Improving Data Breach Notifications For Organizations

Clovis Wanziguya [Department of Information & Communication Technology], Harrison Landis [Department of Statistics],
Hood Semwogeree [Department of Information & Communication Technology], Zhuo Chen [Institution for Software Research]

INTRODUCTION

Data Breach Statistics:

- More than ***7840*** data breaches since January, 2005
- ***1.6*** data breaches per day
- ***10 billion*** breached record since January, 2005
- Estimated ***64 million*** adults in United States received breach notifications with *12 months*
- ***44%*** people first know the breach from resource other than the breached organizations
- ***48 states*** have enacted laws requiring breach notifications by 2017

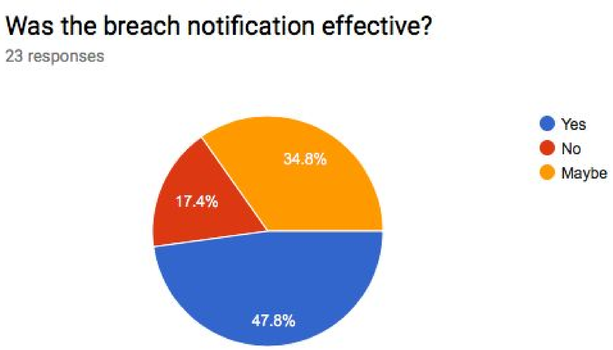
However the notifications may not be user-centric...

Survey

Setup

- Survey through Google involving 25 participants
- Asked whether participants have received notifications or not
- Asked participants to evaluate the effectiveness of notification
- Asked for comments on the notifications

Results



Good Practices Mentioned by Participants:

- Notify customers in time
- Explain what happened clearly
- Offer credit monitoring
- Tell customers what to do

What to avoid:

- Ambiguous words such as "likely", "may"
- Unclear remediation
- No notice from the breached company at all, *WORST!*

Data Breach Notification Evaluation Metric

Scorecard

Category	Question	Score	Details	Category	Question	Score	Details
Time Frame	How long does it take for the organization to notify the relevant authorities after discovering a breach has occured.	0:Company Never Notifies Authorities 5: Company Notifies Authorities Immediatly 0-5	Relevant authorities should be notified immediately upon discovery of a data breach	Notice System / Layout	Medium of communication about the breach (Phone, Email, Physical, Mail, Blog, Radio or TV advert, SMS) in context of organization	5: Yes, The Medium Of Communication Matches The Organizational Context 0: No, The Medium Of Communication Does Not Match The Organizational Context 1 or 5	Some mediums of communication are more appropriate for different organizations than others. A social media company sending notificaitons by physical mail is not going to be as effective as in application notification or email.
	How long does it take for the organization to inform its customers after discovering a breach has occured.	0:Company Never Notifies Customers 5: Company Notifies Customers Within 24 Hours 0-5	Informing customers in a timely manner following the discovery of a breach put them in the best postition to be aware of fraudulent activity on their accounts.		Reading level of breach notice (scored by an online calculator)	Convert Score From Calculator Used To A 0-5 Scale.	Above all else if the customer cannot understand the language within the notification even if the organization covers all of the other topics in this scoring system it doesn't matter as none of that information will be conveyed.
Explanation / Remediation	Explain to customers of how the breach occured	0:Company Never Gives Explanation of Breach 5: Company Lays Out The Details Of The Breach Fully 0-5	An explanation of the details of the breach follows the principle of transparency as to what the organization was doing wrong in respect to protecting their customers data.		Generic Or Customized Format	0: Overly Generic Formatting 5: Customized To Each Individual Customer 0-5	The more the notifications are geared towards individual customers the more trusting customers are of the information included.
	Explain to customers what data was compromised / severity of the breach.	0: No Mention Of What Data Has Been Compromised 5: All Data Compromised Disclosed And Explained 0-5	Giving customers a detailed explanation of which of their data has been compromised and the potential implications of it being leaked.		Follow up after the initial notice	0: No Follow Up 5: Follow up 0 or 5	Follow ups remind customers of breaches they may have forgotten about as well as update them on any developments within the organization or legal system related to the breach.
	Explain to customers what steps the organization is taking to handle the incident	0: No Mention Of Steps Taken 5: Explains All Steps Currently Taken And Future Plans 0-5	Letting customers know what steps are being taken at the organizational level again gives a level of transparency to the process in the present and future.				
	Explain to customers what steps they individually can and should take now and in the future	0: No Metion Of Steps For Customer To Take 5: Lays Out A Detailed Plan Of Steps Customer Should Take 0-5	Giving customers a plan of action for what they can do in order to protect their personal information is important especially when the breach is very large and customers may not be able to speak to a represetative about their individual case.				
	(OPTIONAL) Offer customers some sort of free services relevant to remediation of the breach	5: If They Offer Some Type of Free Service As A Remediation	Not required but helps when free services are given out to help with remediation				

Explanation of Scoring

- Categories and sections based on user feedback from the survey
- Organizations can use the scorecard to evaluate their systems for DBN's.
- Some automatic disqualifiers exist, such as not informing legal authorities or customers of a breach.
- Scoring is generic and doesn't take into account state and local laws regarding DBN's
- Scoring is sector neutral, and not geared towards any specific industry.
- Free services to aid in remediation are counted as a bonus.
- Fair Information Practice Principles are incorporated where applicable.

Future Work

- Recruit a panel of experts including privacy professionals, lawyers, linguists and professional writers to rate breach notifications
- Recruit participants and collect breach notifications they received, ask for their experience in how the process went for them
- Take demographic and behavioral information into account

ACKNOWLEDGEMENTS

- Professor Rebecca Balebako
- Professor Lujo Bauer