Preliminary Investigation on Psychological Traits of Users Prone to be damaged by Cyber-attack

Takeaki Terada Yoshinori Katayama Satoru Torii Hiroshi Tsuda
Fujitsu Limited 4-1-1 Kamikodanaka, Nakahara-ku, Kawasaki-shi, Kanagawa, Japan
{ terada.takeaki, katayama.yoshin, torii.satoru, htsuda }@jp.fujitsu.com

1. INTRODUCTION

Cyber-attack has become increasingly sophisticated in recent years. The attackers perform preparatory investigation about the details of the work of the organization or the person they try to target, and reflect the results of the investigation on making the malicious mail. This mail includes malicious program files or the URL link to malicious websites, and if the targets click the files or the URL, their PCs will be infected with virus program and give the attackers the base for intruding into the targets' organization.

Besides, the data leakage accidents caused by human error are increasing. These accidents happen when people make the operational error such as attaching wrong files to their sending mail or sending their mail to different people with the same family name. Excessive workload and carelessness cause such human errors.

In this way, erroneous determining of human often brings the damage by cyber-attacks and the data leakage accidents. For preventing such affairs, we have been tackled the research on the psychological traits of the people who are prone to be damaged by cyber-attacks or data leakage accidents. The findings may predict the users who will be damaged in the near future and provide them with effective countermeasures appropriate for their each trait.

In this report, we show the result of the preliminary investigation on the psychological traits of the users prone to be damaged by cyber-attacks or the data leakage accidents. We performed this investigation by asking 1,000 internet users about the experience of being damaged in cyberspace in the last 2 years and their way of thinking.

2. RELATED WORK

We are surrounded by various hazards such as disease, traffic accidents, robbery, natural disasters, nuclear accidents, and so on. The possibility of encountering these hazards is called "risk". There are a lot of studies on the relationship between risk and human cognition. Jackson showed that people feel threats on something when they feel they cannot control it [1]. Slovic found that the basic factors of recognizing risk to something are fear and unknownness [2]. In the research on the relationship between psychological states and risk cognition, Bouyer et al. showed that the psychological states such as anxiety and fatalism affect with recognizing risk [3] and Visschers et al. showed that people who don't have any knowledge about something judge risk of it by trusting the strangers who have the knowledge about it [4].

On the other hand, there are also some researchs on the risk cognition in cyber-space. IPA and Kurino et al. examined how to encourage people to apply a security patch to their PCs and found that appealing the damage preventing effect of the patch is more effective than telling the terror of cyber-attack [5][6]. IPA also examined the relationship between the experience of being damaged in cyberspace and personal attributes and found that the user who had the experience of being deceived by phishing email or his accounts were abused, had an overconfidence on his own knowledge concerned with cyber-attack [7][7].

3. RESEARCH QUESTION

The study of [5][6] showed there are the effective psychological approaches to encourage people to take action for their safety, and the study of [7] indicated there are the psychological factors such as overconfidence relative to the experience of being damaged in cyberspace. Then we asked 1,000 internet users about the experience of damage in cyberspace in the last 2 years and their day-to-day thinking

4. METHODOLOGY

4.1 Making of Questionnaire

In the consideration of the question items, we referred to the existing knowledge about the psychological factors for avoiding risk. We show the list of psychological factors relative to the behavior for avoiding risk in Table 1. In addition we considered the factors that may relate to the experience of being damaged in cyberspace. We adopted these factors as the question items of our questionnaire.

Table 1. The psychological factors relative to avoiding risk

Factor	Explanation
Concerns on safety	The tendency to make effort for minimizing risk
Risk reception	The tendency to accept risk
Self-efficacy	The vague confidence on solving the problems by oneself
Stranger trust	The degree to trust strangers
Acquaintance trust	The degree to trust acquaintances
Cautiousness	The cautiousness for things
Authoritarianism	The tendency to obey custom, superior persons, and organizations
Regret anticipation	The tendency to fear failure
Cost recognition	The degree of the mental burden a person feels when performing some measures for avoiding risk
Benefit recognition	The tendency to prefer merits of things more than the risk
Controllability	The subjective sense to be able to control a risk in one's knowledge and skill
Status quo bias	The tendency to want to maintain current situation

Loss aversion bias	The tendency to avoid suffering a loss as much as possible

4.2 Respondents

We performed our questionnaire for approximately 1,000 internets users who are the registered members of Intage Ltd., the market research company in Japan. The users satisfy the following conditions: 1) Male or female whose age is 20 and 69. 2) An office worker who uses his own PC in more than half of his working hours. 3) At least one times of the damaged experience in a cyberspace.

5. RESULTS

In Table 2, we show the analysis result of our questionnaire by the logistic regression analysis. Table 2 shows that the respondent who has high trust in a stranger is prone to be damaged by "Abuse", and who has high "Status quo bias" is vulnerable to "Abuse" and "Privacy Leakage". On the other hand, the respondent who has strong regret anticipation is resistant to "Virus", and who has strong "Loss aversion" is resistant to "Privacy Leak" and "Fraud".

6. DISCUSSION

In this work we found some psychological traits of the users who were damaged in cyberspace. These findings require additional examinations, but those may be useful to detect the users who have high possibility of being damaged in the near future by correlating their behavior on their usual PC. This may enable us to provide users with the individual supports based on their each trait, education and the introduction of the work place culture of low-risk departments to high-risk departments.

For example, we would apply these findings to displaying a warning message with some prescribed probability when the user who has strong benefit cognition clicks URLs on mail, raising users' security consciousness by feeding back their relative evaluation value of risk to each user through personal dashboards, and introducing the work place culture of the department that keeps the low average of the risk values throughout a period of time to the department that keeps the high average.

7. ACKNOWLEDGMENTS

This work is supported by R&D of detective and analytical technology against advanced cyber-attack, administered by the Ministry of Internal Affairs and Communications. And we thank Daisuke Takagi, an assistant professor of the University of Tokyo, for his advising on our work.

8. REFERENCES

[1] Jackson,J.(2006)."Introducing fear of crime to risk research",Risk Analysis,26(1):253-64.

[2] Slovic,P.(1987), Perception of Risk,Science, 236, 280-285.

[3] Bouyer,M.et al.(2001)."Personality Correlates of Risk Perception",Risk Analysis,21,457-465.

[4] Visschers,V.et al.(2008)."Exploring the Triangular Relationship Between Trust,Affect,and Risk Perception: A Review of the Literature",Risk Management,10:156-167.

[5] Investigation Report Concerned with Risk Recognition and Behavior. (2012). Information-technology Promotion Agency, Japan (IPA). http://www.ipa.go.jp/security/economics/report/behavior/index.html

[6] Kurino, S., Yoshikai, N., Takahashi, T. (2012). Proposal of Virtual Experiment System for Computer Viral infection Situation. *IPSJ Technical Report, CSEC-58*. Information Processing Society of Japan (IPSJ).

[7] Investigation Report Concerned with the Damage in Cyberspace and Personal Attributes. (2012). Information-technology Promotion Agency, Japan (IPA). http://www.ipa.go.jp/about/technicalwatch/20120913.html

Table 2. The result of the logistic regression analysis of the data for each type of the damages

Predictor	Virus			Abuse			Privacy Leakage			Fraud		
	Pr(>|z|)		Odds ratio	Pr(>|z|)		Odds ratio	Pr(>|z|)		Odds ratio	Pr(>|z|)		Odds ratio
Safety concerns	0.03	*	0.9	0.06	†	0.9	0.02	*	0.8	0.06	†	0.8
Trust to stranger				0.01	*	1.2						
Cautiousness	0.00	**	1.2									
Regret anticipation	0.04	*	0.9									
Lowness of cost recognition 1	0.09	†	0.9				0.13		1.2	0.04	*	1.2
Lowness of cost recognition 2				0.08	†	1.2						
Prefer benefit to risk 1	0.05	*	1.1									
Prefer benefit to risk 2										0.10		1.2
Negative to sharing information 1				0.12		0.9						
Negative to sharing information 2							0.14		1.2			
Confidence on handling IT							0.00	**	0.7			
Status quo bias				0.05	†	1.2	0.03	*	1.3			
Tendency of loss aversion							0.03	*	0.8	0.07	†	0.8
Desires for possession	0.14		1.1									
Lowness of self-control				0.11		0.9						
Stress due to security measures	0.01	*	0.8	0.00	***	1.4	0.00	**	1.4	0.02	*	1.3
Knowledge about cyber-attacks										0.05	†	1.7
Subjective evaluation of work load										0.02	*	1.3
Frequency of Internet use 1				0.16		1.1						
Frequency of Internet use 2	0.09	†	0.9				0.00	**	1.4	0.14		0.8
PC handliing skill				0.00	***	1.3	0.09	†	1.2			

Note: Signif. codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '†' 0.1 ' ' 1