Applying the Lost-Letter Technique to Assess IT Risk Behaviour

Elmer Lastdrager*, Lorena Montoya*, Pieter Hartel*, Marianne Junger†
*Distributed and Embedded Security Group
†Industrial Engineering and Business Information Systems
University of Twente, The Netherlands
{e.e.h.lastdrager, a.l.montoya, pieter.hartel, m.junger}@utwente.nl

***Abstract*—Information security policies are used to mitigate threats for which a technical prevention is not feasible. Compliance with information security policies is a notoriously difficult issue. Social sciences could provide tools to empirically study compliance with policies. We use a variation of the lost-letter technique to study IT risk behaviour, using USB keys instead of letters. The observational lost-letter study by Farrington and Knight (1979) was replicated in a university setting by dropping 106 USB keys. Labels on the USB keys were used to vary characteristics of the alleged victim. Observers noted characteristics of people who picked a USB key up and whether the USB key was returned. Results show that USB keys in their original box are stolen more than used ones and that people aged 30 or younger and those who place a found USB key in their pocket are more likely to steal. This suggests that the decision to steal a USB key is taken at the moment of pick up, despite ample opportunity to return it. The lost USB key technique proved to be a feasible method of data collection to measure policy compliance and thus also risk behaviour.**

I. Introduction

Information-related security is an important topic on institutional and personal agendas. To reduce the impact of information security breaches, cost-effective ways to protect against attackers must be first identified. Some risks might be mitigated by implementing information security policies. To test the compliance with such policies, data is required. Within social sciences, many data collection tools which can be adapted to information security are available. Methods to collect data include surveys, interviews, observational research and examining existing materials. Although surveys and expert interviews are often used for obtaining data about information security, there is always the question of the validity of the results. During an interview or in a questionnaire, a person may state to follow the information security policy, but in practice fail to follow it. Therefore, we explore the feasibility of using observational research methods as a tool for collecting data, since in general this will yield more reliable data.

One of the methods of observational research is the lost-letter technique [1], [2]. It consists of dropping stamped letters in the streets, thus pretending that the letter was lost before it could be posted. Members of the public who see such a letter have the choice of posting the letter, keeping or not picking it up. The researchers measure the number of letters that are received at the destination address. By varying the addressee's characteristics, one can measure the people's attitude towards certain topics. For example, by addressing letters to different political parties and measuring the return rates of the letters, one can establish popularity of the parties [3]. It is assumed that supporters of a particular political party will feel more inclined to post the found letter than non-supporters, even if they are aware that they are participants of a lost-letter experiment [4]. In a similar way, the public opinion on various other subjects, such as gay marriage or racism, was measured by changing the addressee [5]–[9]. In other studies, (fake) money was put in the envelope [10]–[13], the importance of the letter was indicated on the envelope [14], [15] and the influence of the neighbourhood on the return-rate [16] was measured. Whereas in the standard lost-letter experiment only the influence of the victim's characteristics on the return rate is measured, researchers may decide to observe the dropped letter and note the characteristics of the person picking the letter up [11]–[13]. The lost-letter technique has been shown to be adaptable to modern techniques, such as the lost-(car)key technique [17], the lost-email technique [18]–[21] and the lost-smartphone technique [22].

We adapted the lost-letter technique to evaluate the theft of USB keys. USB keys are important for information security modelling as they may cause issues such as data leaks [23], [24] or the infection of a computer network with malware (for example Stuxnet [25] or malware that is located on USB keys found in public transport [26]). Some of these issues can be mitigated by technical means, such as data leaks which can be prevented by requiring users to use encryption. However, as technical solutions do not mitigate all threats, other means are needed to reduce certain risks. People who find and use a lost USB key put their computer at risk of a virus infection [27] and therefore form a threat to networks. For example, malware infections through USB keys may be prevented by forbidding persons to use untrusted USB keys. These solutions are often implemented as policies within organisations and require compliance of the users. For example, Carnegie Mellon University has a clear policy [28] on found USB keys: "Avoid plugging an unknown USB into your computer or a cluster computer. When a USB drive is found unattended, please give it to a cluster consultant, the Computer Services Help Center, a residence assistant (RA) or to Carnegie Mellon campus police." The lost USB key technique allows organisations to quantify the user's compliance with an information security policy. The resulting data may be used as input for modelling users' behaviour or testing the effectiveness of interventions.

The lost-letter technique and its variations are used to measure altruism [1], but whether or not a person steals a USB key is also influenced by factors other than personality, such as

the context. Theories of crime opportunity [29] can be used to explain the context of the lost USB key pick up. The Routine Activity Approach [29], [30] states that a crime is likely to occur if a likely offender meets a suitable target in absence of a capable guardian. The Routine Activity Approach lists three types of people who can prevent a crime from occurring. First, a handler might convince the offender not to commit a crime. Such a handler may accompany the person picking up the USB key and convince him/her not to steal it but to return the USB key as lost and found instead. The second type is the aforementioned guardian, who watches the target. A guardian could be the owner of the target or a person close by who watches the situation. The third type is a place manager who is responsible for the setting. An example of a place manager is a receptionist or security guard. Applying this to the lost USB key technique, implies that a subject (i.e. person who picks up the USB key) will converge in space and time with a target (i.e. USB key) in absence of a guardian or place manager and without a handler to hold the subject back. In the lost USB key technique, the target is a USB key that the victim is the alleged owner of.

To investigate whether theft of a lost USB key is related to the victim, subject and situational characteristics, an experiment was performed in a university setting, by dropping USB keys near service desks. We used the methodology of Farrington and Knight [11], [12], who look at the effects of the victim's characteristics, and adapted it to use USB keys instead of letters. This allows comparison of our results to their lost-letter experiments. Farrington and Knight used two groups: a control group consisting of unsealed letters containing no money and an experimental group with unsealed letters containing money. The control group in our experiment consisted of USB keys in their original box and the experimental group consisted of USB keys that were labelled to indicate usage. We hypothesise that USB keys from the control group get stolen more, as they do not contain data, therefore the victim does not lose any data. Alternatively, the resell value might drive theft of brand new USB keys. The ownership of a brand new USB key is not clear, making it a relatively easy target. The USB keys from the experimental group are labelled to indicate the sex of the alleged victim and the importance of the contents. We hypothesise that the victim's sex does not make a significant difference, similar to the observations from Farrington and Knight. We expect USB keys with important content to be returned more [15]. For the subject characteristics, we hypothesise that subjects who are alone, casually dressed, young or put the USB key in their pocket will be likely to steal the USB key and that males are more likely to steal than females [11], [12]. Apart from the variables from Farrington and Knight, we note whether the subject was walking in the direction of a service desk prior to picking the USB key up. We hypothesise that subjects who are walking in the direction of a service desk, will be more likely to return the USB key

In this paper, we explore the feasibility of the lost-letter technique to assess risky behaviour in relation to IT security. The contribution is the identification of situational and personal characteristics of the subject and victim that contribute to the theft of a lost USB key. Theft and consequent use of a USB key represent a security threat that organisations are in need of quantifying. Observational research provides a method of objective measurements.

The remainder of this paper is organised as follows. We describe the methodology of the experiment in section II, followed by the results in section III. In section IV we discuss the results, implications and limitations of the experiment as well as the ethical considerations.

II. Method

A field experiment was conducted by using an adapted version of the lost-letter technique that uses USB keys instead of letters. The design was based on the experiments from Farrington and Knight [11], [12], who dropped letters in the streets and observed by whom they were picked up. Teams of students dropped USB keys and observed whether they were picked up and, if applicable, by whom.

A. Design & Concepts

In the experiment, the concepts of victim and subject are used. The victim is the alleged owner of the USB key and the subject is the person who picks up the USB key. The target is the USB key itself.

The experiment used a 2x2 between-subject design. The independent variables were the sex of the victim and the importance of the data on the USB key. The dependent (outcome) variable shows whether or not the USB keys were returned to the service desk. By varying the independent variables, we aim to establish whether the subject's behaviour is influenced by the target's characteristics. In the lost-letter experiment, the recipient's address is listed on the envelope. In the case of a lost USB key, it may not be entirely clear where to return the device. In the lost-key technique (using car keys) by Forbes et al [17], this was solved by attaching a label with name and address information. Similarly, a datafile containing the owner's information could be put on a USB key. In our experiment, we considered USB keys to be stolen if they were not returned to the service desk. The USB keys had labels on both sides to show characteristics of the victim and contents of the USB key. The label on one side showed a male (John) or female (Anna) first name and a surname, whilst the other side showed its importance by labelling its contents to be either academic (thesis, i.e. important) or recreational (music, i.e. not important). Besides the experimental USB keys, a control group consisting of USB keys in their unopened box was used. The person finding a USB key from the control group could directly see that these did not contain any data.

In order to make a comparison of the data, we measured the same variables as Farrington and Knight [11], [12]. Additionally, we added the walking direction of the subject relative to the service desk as a variable. A subject can walk to a service desk, away from it or neither (e.g. in parallel). In relation to the continuous data and the comparison with Farrington and Knight, the estimated age was measured as a continuous variable and later categorised, so that our study could be compared to both studies of Farrington and Knight. Farrington and Knight's 1979 study uses a different categorisation compared to their 1980 study (ages 0-30 and above 30 versus 0-20, 21-50 and above 50), but neither justifies why these specific numbers were used. The number of companions was analysed as continuous data and later

Table I. THE INDEPENDENT AND EXTRANEOUS VARIABLES

Characteristic	Explanation	Categories
Time	Time of drop off	Time (i.e. 10:14)
TimeElapsed	Minutes elapsed into pick up	0,1,2,...
Type	Experimental group	Control (0), Experimental (1)
Sex of victim	Sex of the victim (label)	Female (0), Male (1)
Contents	Importance label	Recreational (0), Academic (1)
Clothing	Clothing of subject	Casual (0), Average (1), Smart (2)
Age of subject	Estimated age	0,1,2,...
Sex of subject	Sex of the subject	Female (0), Male (1)
Companions	Number of companions	0,1,2,...
Behaviour	Placed in pocket/handbag	No (0), Yes (1)
WalkingDirection	Relative to service desk	Towards (0), Away (1), Other (2)

categorised as alone versus accompanied, to allow comparison with Farrington and Knight. The concept behaviour refers to the actions of the subject directly after picking up the USB key (e.g. whether the subject puts the USB key in his/her pocket or handbag). Clothing was categorised as casual (i.e. jeans and t-shirt), average (i.e. trousers and shirt) and smart (i.e. suit), similar to Farrington and Knight. The measured extraneous and independent variables are listed in Table I.

B. Setting

The USB keys were dropped in nine buildings at three Dutch universities. Each selected building has a lobby containing a service desk with a receptionist. The USB keys were dropped in or near the lobby area, but not within sight of the receptionist. This was done to prevent people from feeling observed and wanting to please the receptionist by returning the USB key, or from thinking that the receptionist would pick the USB key up and deal with it. In all buildings that were used, the service desk was commonly known to be the first point of contact for lost and found items. At the time of the experiment, neither university had a policy about found USB keys.

At each location, USB keys were dropped on three ordinary wednesdays in September and October 2012, i.e. during term time. In all buildings, the experiment was conducted during three time slots (10am–11am, 1pm–2pm, 3pm–4pm). These time slots were used in an attempt to reduce the risk of somebody participating twice in the experiment, since finding a similar USB key twice could make people suspicious.

Unused 4 GB USB keys with a retail price of 5 euro were used for this experiment. The USB keys contained no (executable) data. In prior research, Merritt and Fowler [1] used a fake coin and Simon [14] and Simon and Gillen [10] used play-money, which accounts to no economic value, but can, momentarily, lead the subject to believe that the letter contains something of economic value. Farrington and Knight [11] used real money with values of between 0.20 and 5 GBP.

C. Subjects

Subjects were self-selected from the population of people walking through the lobby of one of the buildings. Typically, these include either students or employees of the university, but also contractors (e.g. cleaning staff or construction workers) and visitors. The population of potential subjects of each university is not representative for the population at large. In total 106 people picked up a USB key and therefore became subjects in the experiment.

D. Procedure

Twenty-seven groups of two or three students participated in the experiment. Before starting the experiment, we obtained permission from the faculty's ethical committee (see section IV-E) and from facility management, which runs the service desks and employs the receptionists. Six weeks before running the experiment, all receptionists were informed about the experiment and who to contact in case of questions. In the morning of the experiments, all receptionists were contacted by phone to make sure that they were aware about the experiment and to ask if they had any questions about the procedure. The receptionists were asked to behave as if they were unaware of the experiment and asked to store the returned USB keys separately from other found items. We considered this procedure essential for running the experiment correctly and for avoiding problems for the receptionist.

The students were instructed never to interact with the subjects. They were randomly assigned a location, time and selection of USB keys. Five minutes before the start of the experiment, the students introduced themselves to the receptionist. They would find a suitable location close to the service desk, but not in sight of the receptionist. One student would walk around and pretend to tie his/her shoelaces, look around to see if anybody noticed him/her and drop the USB key before walking away, similar to the procedure used by Farrington and Knight [12]. Another student would observe the USB key from a distance of about 20 meters. The students pretended to be working, reading papers or playing with their phones. If somebody picked the USB key up, a form was filled in, taking note of the subject's characteristics and behaviour and of the situation at that moment.

E. Analysis

Fourteen subjects did not look at the labels of the labelled USB keys, or the observers were unsure, and were excluded from the results as they were not fully exposed to the experimental conditions. For similar reasons, Farrington and Knight [11], [12] excluded cases in their lost-letter experiment. Subjects that picked a USB key up from the control group (i.e. not labelled) were all included. The exclusion of 14 cases reduced our dataset to 92 cases.

Farrington and Knight presented descriptive statistics and a univariate analysis (i.e. each individual variable in relation to the dependent variable). For comparison, we carried out the same analysis, including the extra variables (WalkingDirection, TimeElapsed and Content) that are specific to the lost USB key experiment. Additionally, several multivariate logistic regression models were developed. We tested whether a multi-level logistic regression was needed to account for similar results within the buildings (i.e. intraclass correlation). We found no significant effect of the individual buildings and therefore for simplicity we present the results of a regular logistic regression. A logistic regression measures the amount of variance in the return rate explained by the predictor (i.e. independent and extraneous) variables. Four models were developed: (1) a model based on victim characteristics, (2) a

Table II. NON-RETURN RATES (PERCENT) PER CHARACTERISTIC, COMPARED TO TWO LOST-LETTER EXPERIMENTS

Type	Characteristic	Category	F&K 1979	F&K 1980	Lost USB key
Experiment	Experiment type	Control	11.1 (n=18)***	10.7 (n=28)**	41.2 (n=17) **
		Experimental	30.1 (n=73)	39.3 (n=112)	12.0 (n=75)
Victim	Sex of victim	Male	30.2 (n=43)	50.0 (n=56)	7.9 (n=38)
		Female	30.0 (n=30)	28.6 (n=56)	16.2 (n=37)
	Content	Academic			14.0 (n=43)
		Recreational			9.4 (n=32)
Subject	Clothing	Casual	45.8 (n=24)	53.7 (n=54)**	19.6 (n=51)
		Average/smart	22.4 (n=49)	25.9 (n=58)	14.6 (n=41)
	Estimated age	30 or less		48.5 (n=66)*	25.5 (n=51)*
		31 or more		26.1 (n=46)	7.1 (n=42)
	Estimated age	20 or less	63.6 (n=11)*		0.0 (n=10)
		21-50	29.3 (n=41)		20.5 (n=73)
		51 or more	14.3 (n=21)		11.1 (n=9)
	Sex of subject	Male	30.2 (n=43)	41.3 (n=63)	19.1 (n=68)
		Female	30.0 (n=30)	36.7 (n=49)	12.5 (n=24)
	Companions	Alone	34.1 (n=41)	39.4 (n=71)	15.7 (n=51)
		Accompanied	25.0 (n=32)	39.0 (n=41)	19.5 (n=41)
	Behaviour	Placed in pocket	54.2 (n=24)**		75.0 (n=12)***
		Walk holding the key	19.1 (n=47)		8.9 (n=79)
		Unknown			0.0 (n=1)
	Walking direction	Towards servicedesk			10.4 (n=48)
		Away from servicedesk			25.7 (n=35)
		Other direction			28.6 (n=7)
		Unknown			0.0 (n=2)

Note. N=92. Farrington and Knight (F&K) values from [11], [12]. Significance (χ^2): * $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$

model based on subject characteristics, (3) a combined model based on all characteristics and (4) a compact model, that only uses the best predictor variables. The compact model was developed by narrowing the full model down using the Akaike information criterion (AIC) [31]. The models are reported showing odds ratios between the predictors and the return rate. For example, a predictor in our model with an odds ratio of 2.5 implies that the subject is 2.5 times more likely to steal the USB key if that condition is present. Analysis of the results showed that the predictor behaviour is a very good predictor. However, this minimised the odds ratios for the other variables. For clarification, we included two additional models (Suspect model II and Combined model II) that exclude behaviour. Both models explain less variance, but show more detail for the individual predictors.

Besides the variable age, we included the age squared as predictor in the regression models to compensate for the nonlinearity of the variable, since it is often the case that a given effect increases with age until a certain point and then it decreases (i.e. in the case of crime activity and age [30]). The number of companions (i.e. the size of a group) is not linear either [32], therefore it was squared before including it in the regression. Significance was calculated using Pearson's χ^2.

III. RESULTS

The results of a univariate analysis are listed in Table II together with the results from both studies of Farrington and Knight [11], [12]. A significant difference between the control group and the experimental group was found: people return used USB keys more often than brand new USB keys. For the non-return rates of the experimental and control groups, our results are different from the results of Farrington and Knight, where the control group gets stolen significantly less. There is

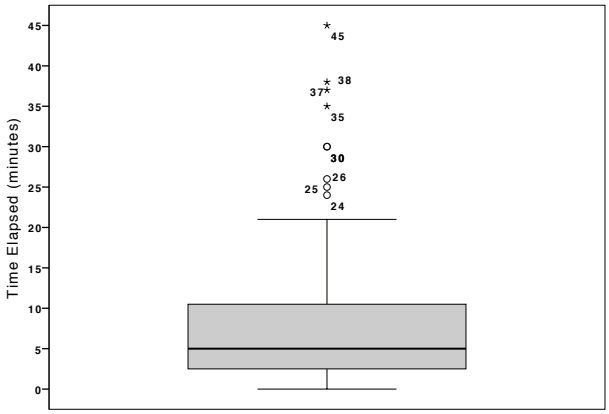

Figure 1. Box plot of the time elapsed between dropping and a subject picking the USB key up (N=92).

no relation between the time or location of dropping a USB key and the return of the device. Figure 1 displays the distribution of the elapsed time between dropping and picking up a USB key. The median time before a USB key is picked up is 5 minutes. After 2 minutes and 15 seconds, 25% of the USB keys is picked up and after 10 minutes and 45 seconds 75% is picked up. No relation was found between the elapsed time and the return rate.

A. Victim Characteristics

We did not find any significant results for the victim characteristics, although in our experiment females were victimised more than males. In their 1979 study, Farrington and Knight observed no difference in victim sex. However, in the 1980 study of Farrington and Knight males were victimised more

Table III. PREDICTORS OF THE THEFT OF LOST USB KEYS

Characteristic (reference)	Victim model		Subject model		Combined model		Compact model		Subject model II		Combined model II	
	OR	95% CI	OR	95% CI	OR	95% CI	OR	95% CI	OR	95% CI	OR	95% CI
Victim's sex (female)												
– Male	0.41*	0.09–1.82			1.40	0.15–12.97					0.57*	0.10–3.05
– Control group†	4.96*	1.01–24.30			3.03	0.30–30.41					9.45*	1.33–67.17
Label (recreational)												
– Academic	1.75	0.39–7.81			0.25	0.01–4.42	0.38	0.03–4.57			2.63	0.43–15.90
– Control group†							4.96	0.73–33.56				
Clothing (casual)												
– Average			1.00	0.17–5.74	1.19	0.20–7.04			0.55	0.14–2.16	0.63	0.14–2.84
– Smart			2.70	0.16–46.58	2.03	0.09–47.27			1.89	0.13–27.13	2.29	0.11–46.96
TimeElapsed			0.90	0.79–1.02	0.91	0.80–1.04			0.99	0.92–1.06	1.00	0.93–1.08
Age			1.04	0.57–1.89	1.09	0.55–2.14			1.26	0.76–2.09	1.33	0.77–2.32
Age^2			0.99	0.99–1.00	0.998	0.998–1.008			.996	.998-1.003	0.99	0.99–1.00
Companions			0.51	0.15–1.80	0.48	0.11–2.04			0.78	0.30–2.05	0.87	0.27–2.75
$Companions^2$			1.14	0.96–1.34	1.14	0.95–1.37	1.04	0.99–1.10	1.06	0.93–1.21	1.06	0.89–1.28
Behaviour			168.55**	7.66–3710.4	269.15**	7.59–9545.5	69.13***	6.76–706.52				
Subject's sex (female)			1.56	0.21–11.65	2.12	0.25–18.03			1.59	0.37–6.79	1.54	0.31–7.60
WalkingDirection (towards service desk)												
– Away			0.91	0.15–5.38	0.84	0.10–6.90			2.82	0.73–10.90	3.55	0.81–15.56
– Other			0.25	0.01–8.89	0.42	0.02–10.78			3.32	0.45–24.21	3.70	0.43–32.18
Constant	0.14**	0.40–0.50	0.16	0.00–3266.1	0.06	0.00–2723.8	0.06***	0.01–0.28	0.01	0.00–21.62	0.00	0.00–6.25
R^2 i.e. variance explained	.103		.418		.474		.412		.134		.240	
Model significance	.03*		0.00***		0.00***		0.00***		0.33		0.09	

Note. N = 92. OR = Odds Ratio. CI = Confidence Interval. †The control group was coded with value 2. Due to collinearity, the output of only one control group is included. Significance (χ^2): * $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$.

than females, although the result was non-significant. Contrary to our hypothesis, the return rate for USB keys labelled as having important contents were returned less than USB keys labelled as containing non-important contents, although the results was not significant.

The interactions sex of subject and sex of victim showed the non-significant result that males stole more from females (20.0%, n=30) than from males (7.7%, n=26), whereas females stole exclusively from males (8.3%, n=12), and never from other females (n=7). Similarly, the interaction of importance with the victim's sex is non-significant, although more USB keys with academic contents of females (21.1%, n=19) were stolen compared to keys with academic content of males (8.3%, n=24).

B. Subject Characteristics

For the subject's characteristics, two significant differences were found. First, the estimated age of the subject is significant when the categorization of Farrington and Knight's 1980 [12] study is used. People who are younger than 30 years tend to steal more often (25.5%, n=51) than people who are older than 30 (7.1%, n=42). This is in agreement with the 1980 study of Farrington and Knight. The relation between age as a continuous variable and the dependent variable is not significant. The characteristic behaviour is correlated to the non-return of the USB keys. Subjects who put the USB key in their pocket or handbag, steal the device in 75% (n=12) of the cases. Subjects holding the USB key in their hand fail to return the device in only 8.9% (n=79) of the cases.

The other subject characteristics were non-significant. A subject who is alone tends to return the USB keys more often than subjects who are accompanied. This contradicts the results of Farrington and Knight. The results of the other subject characteristics were not significant, but comparable to the lost-letter studies. The characteristic clothing was less important than in the studies of Farrington and Knight; people dressed casually stole in 19.6% of the cases and people dressed average or smart stole in 14.6% of the cases. The sex of the subject was not significantly of influence on the return rate, although males stole slightly more (19.1%, n=68) than females (12.5%, n=24). This is in line with the studies of Farrington and Knight. Interestingly, significantly more men (n=68) than women (n=24) picked up the USB key ($\chi^2(1) = 21.0$, $p < 0.001$). A variable that we introduced in our experiment was the walking direction of the subject, which recorded whether the subject was walking towards the service desk, away from it or in a different direction. Even though the result is not significant, people walking in the direction of a service desk returned the USB key more than people walking in another direction. This is in line with our hypothesis.

C. Models

The results of the logistic regression models are listed in Table III. Six models are included. The model with only the victim's characteristics explains around 10.3% of the variance and the model with only the subject's characteristics explains around 41.8% of the variance. The maximum variance we can explain is 47.4%, when all 11 predictor variables are included. The compact model includes only the content, the number of companions squared and the behaviour (whether the key was put in a pocket or handbag) as best predictors and still explains a reasonable 41.2% of the variance. The two models excluding the predictor behaviour explained 13.4% for subject model II and 24.0% for the combined model II, indicating

that behaviour is indeed very relevant to predict the return of a USB key.

IV. Discussion

The current study examined the willingness to return lost USB keys in a university setting and the influence that characteristics of the victim, subject and situation have on the return rate. In case of a lost USB key, the return rate is an indication of risk behaviour, since using a found USB key puts the computer at risk of a virus infection. The results support our hypothesis that USB keys in their original box are stolen more often than USB keys that were used. Furthermore, we found support for the hypothesis that people aged 30 years of younger steal more compared to people who are older than 30. Finally, results show that placing the USB key in a pocket or handbag is a good predictor of theft, which was in line with our expectations. Consequently, the decision to steal is made at the moment of pick up, indicating the feasibility of researching situational and personal characteristics as predictors of risk. No evidence was found to support the other hypotheses.

USB keys from the control group (i.e. in an unopened box) were stolen significantly more than USB keys from the experimental group (i.e. used, with labels). This can be explained by the nature of our experimental set-up. It is likely that subjects estimated the economic value of a used USB key as much lower than the brand new one, therefore the perceived value might have been related to the resell value. The results suggest that subjects who pick a labelled USB key up either perceive its economic value as too low to steal, or have genuinely empathy for the victim, resulting in a higher return rate.

Results showed the elapsed time between dropping a USB key and a subject picking the device up to be low. The implication of this is that a person who loses a USB key containing important content in a public location like a lobby, has only minutes to recover his/her device. The observers indicated that most people who noticed the USB key, picked it up. However, several observers reported people intentionally kicking away the USB key (n=7) or stepping on a USB key and not noticing (n=1).

A. Victim Characteristics

No evidence was found to support the hypotheses about the characteristics of the victim. The nonsignificant results showed females to be victimised more than males, suggesting further research to establish whether the result is coincidental or contradicting prior lost-letter experiments. The results related to the indication of importance of the contents of the USB key did not yield significant effects, but USB keys labelled as important were stolen more often than the devices containing non-important contents. An interesting interaction is the sex of the victim versus sex of the subject. Results suggest that males steal more from females than from other males and females steal more from males than from other females. However, since these results were not significant, there is no evidence to support statements about a higher likelihood to steal from the opposite sex.

B. Subject Characteristics

No evidence was found for using the type of clothing of the subject as predictor of theft. The non-return rates were hardly affected by the clothing, in contrast to results of Farrington and Knight. The estimated age, however, was found to be significant if categorised as 30 years or younger and 31 years or older. Subjects estimated to be 30 years or younger are more likely to keep the USB key than older subjects. This is in line with the results from Farrington and Knight (1980) and age of criminal behaviour in general [30]. When crime is categorised according to the 1979 study of Farrington and Knight, no significant results were found, however, subjects with an estimated age of 20 or younger never stole a USB key in our experiment. The influence of subject's sex on the return rate was marginal, males stole more than females, but there is no significant difference. In prior research, subjects who were alone stole more often, compared to subjects who were accompanied; however, our data show that accompanied subjects steal more often, although these results are not significant. Evidence was found to support that placing the USB key in a pocket or handbag is a very good predictor of theft of the device, suggesting that the decision to steal is taken at the moment when the USB key is picked up. It was hypothesised that, given the opportunity, people would return the USB key. No evidence was found, although subjects walking towards a service desk returned the USB keys more often than subjects walking in another direction, but the result was not significant.

C. Models

A logistic regression was used to create six models. A model with only victim characteristics can explain about 10.3% of the variation, whilst a model with only subject characteristics explains about 41.8%, suggesting that subject characteristics are a more important predictor than victim characteristics. The complete model explains 47.4% of the variation in the non-return rate, while our compact model, consisting of three predicting variables, managed to explain 41.2% of the variation. The three best predictors were: the importance of the contents according to the label, the squared number of companions of the subject and whether the subject placed the USB key in his/her pocket or handbag after picking it up. Within our data sample, theft was best predicted based on the situation (accompanied or not, label on USB keys) and person behaviour (placing USB key in pocket).

D. Limitations

The lost USB key technique inherits several limitations from the lost-letter technique. Similarly to the lost-letter technique [33], a large sample size is needed to obtain significant results. In the current study, the sample size of 92 is too small to obtain significant results on more variables. Observing the lost items is particularly time consuming, although it can provide insights into the exact behaviour of the subject. Collecting data for this type of research has proven difficult, since the number of locations that are available is limited. Locations can only be used when a service desk, reception or other kind of place manager is active, so that people have the option of returning the USB key to that person.

As far as we could observe, none of the subjects realised that an experiment was being conducted. In the university

setting where our experiment was performed, it is common for students to hang around or work in common areas, which is why the observers could remain undetected. At any point in time, there are always people waiting for acquaintances near the entrance and service desk of the buildings, which proved to be an excellent way of hiding the observers. However, one subject reported to the service desk that someone was playing a joke, as he had seen a similarly labelled USB key before. Even though he was aware that something was going on, he did not see the observers. In another situation, a bystander overheard the subject talking to the service desk employee. The bystander mentioned that he had seen such a USB key earlier and that he had inserted it on his/her computer and found that is contained no data. We do not know whether it had been the bystander's intention to find identity information to bring back the USB key. The bystander mentioned to the receptionist that it probably contained a virus and warned the subject about it. However, this indicates the willingness of people to insert found USB keys in their own computer. This situation points out a limitation of the lost-letter method with a limited set of locations. In our setting, we tried to prevent the subject finding multiple USB keys by spreading the observations over three working days with 2 weeks between the experiments, and by randomly allocating time slots and buildings to groups of students.

Another consideration inherent to the use of the lost-letter technique is the self-selection of subjects. We did not take note of the characteristics of people passing by the USB key, so we are unable to make statements about the selection of subjects in relation to the population of potential subjects. Future experiments could consider measuring the number and characteristics of people passing by. This would, however, require more observers. Furthermore, it remains problematic how to reliably measure who sees the USB key, or letter, but decides to not pick it up.

Another issue regarding the validity is the way measurements are recorded. Students in groups of two or three record basic properties of the situation and characteristics of the subject. To minimise errors, students were asked to take good care of this. Especially for age estimation this is problematic. Internal discussions within a single team should smooth the age estimation, but unfortunately, we have no measures of inter-rater reliability.

Our interpretation of the return rate is that only USB keys that were brought to a service desk, either immediately or at a later moment, count as being returned. For the control group, this is the only way of returning them. For USB keys from the experimental group, one can think of scenarios in which the subject would try to insert the USB key in his/her computer in an attempt to find identity information of the victim, other that the name on the label. Thus, our non-return rates consist of subjects who stole the USB keys, of subjects who initially took them, but later decided to search for the owner, and subjects who did not consider the service desk as a method of handing lost property in. Twice the USB key got returned to the service desk at a later moment. A construction worker picked up a USB key before going for lunch outside and returned it to the service desk when entering the building again. On a second occasion, a USB key got picked up by a subject when entering the building but initially passed by the service desk, only to return a few minutes later to return the USB key to the service desk. Two USB keys were relocated (i.e. the subject moved the device from one to another location) and for practical reasons, we counted those as not stolen.

The feasibility of the lost USB key methodology depends mostly on the possibility to return the device to somebody who is responsible for the area. Subjects should feel comfortable to return the USB key. If this is not the case, they may prefer to take it home or relocate it at a central location, which would render the method less useful for measuring altruistic or risky behaviour. In our experiment, the service desk was the most logical –and nearest– location to return the USB key to.

Finally, since we didn't interview the subjects, we are unaware of their motivation for keeping the USB key. Knowing their motivation would be useful information, but it would reveal that an experiment is going on.

E. Ethical Considerations

As with all lost-letter experiments, there are some ethical considerations [18]. Due to the nature of the lost-letter experiment, informed consent is not feasible, as this would invalidate the experiment. Another option would have been to inform subjects about the experiment afterwards and ask for permission retrospectively in a debriefing. However, this would endanger the rest of the observations, since subjects could tell others about the experiment. Once the rumour spreaded, people may have been drawn to the lobby to pick up a 'free USB key'. The observers would need to mention to the subject that they would like to interview him/her in connection with the USB key stolen. For these reasons, we decided to observe and not inform the subjects about the experiment. The implication of this is that a subject who stole a USB key kept the device. We did not consider the lack of debriefing or informed consent problematic, as there are no negative consequences for the subjects. However, one of the subjects inserted the labelled USB key in his computer (see section IV-D) and, after observing it was empty, mentioned to the receptionist that it must contain a virus. This could be avoided by putting some files on the device, thereby pretending it is indeed in use.

In an early stage the use of 'call home' software was discussed as a measure of how many people would use the USB key. We considered this unethical in the environment for our experiment, since the buildings of the universities are open for anybody to enter. Students and employees may bring their own device to the university. If any kind of tracking software were to be on the USB keys, there would be negative consequences (i.e. stress) for the subjects if they became aware. However, for organisations that have buildings with proper access control and exclusively use company-owned hardware, the use of a simple tracking tool sending an anonymous 'USB key plugged in'-message may be feasible to collect aggregated information about compliance.

All observers (students), research assistants and lecture staff had to sign a nondisclosure agreement regarding the personal identifiable information. During the experiment, observers may recognise a subject, or note information that could be related to a specific person.

F. Implications

The lost USB key methodology provides a method for generating relevant data for IT and facility managers to either design or redesign cyber security policies and test compliance with these policies. Variations of the lost letter experiment may open the field of data generation by providing a method to quantify security issues.

ACKNOWLEDGMENTS

The authors would like to thank the students and receptionists that assisted in the experiments. In particular, we thank Eleftheria Makri, Marjolein van Koelen and Matthijs de Haan for their assistance in setting up the experiment.

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 318003 (TREsPASS). This publication reflects only the author's views and the Union is not liable for any use that may be made of the information contained herein.

REFERENCES

[1] C. Merritt and R. Fowler, "The pecuniary honesty of the public at large," *The Journal of Abnormal and Social Psychology*, vol. 43, no. 1, pp. 90–93, 1948.

[2] S. Milgram, L. Mann, and S. Harter, "The Lost-Letter technique: A Tool of Social Research," *Public Opinion Quarterly*, vol. 29, no. 3, pp. 437–438, 1965.

[3] R. L. Shotland, W. G. Berger, and R. Forsythe, "A validation of the lost-letter technique," *The Public Opinion Quarterly*, vol. 34, no. 2, pp. 278–281, 1970.

[4] D. M. Fessler, "Return of the lost letter: Experimental framing does not enhance altruism in an everyday context," *Journal of Economic Behavior Organization*, vol. 71, no. 2, pp. 575–578, 2009.

[5] I. Theodore Montanye, F. Ronald, and R. Kenneth, "Assessing prejudice toward negroes at three universities using the lost-letter technique," *Psychological Reports*, vol. 29, no. 2, pp. 531–537, 1971.

[6] A. Ahmed, "Muslim Discrimination: Evidence From Two Lost-Letter Experiments," *Journal of Applied Social Psychology*, vol. 40, no. 4, pp. 888–898, 2010.

[7] G. B. Forbes, R. K. TeVault, and H. F. Gromoll, "Willingness To Help Strangers As A Function Of Liberal, Conservative Or Catholic Church Membership: A Field Study With The Lost-Letter Technique," *Psychological Reports*, vol. 28, no. 3, pp. 947–949, 1971.

[8] I. Waugh, V. Edmund, and B. Rienzi, "Assessing attitudes toward gay marriage among selected Christian groups using the lost-letter technique," *Psychological Reports*, vol. 86, no. 1, pp. 215–218, 2000.

[9] F. S. Bridges, D. A. Anzalone, S. W. Ryan, and F. L. Anzalone, "Extensions of the lost letter technique to divisive issues of creationism, darwinism, sex education, and gay and lesbian affiliations," *Psychological Reports*, vol. 90, no. 2, pp. 391–400, 2002.

[10] W. E. Simon and M. J. Gillen, "Return Rates Of "Lost" Letters As A Function Of Whether The Letter Is Stamped And Amount Of Money Apparently In The Letter," *Psychological Reports*, vol. 29, no. 1, pp. 141–142, 1971.

[11] D. P. Farrington and B. J. Knight, "Two non-reactive field experiments on stealing from a 'lost' letter," *British Journal of Social and Clinical Psychology*, vol. 18, no. 3, pp. 277–284, 1979.

[12] ——, "Stealing From a "Lost" Letter: Effects of Victim Characteristics," *Criminal Justice and Behavior*, vol. 7, no. 4, pp. 423–436, 1980.

[13] T. Gabor and T. Barker, "Probing the public's honesty: A field experiment using the "lost letter" technique," *Deviant behavior*, vol. 10, no. 4, pp. 387–399, 1989.

[14] W. E. Simon, "Return Rates Of "Lost" Letters As A Function Of Whether The Letter Is Stamped And The Apparent Importance Of The Letter," *Psychological Reports*, vol. 29, no. 3, pp. 937–938, 1971.

[15] K. Deaux, "Anonymous altruism: extending the lost letter technique," *The Journal of Social Psychology*, vol. 92, pp. 61–66, 1974.

[16] J. Holland, A. S. Silva, and R. Mace, "Lost letter measure of variation in altruistic behaviour in 20 neighbourhoods." *PloS one*, vol. 7, no. 8, 2012.

[17] G. B. Forbes, R. K. TeVault, and H. F. Gromoll, "Regional differences in willingness to help strangers: A field experiment with a new unobtrusive measure," *Social Science Research*, vol. 1, no. 4, pp. 415–419, 1972.

[18] S. E. Stern and J. E. Faber, "The lost e-mail method: Milgram's lost-letter technique in the age of the Internet," *Behavior Research Methods, Instruments, & Computers*, vol. 29, no. 2, pp. 260–263, 1997.

[19] J. Vaes, M. Paladino, and J. Leyens, "The lost e-mail: Prosocial reactions induced by uniquely human emotions," *British journal of social psychology*, vol. 41, no. 4, pp. 521–534, 2002.

[20] B. J. Bushman and A. M. Bonacci, "You've got mail: Using e-mail to examine the effect of prejudiced attitudes on discrimination against arabs," *Journal of Experimental Social Psychology*, vol. 40, no. 6, pp. 753–759, 2004.

[21] O. Tykocinski and L. Bareket-Bojmel, "The Lost E-Mail Technique: Use of an Implicit Measure to Assess Discriminatory Attitudes Toward Two Minority Groups in Israel," *Journal of Applied Social Psychology*, vol. 39, no. 1, pp. 62–81, 2009.

[22] "The Symantec Smartphone Honey Stick Project," Symantec, 2012. [Online]. Available: http://www.symantec.com/content/en/us/about/presskits/b-symantec-smartphone-honey-stick-project.en-us.pdf

[23] "Nuclear plant data lost by health and safety watchdog employee," The Guardian, February 17th 2012. [Online]. Available: http://www.guardian.co.uk/environment/2012/feb/17/nuclear-plant-lost-health-safety

[24] The Canadian Press, "Government USB Key With Personal Info Of Thousands Of Canadians Goes Missing," Huffington Post, December 28th 2012. [Online]. Available: http://www.huffingtonpost.ca/2012/12/28/government-personal-info-missing-usb-key-canada_n_2377503.html

[25] N. Falliere, L. Murchu, and E. Chien, "W32.Stuxnet Dossier," Symantec, Tech. Rep., February 2011.

[26] P. Ducklin, "Lost USB keys have 66% chance of malware," December 7th 2011. [Online]. Available: http://nakedsecurity.sophos.com/2011/12/07/lost-usb-keys-have-66-percent-chance-of-malware/

[27] A. Tetmeyer and H. Saiedian, "Security threats and mitigating risk for usb devices," *Technology and Society Magazine, IEEE*, vol. 29, no. 4, pp. 44–49, 2010.

[28] "Social Engineering Using a USB Drive," Carnegie Mellon University, June 2013. [Online]. Available: http://www.cmu.edu/iso/aware/be-aware/usb.html

[29] M. Felson and R. V. Clarke, "Opportunity makes the thief: Practical theory for crime prevention," *Police research series*, no. 98, 1998.

[30] M. Felson and R. Boba, *Crime and everyday life*, 4th ed. SAGE, 2010.

[31] H. Akaike, "Information theory and an extension of the maximum likelihood principle," in *Proceedings of the Second International Symposium on Information Theory*, 1973, pp. 267–281.

[32] H. Klüpfel, "The simulation of crowd dynamics at very large events – calibration, empirical data, and validation," in *Pedestrian and Evacuation Dynamics 2005*. Springer, 2007, pp. 285–296.

[33] L. Liggett, C. Blair, and S. Kennison, "Measuring gender differences in attitudes using the lost-letter technique," *Journal of Scientific Psychology*, pp. 16–24, 2010.