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

Was the breach notification effective?

23 responses
- 34.0% Yes
- 17.4% No
- 47.8% Maybe

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!

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 the process went for them
- Take demographic and behavioral information into account

ACKNOWLEDGEMENTS

- Professor Rebecca Balebako
- Professor Lujo Bauer