Employment Status and Cybersecurity Behaviors

Mohd Anwar [a,*], Wu He [b], Xiaohong Yuan[a]
[a] North Carolina A&T State University, Greensboro, NC
[b] Old Dominion University, Norfolk, VA

***Abstract*—Cybersecurity behaviors of employees are major contributors of cyber attacks in organizations. It is important to investigate an employee's cybersecurity posture within an organization. Using our cybersecurity behavior model, we surveyed employees from different organizations on their perceptions on various cybersecurity-related psychological variables. We study whether employment status differentiates how cybersecurity is perceived and cybersecurity behavior is conducted. We use point bi-serial correlation to evaluate the strength of the relationships between employment status (i.e., full-time vs. part-time) and psychological variables (e.g., perceived severity of threat, perceived vulnerability, etc.). Our results show that full-time employees perceive vulnerability higher than those of part-time employees.**

Keywords—cyber attacks, cybersecurity behaviors; employment status; cybersecurity posture; perceived vulnerability

I. INTRODUCTION

Cybersecurity breaches (e.g., loss of confidentiality, loss of integrity, denial of service) are on the rise in organizations. From big companies like Target or J. P. Morgan to small and midsize organizations, all are victims of cyber attacks. Cybercrime costs the global economy about $450 billion each year [1]. Performing cybersecurity activities such as keeping up-to-date with cybersecurity updates and installing vulnerability patches are significant challenges for organizations.

Studies show that the weakest link in a security chain is human [2, 3]. Although many organizations have adopted state-of-the-art security technologies to protect them from various security threats, that is still not adequate, in reality, some employees do not comply with security policies for many reasons in their day-to-day work [4]. The ultimate success of organizational security depends on the compliance of individual employees with security policies.

Therefore, it is important to investigate an employee's cybersecurity posture within an organization. We use a cybersecurity behavior model (Figure 1) and cross-sectional survey study to assess cybersecurity perception and behaviors of employees. In particular, we study whether employment status differentiates how cybersecurity is perceived and cybersecurity behavior is conducted.

Our results show that full-time employees perceive vulnerability higher than those of part-time employees. Our contributions are discussed in the sections below.

II. RELATED WORK

Several studies investigated the cybersecurity behaviors of employees in organizational contexts [5, 6]. However, these studies did not consider employment type and did not differentiate between full-time employees and part-time employee when they discuss their models or report the findings. In many small and medium-size organizations, part-time employees often receive little training in cybersecurity and they may not be aware of the organization's security guidelines and procedures or top management's expectations if the security climate in their organization is not strong. As a result, individual employees including full-time and part-time employees may have a different perception of the security vulnerability, severity or extent of the damage [7]. Thus, it is critical to understand how employment status will influence an employee's security behavior so that appropriate security training or awareness programs can be designed. However, there is little theoretically grounded empirical cybersecurity research comparing views of full-time employees and part-time employees. Further research is needed to explore and compare the views of full-time employees and part-time employees such as contractors and temporary/seasonal workers that organizations employ.

III. CONCEPTUAL MODEL

Based on Protection Motivation Theory (PMT) [8] and an extensive literature survey on behavioral information security, we developed a cybersecurity behavior model (shown in Fig. 1) that integrates various factors including computer skills (CS), information seeking skills (IS), experience with cybersecurity practice (PE), perceived vulnerability (PV), perceived severity (PS), security self efficacy (SSE), perceived benefits (PB), perceived barriers (PBR), response efficacy (RE), cues to action (CA), and peer behavior (PBEH) to explain employees' self-reported cybersecurity behaviors (SRCB). Based on our model, we conducted a cross-sectional survey study to evaluate the role of employment status on the employees' perception of cybersecurity related factors such as perceived vulnerability of cyber attacks, perceived severity of cyber threats, self-efficacy, etc.

We use a point-biserial correlation to determine whether there is any association between various psychological variables of threat perception (perceived vulnerability in the system, perceived severity of threats) measured in Likert scale, and employment (which has two categories: "full-time" and "part-time").

IV. EXPERIMENT

A. Participants and Settings

We conducted an online survey on employees in various organizations about their perceptions of cybersecurity. As a result, 579 subjects from businesses and university subject

* Corresponding author.

pools completed the survey. However, we removed the data points corresponding to university students without outside employments. Four-hundred-eighty-two (482) participants from this sample were full or part time employees. The main inclusion criterion was that the participants work full-time or part-time and their job requires the use of technology. The Internal Review Board (IRB) of the investigators' institutions approved the study.

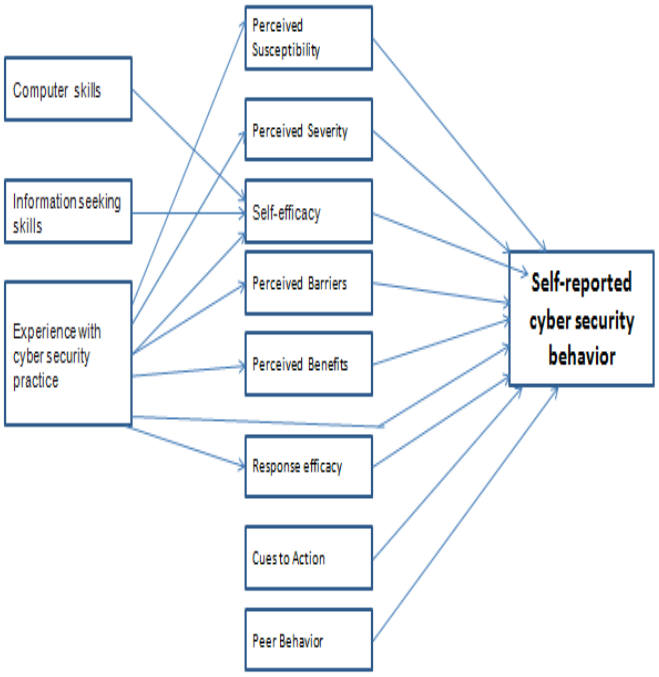

Fig. 1. Cybersecurity behavior model

B. *Measurements*

The survey includes 87 Likert items collecting data to measure an individual's computer skills, self-efficacy, prior experience with computer security practice, and other constructs depicted in the proposed model.

V. RESULTS

We only discuss results that were significant at an alpha level of < 0.01, in order to avoid over interpreting relationships with effect sizes. As Table I shows, there was a negative correlation between perceived vulnerability (PV) and Employment status, which was statistically significant (rpb = -.24, n = 482, p = .0). There was also a statistically significant negative correlation between prior experience with cyber security practice (PE) and employment status, (rpb = -.27, n = 482, p = .0) as well as between computer skills (CS) and employment status (rpb = -0.17, n = 482, p = .0).

TABLE I. POINT-BISERIAL CORRELATION COEFFICIENT

	Fulltime Employee (N=265)		Part-time Employee (N=217)			
	M	SD	M	SD	r_{pb}	p
PBEH	4.12	1.26	4.19	1.25	0.0261	0.5683
CS	5.14	0.74	4.86	0.81	-0.1766	0.0001
IS	4.94	0.63	4.77	0.61	-0.1304	0.0041
PE	4.99	1.20	4.27	1.37	-0.2713	0.0000
PV	4.63	1.01	4.13	1.00	-0.2398	0.0000
PS	4.77	1.58	4.61	1.64	-0.0496	0.2768
PB	5.70	0.95	5.68	0.88	-0.0109	0.8108
PBR	3.35	1.34	3.55	1.30	0.0773	0.0902
RE	5.64	0.90	5.41	0.86	-0.1262	0.0055
CA	4.10	1.59	3.77	1.52	-0.1053	0.0208
SSE	4.35	1.50	3.99	1.39	-0.1199	0.0084
SRCB	5.48	0.92	5.34	0.93	-0.0743	0.1035

VI. CONCLUSION

Employment status is an important factor mediating cybersecurity behaviors in general. Our study shows that cybersecurity posture of part-time employees is not as strong as that of full-time employees. Organizations need to take initiatives to improve cybersecurity behaviors of part-time employees.

ACKNOWLEDGMENT

This work was supported in part by the U.S. National Science Foundation under Grant SES-1318470 and SES-1318501.

REFERENCES

[1] T. Warren, J. Favole, S. Haber, and E. Hamilton, "Cybercrime costs more than you think" in Hamilton Place Strategies Report, 2016.

[2] R.E. Crossler, A.C. Johnston, P.B. Lowry, Q. Hu, M. Warkentin and R. Baskerville, "Future Directions for Behavioral Information Security Research," Computers & Security, 32, pp. 90-101, 2013

[3] C. Vroom and R. von Solms, "Towards information security behavioral compliance," Information Management & Computer Security, 6(4), 167-173, 2004.

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

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

[6] J. Y. Son, "Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies," Information & Management, 48(7), 296-302, 2011.

[7] B.Y. Ng, A. Kankanhalli and Y.C. Xu, "Studying users' computer security behavior: A health belief perspective," Decision Support Systems, 46(4), 815-825,2009.

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