Individuals’ Awareness, Perception, and Responses to Data Breaches that Affected Them

Peter Mayer*, Yixin Zou*, Florian Schaub, and Adam J. Aviv
A **data breach** leaks private, sensitive, or confidential personal information to unauthorized third-parties.

**Identity thieves raked in billions with your data, even as breaches fell in 2020**

On Data Privacy Day, here’s how raked in billions are long after your data is stolen.

---

**INDIGNITY: REDEFINING THE HARM CAUSED BY DATA BREACHES**

*George Ashenmacher*

What we have been examining is one facet of man’s struggle for a human dimension in a highly structured society, for dignity notwithstanding dependence.

*Science has vastly complicated this elemental contest.*

---

Image sources: CNET (left), heinonline (right)
Annual number of data breaches and exposed records in the United States from 2005 to 2020 (in millions)

Data source: Identity Theft Resource Center
Image source: Statista
How did you respond to the notification you received? (Ponemon Institute, 2014)

- Ignored it and did nothing: 32%
- Accepted the free identity theft protection service: 29%
- Contacted the organization for more info: 21%
- Followed the advice in the notification: 18%
Prior work asked about breaches in general or intended reactions in hypothetical scenarios.

We examined individuals’ reactions to real-world breaches that have exposed their personal data.

Ecologically valid responses  Mitigate potential recall bias
We built our own survey platform that could query the API of **Have I Been Pwned**.
Research Questions

RQ 1  Factors influencing the likelihood of exposure to data breaches?

RQ 2  Perceptions of causes and impacts when affected by data breaches?

RQ 3  Participants' awareness of data breaches?

RQ 4  Participants' emotional reactions to data breaches?

RQ 5  Participants' behavioral responses to data breaches?
We asked participants to provide their **most commonly used email address** for querying HIBP.

Note: we maintained email addresses in ephemeral memory to query HIBP; at no point did we access or track participants’ email addresses.
We asked participants to provide their *most commonly used email address* for querying HIBP.

For up to 3 breaches:
- Awareness
- Perception
- Emotional reaction
- Behavioral reaction
1. Email-related questions

We asked participants to provide their most commonly used email address for querying HIBP.

2. Breach-related questions

For up to 3 breaches:
- Awareness
- Perception
- Emotional reaction
- Behavioral reaction

3. Demographics and debrief

We showed a complete list of breaches and provided resources to help participants with the coping process.
What did we find?
Factors influencing the likelihood of exposure to data breaches?
Factors influencing the likelihood of exposure to data breaches

73% participants had one or more data breaches.

5.4 as the average number of breaches per participant.

189 unique breaches across all provided email addresses.

Leaked data types in our sample's breaches (n=189): Password (86%), Username (58%), IP address (43%), Name (39%), Date of birth (25%), Phys. address (16%), Gender (16%), Phone (15%), Geo location (13%), Site activity (11%).
RQ 1  **Factors influencing the likelihood of exposure to data breaches**

The number of breaches associated with an email address **increases 8% per year of use.**
Factors influencing the likelihood of exposure to data breaches?

Exposure to breaches was common. The longer the email was used, the more likely it was exposed.
Perceptions of causes and impacts when affected by data breaches?
Perceptions of **causes** and **impacts** when affected by data breaches

<table>
<thead>
<tr>
<th>Email practices (159; 53%)</th>
<th>Insecure behaviors (31; 10%)</th>
<th>External factors (42; 14%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>“It’s on the website of every business I have an online relationship with.”</td>
<td>“Because I was not careful with what emails I clicked.”</td>
<td>“These companies did not try hard enough to keep my info private.”</td>
</tr>
</tbody>
</table>

**Self-Blame**

**External Blame**
RQ 2  Perceptions of causes and impacts when affected by data breaches

More than half of responses assessed the breach’s impact as none (343; 43%) or very little (85; 11%).

Experienced impacts  “I receive phone calls constantly from scam artists...It has caused me to rarely ever answer my phone.”

Anticipated impacts  “Not at all, just scammers occasionally attempt to access some of my older accounts that hold no sensitive information.”
RQ 2

Perceptions of **causes** and **impacts** when affected by data breaches?

Most participants **blamed themselves** for being affected, and thought the breach **would not impact** them.
Participants' **awareness** of data breaches?
RQ 3  Participants' *awareness* of data breaches

“Prior to this study, were you aware that you are affected by this breach?”

(n=792)
RQ 3

Participants' **awareness** of data breaches?

Participants were **unaware** of most breaches displayed to them.
Participants' *emotional reactions* to data breaches?
Participants' **emotional reactions** to data breaches

Data types that received >50% “somewhat concerned” or above responses. The median concern level regarding a breach was **somewhat concerned**.
Participants' emotional reactions to data breaches?

Overall concern level remained low; more concern about exposed password, physical address, and phone number.
RQ 5

Participants’ **behavioral responses** to data breaches?
Participants’ behavioral responses to data breaches

Password triggered more concerns than other data types.

Possibly because most leaked data types were non-sensitive records.
**RQ 5**

Participants’ **behavioral responses** to data breaches

<table>
<thead>
<tr>
<th></th>
<th>Est.</th>
<th>OR</th>
<th>95% CI</th>
<th>p-value</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Intercept)</td>
<td>−3.27</td>
<td>0.04</td>
<td>[0.002,0.61]</td>
<td>.02</td>
</tr>
<tr>
<td>Awareness yes (vs. no)</td>
<td>5.97</td>
<td>390.48</td>
<td>[45.72,3334.79]</td>
<td>&lt; 0.001</td>
</tr>
<tr>
<td>Breach age years</td>
<td>−0.03</td>
<td>0.97</td>
<td>[0.77,1.21]</td>
<td>.77</td>
</tr>
<tr>
<td>Num. of types numeric</td>
<td>.12</td>
<td>1.13</td>
<td>[0.85,1.50]</td>
<td>.39</td>
</tr>
<tr>
<td>Password yes (vs. no)</td>
<td>−0.18</td>
<td>0.84</td>
<td>[0.18,3.79]</td>
<td>.82</td>
</tr>
<tr>
<td>Physical Addr. yes (vs. no)</td>
<td>−0.26</td>
<td>0.77</td>
<td>[0.16,3.71]</td>
<td>.75</td>
</tr>
<tr>
<td>Phone Num. yes (vs. no)</td>
<td>−0.29</td>
<td>0.75</td>
<td>[0.19,3.02]</td>
<td>.69</td>
</tr>
<tr>
<td>Date of birth yes (vs. no)</td>
<td>−0.24</td>
<td>0.79</td>
<td>[0.17,3.62]</td>
<td>.76</td>
</tr>
<tr>
<td>IP Addr. yes (vs. no)</td>
<td>−0.20</td>
<td>0.82</td>
<td>[0.26,2.64]</td>
<td>.74</td>
</tr>
<tr>
<td>Name yes (vs. no)</td>
<td>−0.19</td>
<td>0.83</td>
<td>[0.21,3.22]</td>
<td>.79</td>
</tr>
<tr>
<td>Concern numeric</td>
<td>0.80</td>
<td>2.22</td>
<td>[1.28,3.86]</td>
<td>.005</td>
</tr>
</tbody>
</table>

For a one-unit increase on a 5-point scale, the odds of having taken action increased by 2.2.

To react to a data breach, one need to be aware of the breach.

Logistic regression on having taken any of the ten provided actions (yes vs. no).
Participants’ behavioral responses to data breaches?

Changing passwords was more popular than other actions. Prior awareness and higher concern were key motivators.
Summary of Results

We surveyed (n=413) individuals’ **awareness, perception, and responses** to specific breaches that affected them.

- Exposure to breaches **increases** as an email address gets used for a longer time.

- Participants were **unaware of most breaches** displayed to them.

- Most participants **blamed themselves** for being affected, and thought the breach **would not impact** them.

- Participants’ overall concern level **remained low**, yet **awareness and concern** were key motivators of **taking action**.
What are the implications?
Tools to help consumers react to breaches

As an email gets used longer, the email address becomes more likely to appear in data breaches.

Promote tools that automate the creation of unique email aliases.

The image features “Sign in with Apple.” Source: MacRumors.
Tools to help consumers react to breaches

74% of shown breaches were new to participants.

Use in-situ methods to notify consumers of breaches.

Firefox Lockwise Password Manager. Source: Neowin LLC.
Increase responsibility of breached companies

Set stricter requirements for notifying affected consumers.

GDPR Art. 34:

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

Deliver notifications via multiple channels.

Make sure notifications are understandable and usable.

Mandate notifications for all breaches considering harms in legal terms.
Increase responsibility of breached companies

Require companies to be more involved in helping consumers **recover from breaches**.

**WHAT YOU CAN DO**

We are offering a complimentary one-year membership of Experian’s® IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides identity protection services focused on identification and resolution of identity theft. IdentityWorksSM Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorksSM Credit 3B, including instructions on how to activate the complimentary one-year membership, please see the additional information provided with this letter.

How about providing tools such as email alias generators or password managers?

Exposure to breaches **increases** as an email address gets used for a longer time.

Participants were **unaware of most breaches** displayed to them.

Most participants **blamed themselves** for being affected, and thought the breach **would not impact** them.

Participants’ overall concern level **remained low, yet awareness and concern** were key motivators of **taking action**.