Does Explicit Information Security Policy Affect Employees' Cyber Security Behavior? A Pilot Study

Ling Li, Old Dominion University, Norfolk, Virginia, USA; lli@odu.edu
Wu He, Old Dominion University, Norfolk, Virginia, USA; whe@odu.edu
Ash Ivan, Old Dominion University, Norfolk, Virginia, USA; IAsh@odu.edu
Li Xu, Old Dominion University, Norfolk, Virginia, USA; lxu@odu.edu
Mohd Anwar, North Carolina A & T University, USA; manwar@ncat.edu
Xiaohong Yuan, North Carolina A & T University, USA; xiaohongy@gmail.com

Abstract— **In this pilot study, we have (i) examined the relative importance of ten factors that can be used for developing new training methods and materials to improve employees' awareness and skills to defend against cyber risks, and (ii) investigated the relationship between an explicit security policy at the organizational level and individual employee's behavior and beliefs toward cybersecurity issues. Our results show that an explicit cybersecurity policy does positively affect employee's behavior towards information security risks. The insights drawn from this pilot study can be employed toward encouraging and enhancing employees' cybersecurity behavior both in the workplace and outside the workplace.**[1]

Keywords- information security; cyber security behavior; pilot study;cues to action, self-efficacy

I. INTRODUCTION

As the Internet applications increases in volume and complexity, malicious content and attacks are evolving and as a result the society is facing a greater security risk in the cyberspace than before. In recent years, Web 2.0 sites and social media sites are becoming very popular among Internet users. However, Web 2.0 sites and social media sites such as Blog, Facebook, MySpace, Twitter, and LinkedIn can pose a variety of serious security risks and threats to unwary users and their organizations.

As more and more organizations become increasingly concerned about the cyber risks in the workplace, many organizations are looking to implement their cybersecurity policy effectively. However, a global security study by Cisco [1] [2] revealed that security policies do not always work effectively for employees. Some employees in their organizations do not understand security policies and tend to underestimate security risks even though these employees receive a written security policy and instructions.

In this pilot study, we intend to extend the published studies on cybersecurity by theoretically defining the conceptual domains of employs' online security behavior and beliefs, and developing operational measures specific to advancing online security behavior research in the cyberspace workplace. We believe that this research context is particularly applicable for the emerging area of information security policy.

II. BACKGROUND

In order to develop effective security policies and provide awareness training to employees on a regular basis, employee's online security behavior must be understood before effective policies and training materials can be developed. In the past, various security measures have been proposed. For example, anti-virus software have been developed, information management standards have been proposed, secure systems design methods have been tested, and information systems security policies have been established [3][4][5][6]. However, not many organizations could successfully adopt these measures. On the other hand, very often, employees do not actively comply with information systems security policies and procedures. This kind of behavior places the organizations' assets and business in danger [6] [7]. Therefore, availability of security policy at the organizational level and employee's behavior towards security policies must be fully understood before proper user education and training materials can be developed to enhance security awareness and personal responsibility to prevent security breach such as malware and system hacking [6].

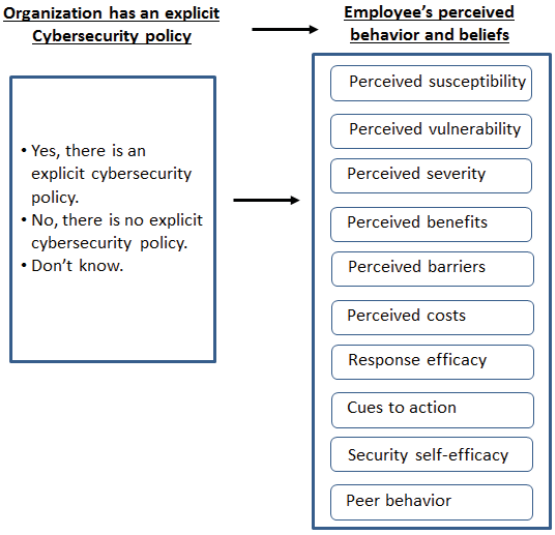

Figure 1. Conceptual Model

[1] This research is sponsored by National Science Foundation. Grant Award No. SES-1318470

978-1-4799-5554-1/14 $31.00 © 2014 IEEE
DOI 10.1109/ES.2014.66

The information security community has come to realize that the weakest link in a cybersecurity chain is human behavior. In this paper, we articulate on the following research question: how can we effectively improve employees' cybersecurity posture to engage them in secure behavior online? To address this question, we intend to (i) examine the relative importance of the factors that can be used as a foundation for developing new training methods and materials to improve employee's awareness and skills to defend against cyber security risks, and (ii) investigate the relationship between the availability of security policy at the organization and individual employee's behavior and beliefs toward cybersecurity issues.

Figure 1 illustrates a conceptual model for analyzing the effects of explicit cybersecurity policy on employee's behavior and beliefs toward cyber risks. Some of the variables used in the model re adopted from the Protection Motivation Theory (PMT) [8] [9]. PMT includes three factors that explain how threats are perceived, termed as threat appraisal factors. These are rewards or benefits (any intrinsic or extrinsic motivation for increasing or keeping an unwanted behavior), severity (the magnitude of the threat), and vulnerability (the extent to which the individual is perceived to be susceptible to the threat). PMT also includes three factors that explain an individual's ability to cope with the threat, termed as coping appraisals. They are response efficacy (the belief in the perceived benefits of the coping action by removing the threat), response cost (to the individual in implementing the protective behavior), and self-efficacy (self-confidence in his/her skills or ability in practicing computer security). In addition, some other studies [10] [11] [12] show that perceived barriers, peer behavior, and cues to action (experiences or triggers that would motivate and activate a user to practice computer security) also have some effects on users' security behavior. Ten hypotheses that are generated based on the conceptual model (Figure 1) and the published literature will be tested using data from a survey on "Employees' Online Security Behavior and Beliefs."

H1: Explicit cybersecurity policy affects employee's perceived susceptibility to security incidents.
H2: Explicit cybersecurity policy affects employee's perceived vulnerability of security incidents.
H3: Explicit cybersecurity policy affects employee's perceived severity of security incidents.
H4: Explicit cybersecurity policy affects employee's perceived benefits of practicing security procedures.
H5: Explicit cybersecurity policy affects employee's perceived barrier of practicing security procedures.
H6: Explicit cybersecurity policy affects employee's perceived cost of practicing security practices.
H7: Explicit cybersecurity policy affects employee's response efficacy of practicing security practices.
H8: Explicit cybersecurity policy affects employee's cues to action when practicing security practices.
H9: Explicit cybersecurity policy affects employee's security self-efficacy.
H10: Explicit cybersecurity policy affects peer behavior of practicing security practices.

III. DATA, METHOD AND RESULTS

A. Data Collection

In this research, the unit of analysis is individual employee. The data is collected from late 2013 to early 2014 at a state university in Virginia, USA. The behavior and belief variables are assessed on a seven-point Likert scale, ranging from strongly disagree (1) to strongly agree (7). A total of 197 responses are used for analysis. The demographic data presented in Table I shows that sixty-nine percent of the respondents are female and thirty-one percent are male. The vast majority of the participants are under thirty years old (96%). A little over 26% of the participants have an associate degree and a quarter of the respondents have a bachelor's degree.

TABLE I. RESPONDENTS' DEMOGRAPHIC INFORMATION

Measures	Item	Frequency	Percent
Gender	Male	62	31.47
	Female	135	68.53
Age	< 18	80	40.61
	18-20	103	52.28
	21-30	7	3.55
	31-40	5	2.54
	41-50	2	1.02
Education Background	High Schol	65	32.99
	Associate	52	26.4
	Bachelor	50	25.38
	Other	30	15.23

Table II provides information about participants' employment information. About 82% percent of respondents are employed; among them 66% have a part-time position and a little more than 15% have a full time job. Job responsibility ranges from senior manager, middle manager to administrative support. The length of tenure with the current company ranges from more than 20 years to less than a year.

Table III provides the company information of the participants. Respondents' industry includes retail and wholesale, healthcare and medicine, finance, information technology, education, real estate, telecommunication, military and others. The company size can be as large as more than 1,000 people and as small as 20 or fewer.

When the respondents were asked if his/her company had an explicit cybersecurity policy in place (Table III), about 40% of the participants answered "yes," 17% answered "no," and about 44% have no knowledge about their company's information security policy.

B. Constructs and Reliability

The analysis consists of two steps. Step one identifies relative factors that can be used as a foundation for developing new training methods and materials to improve employees' awareness and skills to defend against cyber risks using factor analysis. Step two investigates the

relationship between organizational security policy and individual employee's behavior and beliefs toward cybersecurity issues using a one-way analysis of variance, ANOVA.

TABLE II. RESPONDENTS' EMPLOYMENT INFORMATION

Measures	Item	Frequency	Percent
Employment	Full time	30	15.23
	Part-time	131	66.5
	Volunteer	16	8.12
	Other	20	10.15
Job responsibility	Senior Manager	8	4.06
	Middle Manager	18	9.14
	First Level Supervisor	10	5.08
	Technician	19	9.64
	Instructor	4	2.03
	Analysit	55	27.92
	Admin Support	83	42.13
Functional Area	Accounting	27	13.71
	Info Tech	8	4.06
	Instruction	1	0.51
	Operations	22	11.17
	Marketing / Sale	59	29.95
	Other	80	40.61
Tenue at Current Org.	< 1 year	78	39.59
	1-2 years	62	31.47
	3-5 years	41	20.81
	6-10 years	11	5.58
	11-20 years	3	1.52
	>20 years	2	1.02

TABLE III. RESPONDENTS' COMPANY INFORMATION

Measures	Item	Frequency	Percent
Industry	Government	11	5.58
	Education	46	23.35
	Finance/Banking/Insurance	2	1.02
	Information Technology	7	3.55
	Retail / wholesale	62	31.47
	Real Estate	2	1.02
	Telecommunications	5	2.54
	Healthcare / medical	19	9.64
	Military	4	2.03
	Other	39	19.8
Company Size	<=20	60	30.46
	21-50	36	18.27
	51-100	31	15.74
	101-500	23	11.68
	501-1000	8	4.06
	>1000	39	19.8
Company Annual Revenue	< $500,000	26	13.2
	$500,000- 1 Million	19	9.64
	$ 1 million - <$5 million	14	7.11
	$5 million - <$50 million	10	5.09
	$50 million - $100 million	6	3.05
	> $100 million	9	4.57
	I don't know	113	57.36
Information Security Policy	No	33	16.75
	Yes	78	39.59
	Don't know	86	43.65

We identified a total of ten theory-based constructs from an employee's perspective. Then, we apply a rigorous procedure for ensuring the psychometric adequacy of the resulting new multi-item measurement scales. Our hypotheses focus on the relationship among ten constructs. In this section, we provide evidence that the measurements of these constructs have been effective in terms of reliability. All of the survey items that were used for the measurement of the constructs are listed in Table IV. Additionally, Table IV reports construct symbols, factors, survey questions, means, standard deviations, and Cronbach Alpha for each factor. Empirical support for effective measurement is provided by a Cronbach Alpha.

TABLE IV. QUESTIONS AND RESULTS

Symbol	Factor	Survey Questions	Mean	Std Dev	Cronbach α
Suscep	Perceived susceptibility				0.82
		I feel that my organization could become vulnerable to security breaches	4.44	1.5	
		I feel that I could fall victim to a malicious attack if I fail to comply with my organization's information security policy.	4.12	1.56	
		I believe that my effort to protect my organization's information will reduce	4.68	1.41	
		My organization's data and resources may be compromised if I don't pay adequate attention to Information security policies and guidelines.	4.53	1.47	
Vulner	Perceived vulnerability				0.69
		I feel that my chance of receiving an email attachment with a virus is high.	3.69	1.53	
		I feel that my chance of receiving malware on social media sites is high.	4.07	1.55	
		workplace.	3.29	1.56	
		It is likely that my organization's information and data is vulnerable to security breaches.	3.94	1.4	
Severe	Perceived severity				0.8
		Having my computer infected by a virus as a result of opening a suspicious email attachment is a serious problem for me.	4.13	1.96	
		At work, having my confidential information accessed by someone without my consent or knowledge is a serious problem for me.	4.96	1.87	
		Loss of data resulting from hacking is a serious problem for me.	4.88	1.9	
Benef	Perceived benefits				0.72
		I believe that checking the filename of the email attachment can help me avoid viruses that may infect my computer.	5.38	1.44	
		I believe that compliance with my organization's information security policy will reduce the risk of losing valuable work.	5.3	1.28	
		Cyber security training makes me feel more equipped to deal with	5.15	1.24	
		I believe that using strong passwords that are at least eight characters long and consist of some combination of letters, numbers, and special characters will make my online accounts more secure.	5.83	1.23	
		I believe that changing the default privacy and security settings on my social media sites will make my personal information more secure.	5.6	1.15	
		I believe that backing up important files on my computer will reduce my concern for security.	5.19	1.41	
Barrier	Perceived barriers				0.76
		It is inconvenient to check the security of an email with attachments.	3.79	1.65	
		Changing the privacy setting on social media sites is inconvenient.	3.4	1.77	
		Backing up a computer regularly is inconvenient.	3.82	1.71	
		Cyber security training takes too much time from work.	3.42	1.45	
Costs	Perceived costs				0.44
		Updating a computer regularly is costly.	3.95	1.62	
		training.	3.42	1.36	
		It costs the organization a lot of money to handle cyber security breach	4.52	1.44	
Reffic	Response efficacy				0.83
		Complying with the information security policies in my organization will keep security breaches down.	5.02	1.22	
		If I comply with information security policies, the chance of information security breaches occurring will be reduced.	5.18	1.1	
		Careful compliance with information security policies helps to avoid security problems.	5.37	1.08	
		Using information security technologies is an effective way to protect confidential information.	5.44	1.02	
CueAct	Cues to action				0.86
		My organization distributes security newsletters or articles.	3.52	1.68	
		My organization organizes security talks and training.	3.62	1.74	
		My organization's Information Technology helpdesk sends out alert messages/emails concerning security.	3.91	1.78	
		My organization constantly reminds me to practice its computer and Internet security policies.	3.86	1.71	
SecEffi	Security self-efficacy				0.87
		I believe that I can protect my personal information on social networking sites.	4.76	1.49	
		I know how to apply security patches to operating systems.	3.04	1.83	
		I feel confident in setting the Web browser to different security levels.	4.53	1.72	
		I feel confident in handling virus-infected files.	3.38	1.94	
		I feel confident in getting rid of spyware and malware from my computer.	3.76	1.85	
		I have the skills to implement security measures to stop people from getting my confidential information;	3.9	1.79	
		I have the skills to implement security measures to stop people from damaging my computer.	4.07	1.79	
PeerBeh	Peer behavior				0.80
		My colleagues at work update their computers regularly.	4.12	1.3	
		regularly.	4.13	1.37	
		I am convinced that other employees comply with the organization's information security policy.	4.23	1.3	
		The majority of employees in my organization attend cyber security training.	3.65	1.68	

The reliabilities for perceived susceptibility was measured using four items and its Cronbach Alpha is 0.82 (Table IV). The reliability for perceived vulnerability is 0.69 and the reliability for perceived severity is 0.80. The reliability for perceived benefits and barriers are 0.72 and 0.76 respectively. The Cronbach Alpha value for costs is

0.44, which is below the acceptable value of 0.60. The reliability values for response efficacy, cues to action, and security self-efficacy are 0.83, 0.86, and 0.87 respectively. Finally, the reliability for peer behavior is 0.80.

The result of factor analysis provides the explanation to our first research objective that is to examine the relative importance of the factors for developing new training methods and materials to improve employees' awareness and skills to defend against cyber security risks.

C. Results from AVONA Analysis

The relationship between the cybersecurity policy at the organizational level and individual employee's behavior and beliefs toward cybersecurity issues was analyzed using a one-way ANOVA, between group design. Since organizational explicit information security policy is a categorical variable with three groups, analysis of variance (ANOVA) is applied to analyze the association between security policy and employee's behavior and beliefs. ANOVA is a statistical method for determining the existence of differences among several population means. Thus it is an appropriate method to analyze the differences of information security policy. Furthermore, the post hoc procedure, Tukey's HSD test, is applied to compare the difference of the three groups related to cybersecurity policy availability. The three levels of security policy awareness (i.e. yes, no, and don't know) are shown at the bottom of Table III. The Analysis of Variance (ANOVA) revealed a significant effect for perceived susceptibility ($F=6.09$; $p < 0.05$), perceived severity ($F=2.98$; $p < 0.1$), perceived cues to action ($F=16.7$; $p < 0.001$), perceived security self-efficacy ($F=5.53$; $p < 0.01$) and perceived peer behavior ($F= 8.43$; $p < 0.001$). These results support hypotheses H1, H2, H3, H8, H9, and H10 that are proposed in section II.

D. Comparison of With/Without Explicit Cybersecurity Policy at Organizational Level

Step two specifies the relationship between the organizational level security policy and individual employee's behavior and beliefs toward cybersecurity issues. Results from Tukey's HSD test showed that employees who are aware of their organizational explicit cybersecurity policy feel much stronger about the importance of security breaches than those respondents whose companies either don't have an explicit security policy or don't know if their companies have one (Figure 2). Employees in an organization that has explicit security policy also are more worried about security breaches (Figure 3). Respondents in an organization that has explicit security policy reported that their companies have taken actions to improve their employees' security awareness (Figure 4). Figure 5 shows that respondents in an organization that has explicit security policy feel that they have responsibility to protect their personal information. These participants also know the measures to protect themselves. At the same time, participants in an organization that has explicit security policy feel that their colleagues at work are more responsible for taking appropriate measures to protect their cybersecurity (Figure 6).

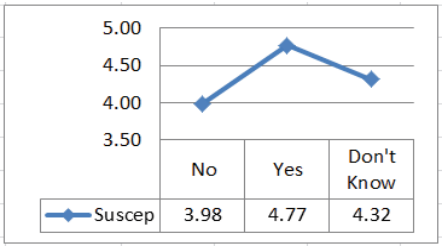

Figure 2. Post Hoc Analysis for Perceived Susceptibility (no-yes, sig < 0.05; yes-don't know sig<0.05)

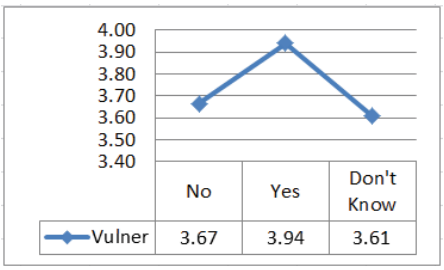

Figure 3. Post Hoc Analysis for Perceived Vulnerability (no-yes, sig < 0.05; yes-don't know sig<0.05)

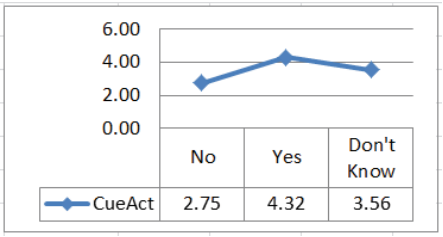

Figure 4. Post Hoc Analysis for Perceived Cues to Action (no-yes, sig < 0.05; yes-don't know sig<0.05)

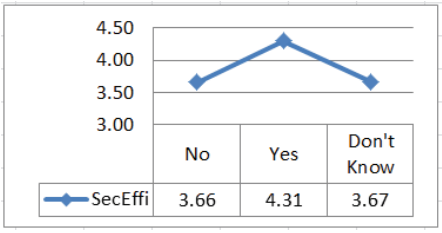

Figure 5. Post Hoc Analysis for Perceived Security Self-efficacy (yes-don't know sig<0.05)

The Post Hoc analysis provides an answer to our second objective (i.e. to explore the relationship between the availability of security policy at the organizational level and individual employee's behavior and beliefs toward cybersecurity issues). Our results show that employees in an organization that has an explicit security policy in place tend to be more worried about security breaches if they don't adhere to the company's information security policy and are more responsible for taking appropriate measures to protect cybersecurity of their organization.

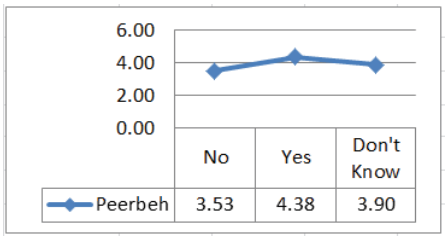

Figure 6. Post Hoc Analysis for Perceived Peer Behavior (no-yes, sig < 0.05; yes-don't know sig<0.05)

IV. CONCLUSIONS

In this pilot study, we have (i) examined the relative importance of ten factors that will be used for developing new training methods and materials to improve employee's awareness and skills to defend against cybersecurity risks, and (ii) investigated the relationship between the availability of cybersecurity policy and individual employee's behavior and beliefs toward cybersecurity issues. Six out of ten hypotheses that are proposed to test employee's online security behavior and beliefs have been supported by the data that we collected using a survey instrument.

Our results show that an explicit cybersecurity policy does positively affect employee's behavior towards information security risks. The insights drawn from this pilot study can be employed toward encouraging and enhancing employees' cybersecurity behavior both in the workplace and outside the workplace. We hope the findings from this study will be used to help organizations develop more effective employee cybersecurity training and education programs and to help organizations to implement more effective cybersecurity policies.

REFERENCES

[1] Cisco Systems. (2008a). Data leakage worldwide: The effectiveness of security policies. Retrieved Oct. 12, 2011, from World Wide Web: http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/white_paper_c11-503131.pdf

[2] Cisco Systems. (2008b). Data leakage worldwide: The effectiveness of corporate security policies. Retrieved May 12, 2011, from World Wide Web: http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/Cisco_STL_Data_Leakage_2008_.pdf

[3] G. Dhillon, and J. Backhouse, "Current directions in IS security research: toward socio-organizational perspectives", Information Systems Journal. 11, 2, 2001.

[4] M. T. Siponen, "Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods", Information and organization, 15, 4, 2005, 339-375

[5] R. Villarroel, E. Fernández-Medina, and M. Piattini, "Secure information systems development – a survey and comparison", Computers & Security, 24, 4, 2005, 308-321.

[6] S. Pahnilaa, M. Siponena and A. Mahmood, "Employees' Behavior towards IS Secur ity Policy Compliance," Proceedings of the 40th Hawaii International Conference on System Sciences – 2007, p. 7695-2755

[7] J. M. Stanton, K.R. Stam, P. Mastrangelo, and J. Jolton, "An analysis of end user security behaviors", Computers & Security, 24, 2005, 124-133

[8] R.W. Rogers, "Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation", In J. Cacioppo & R. Petty (Eds.), Social Psychophysiology. New York: Guilford Press, 1983.

[9] R.W. Rogers, and S. Prentice-Dunn, S., "Protection motivation theory", In Gochman, D. S. (ed.), Handbook of Health Behavior Research. New York, Plenum, pp. vol. 1, pp. 113–132, 1997.

[10] A. Vance, M. Siponen, and S. Pahnila, S., "Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory", Information & Management, 49, pp. 190-198, 2012.

[11] B.Y. Ng, A. Kankanhalli, and Y. Xu, "Studying users' computer security behavior using the health belief model", Decision Support Systems, 46(4), 815-825, 2009.

[12] T. Hearth, and H.R. Rao, "Protection motivation and deterrence: a framework for security policy compliance in organizations", European Journal of Information Systems, 18(2): 106-125, 2009.