</td>
<td>0.23</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.00</td>
<td>0.01</td>
</tr>
<tr>
<td><strong>Power Failure</strong></td>
<td>Pearson Correlation</td>
<td>0.17</td>
<td>0.23</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.07</td>
<td>0.59</td>
</tr>
<tr>
<td><strong>Software Problems</strong></td>
<td>Pearson Correlation</td>
<td>0.10</td>
<td>0.08</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.29</td>
<td>0.39</td>
</tr>
<tr>
<td><strong>Data Integrity</strong></td>
<td>Pearson Correlation</td>
<td>0.26</td>
<td>0.15</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.00</td>
<td>0.02</td>
</tr>
<tr>
<td><strong>Transaction Integrity</strong></td>
<td>Pearson Correlation</td>
<td>0.10</td>
<td>0.10</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.26</td>
<td>0.69</td>
</tr>
<tr>
<td><strong>Outsider Access Abuse</strong></td>
<td>Pearson Correlation</td>
<td>0.23</td>
<td>0.22</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.01</td>
<td>0.02</td>
</tr>
<tr>
<td><strong>Data Secrecy</strong></td>
<td>Pearson Correlation</td>
<td>0.18</td>
<td>0.11</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.05</td>
<td>0.22</td>
</tr>
<tr>
<td><strong>Data Availability</strong></td>
<td>Pearson Correlation</td>
<td>0.3</td>
<td>0.24</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.00</td>
<td>0.01</td>
</tr>
<tr>
<td><strong>Data Theft</strong></td>
<td>Pearson Correlation</td>
<td>0.26</td>
<td>0.30</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td><strong>Data Sabotage</strong></td>
<td>Pearson Correlation</td>
<td>0.28</td>
<td>0.31</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td><strong>User Errors</strong></td>
<td>Pearson Correlation</td>
<td>0.29</td>
<td>0.30</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td><strong>Natural Disasters</strong></td>
<td>Pearson Correlation</td>
<td>0.33</td>
<td>0.29</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td><strong>Fraud</strong></td>
<td>Pearson Correlation</td>
<td>0.19</td>
<td>0.25</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.04</td>
<td>0.01</td>
</tr>
</tbody>
</table>

*Note: *Significant at the 0.01 level. *bSignificant at the 0.05 level.*
### Pearson’s Correlations of Passive-Avoidance Leadership and Two Factors

<table>
<thead>
<tr>
<th></th>
<th>Passive-Avoidance Leadership</th>
<th>MBEP</th>
<th>LF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insider Access Abuse</td>
<td>Pearson Correlation</td>
<td>0.12</td>
<td>0.11</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.20</td>
<td>0.23</td>
</tr>
<tr>
<td>Viruses</td>
<td>Pearson Correlation</td>
<td>0.01</td>
<td>0.05</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.96</td>
<td>0.60</td>
</tr>
<tr>
<td>Power Failure</td>
<td>Pearson Correlation</td>
<td>0.19b</td>
<td>0.23a</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.03</td>
<td>0.01</td>
</tr>
<tr>
<td>Software Problems</td>
<td>Pearson Correlation</td>
<td>0.03</td>
<td>0.09</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.73</td>
<td>0.34</td>
</tr>
<tr>
<td>Data Integrity</td>
<td>Pearson Correlation</td>
<td>0.09</td>
<td>0.12</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.35</td>
<td>0.20</td>
</tr>
<tr>
<td>Transaction Integrity</td>
<td>Pearson Correlation</td>
<td>0.03</td>
<td>0.08</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.74</td>
<td>0.42</td>
</tr>
<tr>
<td>Outsider Access Abuse</td>
<td>Pearson Correlation</td>
<td>0.13</td>
<td>0.11</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.14</td>
<td>0.24</td>
</tr>
<tr>
<td>Data Secrecy</td>
<td>Pearson Correlation</td>
<td>0.05</td>
<td>0.03</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.57</td>
<td>0.71</td>
</tr>
<tr>
<td>Data Availability</td>
<td>Pearson Correlation</td>
<td>0.15</td>
<td>0.12</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.11</td>
<td>0.17</td>
</tr>
<tr>
<td>Data Theft</td>
<td>Pearson Correlation</td>
<td>0.16</td>
<td>0.16</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.09</td>
<td>0.08</td>
</tr>
<tr>
<td>Data Sabotage</td>
<td>Pearson Correlation</td>
<td>0.13</td>
<td>0.13</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.15</td>
<td>0.17</td>
</tr>
<tr>
<td>User Errors</td>
<td>Pearson Correlation</td>
<td>0.14</td>
<td>0.15</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.11</td>
<td>0.09</td>
</tr>
<tr>
<td>Natural Disasters</td>
<td>Pearson Correlation</td>
<td>0.09</td>
<td>0.11</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.34</td>
<td>0.23</td>
</tr>
<tr>
<td>Fraud</td>
<td>Pearson Correlation</td>
<td>0.13</td>
<td>0.14</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.16</td>
<td>0.11</td>
</tr>
</tbody>
</table>

*Note: *Significant at the 0.01 level. "Significant at the 0.05 level."
APPENDIX D: MULTIPLE REGRESSION ANALYSIS
Multiple Regression Analysis – Leadership Styles

<table>
<thead>
<tr>
<th>Criterion (Security Concern)</th>
<th>Factors (Three Leadership Styles)</th>
<th>$R$</th>
<th>$R^2$</th>
<th>Unstd $B$</th>
<th>Std $\beta$</th>
<th>$t$</th>
<th>$p$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insider Access Abuse</td>
<td>(Constant)</td>
<td>0.75</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Viruses</td>
<td>(Constant)</td>
<td>2.26</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Power Failure</td>
<td>(Constant)</td>
<td>2.82</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Integrity</td>
<td>(Constant)</td>
<td>1.35</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Outsider Access Abuse</td>
<td>(Constant)</td>
<td>1.44</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Secrecy</td>
<td>(Constant)</td>
<td>1.77</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Availability</td>
<td>(Constant)</td>
<td>1.34</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Theft</td>
<td>(Constant)</td>
<td>1.18</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Sabotage</td>
<td>(Constant)</td>
<td>0.84</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Errors</td>
<td>(Constant)</td>
<td>1.38</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Natural Disaster</td>
<td>(Constant)</td>
<td>0.81</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fraud</td>
<td>(Constant)</td>
<td>1.49</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: Software problems and transaction integrity had no significant relationship with leadership.
<table>
<thead>
<tr>
<th>Criterion (Security Concern)</th>
<th>Factor (Nine Leadership Factors, Policies or Technologies)</th>
<th>R</th>
<th>R^2</th>
<th>Unstd B</th>
<th>Std β</th>
<th>t</th>
<th>p</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insider (Constant)</td>
<td></td>
<td>1.23</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Abuse</td>
<td>Computer Emergency Response Team</td>
<td>0.36</td>
<td>0.13</td>
<td>1.02</td>
<td>0.30</td>
<td>3.62</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>MBEA</td>
<td>0.43</td>
<td>0.19</td>
<td>0.33</td>
<td>0.22</td>
<td>2.64</td>
<td>0.01</td>
</tr>
<tr>
<td></td>
<td>Encryption</td>
<td>0.47</td>
<td>0.23</td>
<td>0.53</td>
<td>0.20</td>
<td>2.41</td>
<td>0.02</td>
</tr>
<tr>
<td>Viruses (Constant)</td>
<td></td>
<td>0.71</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Anti-virus software</td>
<td>0.41</td>
<td>0.17</td>
<td>2.11</td>
<td>0.39</td>
<td>4.83</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Computer Emergency Response Plan</td>
<td>0.48</td>
<td>0.23</td>
<td>0.49</td>
<td>0.20</td>
<td>2.37</td>
<td>0.02</td>
</tr>
<tr>
<td></td>
<td>CR</td>
<td>0.51</td>
<td>0.26</td>
<td>0.29</td>
<td>0.18</td>
<td>2.10</td>
<td>0.04</td>
</tr>
<tr>
<td>Power Failure (Constant)</td>
<td></td>
<td>2.44</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Computer Emergency Response Plan</td>
<td>0.26</td>
<td>0.07</td>
<td>0.98</td>
<td>0.36</td>
<td>4.10</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>MBEP</td>
<td>0.38</td>
<td>0.14</td>
<td>0.42</td>
<td>0.26</td>
<td>3.03</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Security Evaluation Systems</td>
<td>0.42</td>
<td>0.18</td>
<td>-0.67</td>
<td>-0.20</td>
<td>-2.23</td>
<td>0.03</td>
</tr>
<tr>
<td>Data Integrity (Constant)</td>
<td></td>
<td>2.27</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Intrusion Detection</td>
<td>0.30</td>
<td>0.09</td>
<td>0.54</td>
<td>0.20</td>
<td>2.19</td>
<td>0.03</td>
</tr>
<tr>
<td></td>
<td>Computer Use and Misuse Policy</td>
<td>0.35</td>
<td>0.12</td>
<td>0.51</td>
<td>0.20</td>
<td>2.17</td>
<td>0.03</td>
</tr>
<tr>
<td></td>
<td>MBEA</td>
<td>0.39</td>
<td>0.15</td>
<td>0.28</td>
<td>0.18</td>
<td>2.13</td>
<td>0.04</td>
</tr>
<tr>
<td>Transaction Integrity (Con</td>
<td></td>
<td>1.6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Anti-virus software</td>
<td>0.22</td>
<td>0.05</td>
<td>1.56</td>
<td>0.22</td>
<td>2.51</td>
<td>0.01</td>
</tr>
<tr>
<td>Outside Access (Constant)</td>
<td></td>
<td>2.07</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Intrusion Detection</td>
<td>0.38</td>
<td>0.14</td>
<td>0.99</td>
<td>0.36</td>
<td>4.23</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>MBEA</td>
<td>0.41</td>
<td>0.17</td>
<td>0.27</td>
<td>0.17</td>
<td>2.03</td>
<td>0.04</td>
</tr>
<tr>
<td>Data Secrecy (Constant)</td>
<td></td>
<td>1.40</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Information Security Policy</td>
<td>0.34</td>
<td>0.11</td>
<td>0.62</td>
<td>0.21</td>
<td>2.30</td>
<td>0.02</td>
</tr>
<tr>
<td></td>
<td>System Activity Monitors</td>
<td>0.40</td>
<td>0.16</td>
<td>0.83</td>
<td>0.23</td>
<td>2.55</td>
<td>0.01</td>
</tr>
<tr>
<td></td>
<td>Anti-virus Software</td>
<td>0.44</td>
<td>0.19</td>
<td>1.35</td>
<td>0.18</td>
<td>2.16</td>
<td>0.03</td>
</tr>
<tr>
<td>Data (Constant)</td>
<td></td>
<td>0.71</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Criterion (Security Concern)</td>
<td>Factor (Nine Leadership Factors, Policies or Technologies)</td>
<td>R</td>
<td>R²</td>
<td>B</td>
<td>β</td>
<td>t</td>
<td>p</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------------------</td>
<td>----</td>
<td>-----</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
</tr>
<tr>
<td>Availability</td>
<td>IIA</td>
<td>0.36</td>
<td>0.13</td>
<td>0.60</td>
<td>0.28</td>
<td>3.37</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Computer Use and Misuse Policy</td>
<td>0.45</td>
<td>0.21</td>
<td>0.78</td>
<td>0.28</td>
<td>3.46</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>MBEA</td>
<td>0.48</td>
<td>0.23</td>
<td>0.27</td>
<td>0.17</td>
<td>2.05</td>
<td>0.00</td>
</tr>
<tr>
<td>Data Theft (Constant)</td>
<td>MBEA</td>
<td>0.30</td>
<td>0.09</td>
<td>0.47</td>
<td>0.28</td>
<td>3.44</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Computer Emergency Response Team</td>
<td>0.41</td>
<td>0.16</td>
<td>0.76</td>
<td>0.21</td>
<td>2.40</td>
<td>0.02</td>
</tr>
<tr>
<td></td>
<td>Anti-virus software</td>
<td>0.45</td>
<td>0.20</td>
<td>1.22</td>
<td>0.17</td>
<td>2.07</td>
<td>0.04</td>
</tr>
<tr>
<td></td>
<td>System Activity Monitors</td>
<td>0.47</td>
<td>0.23</td>
<td>0.61</td>
<td>0.17</td>
<td>2.03</td>
<td>0.04</td>
</tr>
<tr>
<td>Data Sabotage (Constant)</td>
<td>MBEA</td>
<td>0.31</td>
<td>0.10</td>
<td>0.45</td>
<td>0.27</td>
<td>3.23</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Computer Emergency Response Team</td>
<td>0.41</td>
<td>0.17</td>
<td>0.81</td>
<td>0.22</td>
<td>2.56</td>
<td>0.01</td>
</tr>
<tr>
<td></td>
<td>Intrusion Detection</td>
<td>0.45</td>
<td>0.20</td>
<td>0.58</td>
<td>0.20</td>
<td>2.31</td>
<td>0.02</td>
</tr>
<tr>
<td>User Errors (Constant)</td>
<td>MBEA</td>
<td>0.30</td>
<td>0.09</td>
<td>0.36</td>
<td>0.27</td>
<td>3.22</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Computer Emergency Response Team</td>
<td>0.40</td>
<td>0.16</td>
<td>0.74</td>
<td>0.25</td>
<td>2.96</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Anti-virus software</td>
<td>0.43</td>
<td>0.19</td>
<td>1.00</td>
<td>0.17</td>
<td>2.05</td>
<td>0.04</td>
</tr>
<tr>
<td>Natural Disaster (Constant)</td>
<td>MBEA</td>
<td>0.34</td>
<td>0.12</td>
<td>0.88</td>
<td>0.32</td>
<td>3.87</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Computer Emergency Response Plan</td>
<td>0.43</td>
<td>0.19</td>
<td>0.38</td>
<td>0.27</td>
<td>3.22</td>
<td>0.00</td>
</tr>
<tr>
<td>Fraud (Constant)</td>
<td>MBEA</td>
<td>0.25</td>
<td>0.06</td>
<td>0.40</td>
<td>0.24</td>
<td>2.79</td>
<td>0.01</td>
</tr>
<tr>
<td></td>
<td>Computer Emergency Response Team</td>
<td>0.32</td>
<td>0.10</td>
<td>0.70</td>
<td>0.19</td>
<td>2.20</td>
<td>0.03</td>
</tr>
</tbody>
</table>

*Note: One security problem, software problems, had no significant relationship with any leadership style, policy or technology.*
APPENDIX E: SMALL BUSINESS SECURITY CHECKLIST
### Microsoft Windows PC Security Checklist

<table>
<thead>
<tr>
<th>Priority</th>
<th>Task</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Perform full virus scans on a regular schedule</td>
<td>Anti-virus software is available from several software vendors such as McAfee, Symantec, F-Secure, CA, and Microsoft.</td>
</tr>
<tr>
<td>High</td>
<td>Turn on anti-spyware software</td>
<td>Anti-spyware is available from Microsoft Windows Defender or vendors like McAfee.</td>
</tr>
<tr>
<td>High</td>
<td>Install latest patches and software updates</td>
<td>Microsoft’s Windows Update site, which can be invoked by an icon in the Control Panel, provides patches and updates for download.</td>
</tr>
<tr>
<td>High</td>
<td>Configure Browser to default (Medium-High)</td>
<td>Internet Explorer allows the user to set security levels. Keep browser to default security, unless custom settings are needed.</td>
</tr>
<tr>
<td>High</td>
<td>Turn on PC firewall</td>
<td>A Personal Firewall is provided by Microsoft Windows as well as vendors like McAfee.</td>
</tr>
<tr>
<td>High</td>
<td>Change strong passwords regularly</td>
<td>Passwords of at least eight characters, with numbers and upper case letters, should be changed every 90 days.</td>
</tr>
<tr>
<td>High</td>
<td>Only administrator has full rights</td>
<td>Create user accounts that have lesser privileges than the administrator.</td>
</tr>
<tr>
<td>High</td>
<td>Backup hard disk</td>
<td>Backup to external hard disk weekly.</td>
</tr>
<tr>
<td>Recommended</td>
<td>Turn on pop-up blocker</td>
<td>Pop-up blockers available via toolbars from Google as well as browsers such as IE.</td>
</tr>
<tr>
<td>Recommended</td>
<td>Turn on Phishing filter</td>
<td>Phishing filter available from IE7 browser and other software such as Google Desktop.</td>
</tr>
</tbody>
</table>
### Network Security Checklist

<table>
<thead>
<tr>
<th>Priority</th>
<th>Task</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Install packet-filtering, SPI firewall and proxy server</td>
<td>Many routers from vendors like Linksys provide packet-filtering, stateful packet inspection (SPI) firewall and a proxy server.</td>
</tr>
<tr>
<td>High</td>
<td>Ensure secure wireless network</td>
<td>WEP or WPA security keys recorded in the router allow secure wireless communication.</td>
</tr>
<tr>
<td>High</td>
<td>Prevent Broadcast or Multicast storms</td>
<td>Configure all routers to not repeat broadcast packets.</td>
</tr>
<tr>
<td>High</td>
<td>Ensure strong passwords in all computers</td>
<td>Ensure passwords are at least eight characters with a mixture of numbers and upper case letters. Force password changes every 6 months.</td>
</tr>
<tr>
<td>High</td>
<td>Ensure all servers are physically secure</td>
<td>Security involves access privileges by administrators, physical security from fire, natural disasters, and sabotage.</td>
</tr>
<tr>
<td>High</td>
<td>Backup server data</td>
<td>Daily backups of server data, and weekly transition of data to a remote storage location.</td>
</tr>
<tr>
<td>High</td>
<td>Server and client Patches and Updates</td>
<td>Install latest patches and updates regularly from Microsoft and other software vendors.</td>
</tr>
<tr>
<td>Recommended</td>
<td>Install and run security software from Microsoft</td>
<td>Download, install and run the Microsoft Baseline Software Analyzer (MSBA) and the 2007 Microsoft Office Security Guide.</td>
</tr>
<tr>
<td>Recommended</td>
<td>Intrusion detection (IDS) software</td>
<td>Several vendors provide IDS, including the open source Snort for Linux and Windows.</td>
</tr>
</tbody>
</table>

### Basic Online Fraud Policy Checklist

<table>
<thead>
<tr>
<th>Policy</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reputable vendors</td>
<td>Reputable banks, online merchants and smaller vendors can be identified by secure logos such a BBB Online.</td>
</tr>
<tr>
<td>Phishing scams</td>
<td>No online vendor asks for social security numbers and other identifying information over the phone, pop-up windows and other solicitation.</td>
</tr>
<tr>
<td>Pharming</td>
<td>Ensure that the website is the legitimate web site, has the padlock image, and identified by SSL technology using https://</td>
</tr>
<tr>
<td>Public computers</td>
<td>Public computers in libraries, internet cafes, airports, schools and other venues may be insecure and contain stealth key logger software.</td>
</tr>
<tr>
<td>Review Credit Report</td>
<td>Review credit report every six months from Equifax, Experian or TransUnion.</td>
</tr>
<tr>
<td>Security questions</td>
<td>Choose your security questions and answers carefully as the answer to some questions may be readily available to cyber and identity thieves.</td>
</tr>
<tr>
<td>Passwords</td>
<td>Change passwords to banks and financial institutions every 6 months.</td>
</tr>
</tbody>
</table>
### Basic Information Security Policies

<table>
<thead>
<tr>
<th>Policy</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Downloading Software</td>
<td>Written policies to prohibit downloading of software by users. Only IT administrators with privileges can download software from the internet.</td>
</tr>
<tr>
<td>Email Attachments</td>
<td>Policies prevent email attachments over 12MB in size from reaching users, and block or quarantine high-risk file types in email attachments.</td>
</tr>
<tr>
<td>Terminated Employees</td>
<td>Policies to ensure that terminated employees are relieved of access to computers and physical facilities. Transfer of hardware such as laptops, peripherals and devices such as memory cards, PDAs, and cell phones.</td>
</tr>
<tr>
<td>Security Training</td>
<td>All employees are made aware of organizational and information security policies. All employees affirmatively agree to follow policies.</td>
</tr>
<tr>
<td>Disaster Recovery</td>
<td>Documented disaster recovery plan is understood by IT staff and owners. Security drills to prepare for disasters conducted every year.</td>
</tr>
<tr>
<td>Background Checks</td>
<td>All administrators of computers and networks require extensive background checks for criminal activities, credit and references.</td>
</tr>
<tr>
<td>Encryption</td>
<td>All sensitive communications with external vendors must follow encryption policies. All laptops must have encrypted hard disks.</td>
</tr>
<tr>
<td>Audits</td>
<td>Basic security audits of computers and servers performed every six months. A full security audit of entire facility conducted every year.</td>
</tr>
<tr>
<td>Security Audits</td>
<td>Users are provided security bulletins and warnings of current scams, viruses, malware and other attacks.</td>
</tr>
<tr>
<td>Media Destruction</td>
<td>Old or obsolete media and computers are first cleaned of data. Peripherals and old computers can be recycled or donated to charities.</td>
</tr>
<tr>
<td>Security Bulletins</td>
<td>Users are provided security bulletins and warnings of current scams, viruses, malware and other attacks.</td>
</tr>
</tbody>
</table>

### Basic Computer Use and Misuse Policies

<table>
<thead>
<tr>
<th>Policy</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passwords</td>
<td>Employees agree to not share passwords and account information with other employees. Passwords should be changed every six months.</td>
</tr>
<tr>
<td>Disclaimers</td>
<td>All emails and written online communication from employees contain a legal disclaimer that protects company from legal liability.</td>
</tr>
<tr>
<td>Posting to Newsgroups</td>
<td>Employees must follow clear documented rules when posting messages to public newsgroups and blogs.</td>
</tr>
<tr>
<td>Privacy</td>
<td>Employees must adhere to the documented privacy policy of the business, as well as privacy policies of partners and other vendors.</td>
</tr>
<tr>
<td>Intellectual Property</td>
<td>Employees are prohibited from copying or downloading copyrighted material in violation of copyright laws, or without an active license.</td>
</tr>
<tr>
<td>Harassment and Abuse</td>
<td>Employees are prohibited from any form of online harassment, forwarding chain letters, sending unsolicited email and other messages.</td>
</tr>
</tbody>
</table>
APPENDIX F: RESOURCES FOR CYBERCRIME VICTIMS
### Resources for Cybercrime Victims

<table>
<thead>
<tr>
<th>Resource</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>IC3</td>
<td>The Internet Crime Complaint Center (IC3, 2006) is a partnership between the US FBI and the National White Collar Crime Center (NW3C, 2006). The Internet Crime Complaint Center accepts online complaints from all businesses located in the United States, and coordinates responses with local, state and Federal law enforcement agencies. The IC3 handles a variety of crimes ranging from auction fraud, counterfeit cashier’s checks, credit card fraud, escrow services fraud, internet extortion, investment fraud, identity theft, Nigerian letter, phishing, spam and other pyramid schemes.</td>
</tr>
<tr>
<td>US DoJ</td>
<td>The United States Department of Justice (USDoJ, 2008) provides a list of appropriate federal investigative law enforcement agencies to report various types of computer, internet-related, or intellectual property crime. These agencies include the US FBI and US Secret Service.</td>
</tr>
<tr>
<td>FTC</td>
<td>The Federal Trade Commission accepts online (FTC, 2008) complaints from individuals and businesses who are victims of identity theft. The online web site provides resources and information for individuals and businesses to recover from an incident of identity theft. The FTC also provides an identity theft hotline at 1.877.ID.THEFT (438.4338). Filing a complaint with the FTC generates a detailed Identity Theft Report.</td>
</tr>
<tr>
<td>Credit Reports</td>
<td>Toll Free Numbers are available from three consumer reporting companies to place a fraud alert on the account of a business who may be a victim of fraud or identity theft. These companies include Equifax (1.800.525.6285) or Experian (1.888.397.3742) or TransUnion (1.800.680.7289). Victims may place a fraud alert on their credit reports, or may choose to place a credit freeze on their credit report.</td>
</tr>
<tr>
<td>Local Police Department</td>
<td>The Identity Theft Report, generated by filing a complaint with the FTC, may be submitted to the local police department. While the procedures for filing a local police report vary by jurisdictions, the Identity Theft Report may be incorporated into the local police report.</td>
</tr>
<tr>
<td>Local Bank</td>
<td>The local bank of a small business may retain an individual responsible for handling cases of online fraud, identity theft and cyber extortion. The Identity Theft Report from the FTC can be submitted to the bank.</td>
</tr>
</tbody>
</table>