Are Firms Perceived As Safer After an Information Breach?

Hsiao-Ching Kuo, University South Florida, USA
Sajeev Varki, University South Florida, USA

With hackers being active in their attempts to steal customer information, prior research has focused on how information breach influences firms at an aggregate level. We examine consumers’ decision at the individual level and find that consumers would feel safer to stay with the breached firm if attack is random.

[to cite]:

[url]:
http://www.acrwebsite.org/volumes/1017691/volumes/v42/NA-42

[copyright notice]:
This work is copyrighted by The Association for Consumer Research. For permission to copy or use this work in whole or in part, please contact the Copyright Clearance Center at http://www.copyright.com/.
Are Firms Perceived As Safer After An Information Breach?

Hsiao-Ching Kuo, University of South Florida, USA
Sajeev Varki, University of South Florida, USA

EXTENDED ABSTRACT

While companies have taken great efforts to collect consumer information in order to improve consumers’ overall experience, hackers have been equally active in their attempts to steal this data. For example, Facebook was attacked by the Ramnit worm in 2012 which stole Facebook login credentials from over 45,000 users (Karlin 2012) and Target was hacked with 70 million of customer information being compromised (Smith 2014). Research has shown that firms that experience information breaches are financially impacted by stock market reactions (Malhotra and Malhotra 2011; Campbell et al. 2003). Investors apparently expect consumers to leave when a firm is breached which could explain the drop in valuations.

We propose the idea that the customers of a firm that has been hacked may prefer to stay with the firm that has been hacked (rather than leave), provided that the attack were perceived to be a random event. Gambler’s fallacy provides an explanation for this counterintuitive response. Gambler’s fallacy refers to the mistaken belief that the randomness expressed in large samples will be expressed even in small samples (Ayton and Fischer 2004; Tune 1964). Thus, when individuals see heads in the tosses of a coin they believe to be fair, they are more prone to predict that the next outcome is more likely to be a tail than a head. In our context, when attacks are considered random, individuals would expect future attacks as less likely given that an attack has already occurred. Conversely, when people believe that the source of a sequence of events is non-random (systematic), they would expect the previous outcomes to repeat into the future and expect future attacks as more likely. Hence, our study examines how the perceived nature of the attack—whether random or systematic—influences how consumers feel about the safety of their information and their intention to stay or switch from a firm after a hack attack. Four studies are conducted to examine the relationship between the effect of the perceived nature of the attack (random vs. systematic) on consumers’ intention to stay with the firm.

Four experiments show that consumers by default tend to switch from a firm after an information breach as they assume the attack is systematic. However, when the attack is considered random, consumers tend to stay with the firm regardless of the security level at the firm. This is because when the attack is random, consumers predict a lower likelihood of future attack and hence perceive the firm to be safer. However, if the attack is considered systematic, consumers are only willing to stay if the firm has an excellent security system (vs. average security system). Additionally, consumers are less likely to stay when they are almost breached than when they are actually breached if the hack attack is considered random, lending credence to the expression that ‘the bark is often worse than the bite’.

In study 1 we conducted a 2 (nature of attack: random vs. control) x 2 (level of security system: excellent vs. average) between-subject design. The results show that consumers are more likely to stay with the breached firm if they consider the attack to be random. However, no interaction was found in study 1 showing that the effect of randomness holds true in both excellent and average security conditions.

In study 2 we conducted a 3 (nature of attack: random vs. systematic vs. control) x 2 (level of security system: excellent vs. average) between-subject design. We also included an ‘undecided’ option to tease out the potential confound of status quo effects. The results show that after excluding the undecided participants, a higher percentage of participants choose to stay with the firm if the attack is considered random than systematic, regardless of the security level at the firm. Interestingly, those in the systematic condition respond similarly as those in the control group and indicate a greater likelihood of staying only if the security level at the firm is excellent. This shows that consumers by default perceive the attack to be systematic if no additional cue on the randomness of attack is provided. Perceived safety at the firm is found to mediate these effects.

In study 3 we take into account of “near-miss” events and examine consumers’ responses to random and systematic attacks when the attack results in a hit, resilient near-miss, and a vulnerable near-miss. Thus, a 2 (random vs. systematic) x 3 (breach condition: hit vs. resilient near-miss vs. vulnerable near-miss) between-subject design was conducted. We find that consumers are more likely to stay with the firm if the attack results in a resilient near-miss than a hit. Interestingly, consumers are less likely to stay with the firm if the random attack results in a vulnerable near-miss than an actual hit, lending credence to the expression that “the bark is often worse than the bite” where the fear of threat (vulnerable near-miss) can sometimes be greater than the actual harm (hit).

In study 4 we consider a dynamic setting which simulates a sequence of attacks. This allows us to examine whether consumer feel safer after a random attack is due to their lower perceived likelihood of future attacks. A one factor, two level (random vs. systematic) design was conducted. Participants were shown different patterns of attack sequence (“OXOOXXXXX” vs. “OOOOOOOXXXXX” with “O” refers to no attack attempt and “X” refers to attack attempt being made) that differ in their switching rates as prior research has shown that people tend to perceive greater randomness when the switching rate is higher (Falk 1981). As expected, when consumers perceive an attack to be random, they predict that the firm is less likely to be hacked in the future and thus feel safer to stay with the breached firm.

In summary, this study contributes to the marketing literature by focusing on how individuals respond to information breaches in a digital economy rife with information theft. With a different perception of nature of attack, consumers will feel safer to stay with the firm.

REFERENCE


