Manuscript received December 1, 2020; initial decision January 8, 2021; revised March 3, 2021; accepted April 8, 2021. Date of current version: April 19, 2021.

(Corresponding author: *Zahra Hassenzadeh*.)

Z. Hassanzadeh is with Public Services and Procurement Canada, Ottawa, ON, K1A 0X1Canada (email: ZahraHassanzadeh@cmail.carleton.ca).

R. Biddle is with the School of Computer Science, Carleton University, Ottawa, ON K1S 5B6, Canada (email: Robert.Biddle@carleton.ca).

S. Marsen is with the Marshall School of Business, University of Southern California, Los Angeles, CA 90089 USA (email:).

Research Article

User Perception of Data Breaches

—ZARA HASSENZADEH ( ), ROBERT BIDDLE ( ), AND SKY MARSEN ( )

***Abstract*—Background:** *Data breaches happen when an unauthorized party gains access to personally identifiable information. They are becoming more common and impactful, raising serious concerns for individuals as well as companies.* **Literature Review:** *Although there is considerable literature on users' mental models in security and privacy, there has been limited study of mental models related to data breaches.* **Research Questions:** *1. How do users understand data breaches? 2. What are their perceptions of the causes, responsibilities, consequences, as well as possible prevention and appropriate follow up?* **Methodology:** *We explored end-user understanding of internet data breaches by conducting a study with 35*

participants. They were asked to draw their understanding of data breaches and answer some open-ended and closed-ended questions afterwards. **Results/Discussion:** *Although their drawings varied in detail and complexity, we identified four patterns in the participants' drawings: they illustrated abstractions of attacks to gain administrator access, end-user access, backdoor access, or access using database server vulnerabilities. We found that participants had a basic model of how an internet data breach happens, but with significant uncertainties regarding system vulnerabilities, causes, consequences, prevention methods, and follow-up steps after a breach.* **Conclusions:** *In all, end-user mental models of internet data breaches are basic and show gaps that emphasize the need for improved communication to increase users' awareness and help them hold companies accountable.*

Index Terms—*Cybersecurity, internet data breaches, mental models.*

Data breach incidents are becoming more common and have aroused broad concern. According to the *Risk Based Security* report, a global database of public data breaches, over 8 billion records were exposed in the first quarter of 2020 [1]. A data breach is an incident in which cybercriminals attack a system, infiltrate a data source, and extract personally identifiable information that can be helpful to distinguish an individual's identity [2]. All computer attacks do not necessarily lead to a data breach. However, attackers may probe to find system vulnerabilities and compromises that allow them to get access to companies' servers and expose their data. Attackers can also use targeted malware attacks to gain access to a target system.

Intrusion detection systems (IDS) are deployed to defend companies from the breaches and attacks that arise on a daily basis. Intrusion detection systems monitor a network or system for malicious activity. Generally, they will notify administrators of a possible intrusion or collect the

malicious activity centrally using security information and an event management system. However, IDS are not completely effective.

Researchers in cybersecurity emphasize the role of security mechanisms such as firewalls, authentication mechanisms, virtual private networks (VPNs), and security technology such as intrusion detection systems, which are complementary to security mechanisms [3]. Despite increased awareness and improvement of security mechanisms, companies still practice insufficient cybersecurity measures, which cause breaches such as the breaches of Equifax in 2017 [4], Marriott International in 2014-2018, LinkedIn in 2012 and 2016, Yahoo in 2013-2014, and many more [5].

Despite the increase in cyberbreaches, there has been surprisingly little engagement from the public, and many people continue using services after breaches. Some suggest that notable data breaches do not change customers' behavior, attributing it "breach fatigue" [6]. Users' understanding of how things work is important in making security decisions because it pinpoints the mental models that shape the way that they see the breach [7]-[9]. Therefore, finding the gaps in the users' mental models would indicate how communication can be designed to help users reach reasonable security expectations for companies to keep their data safe.

Considerable literature in computer security and privacy addresses mental models; however, research on mental models related to data breaches is rare. The goal of our research was to address this gap by exploring user misunderstanding of internet data breaches that endangers the user's personally identifiable information. Our objective was to investigate some problematic beliefs about data breaches in users' mental models to trace patterns that could be used to inform the design of relevant communication materials produced by organizations and regulatory

authorities. As well as contributing generally to research on the mental models of users related to data breaches, this project aimed specifically to pinpoint certain user misconceptions about data breaches that risk and crisis communicators in organizational, regulatory, and instructional contexts should consider.

To this end, we conducted a study in which we asked users to describe and illustrate their understanding of how a data breach happens. We collected data about participants' perceptions of internet data breaches; their perceptions of the causes, motivations, and consequences of those breaches; as well as their attitudes towards preventing a data breach. This study complements our earlier research on image-repair strategies following a data breach [10], which focused on the public communication of organizations and media responses after a data breach. That study explored the ways that organizations attempt to influence and direct users' and more generally the public's perception of the breach so as to reduce organizational accountability.

LITERATURE REVIEW

Mental models are explanatory representations that humans develop when interacting with environments, with others, and with technology. Mental models are employed by discourse analysts, psychologists and sociologists to identify people's problem-solving techniques based on the way they perceive the problem and the context in which it arises [7], [11]. A mental model approach has been employed in crisis communication research to study the public's reactions to crisis events and open the way for the design of more effective communication practices. For example, Morgan et al. [12] explain the importance of communicating risk based on the public's existing beliefs and assumptions and not on what "experts" think that they should know.

Regarding data breaches, most users' decisions are shaped by their mental models [13], which act like filters affecting the way they see and interpret the world [7]-[9]. Because mental models show established ways of interaction with a system, they can be useful in designing protocols for communicating security-related concepts and processes to nonspecialist users.

Jean Camp [14] presented five possible mental models for security failures by using metaphors: physical security, medical infection, criminal behavior, economic failure, and warfare. Each of these models implies a different solution, and therefore, when communicating with users, computer security experts should consider which model will meet user expectations.

- Physical security models are somewhat understood; for instance, the metaphor of a wall might help to understand a network security practice. This metaphor encourages users to secure their computers.

- The public health model reminds users to protect themselves and draws on the need for shared responsibility for community health.

- In the criminal behavior model, malicious behavior is a crime and can result in victims suffering a significant loss. So law enforcement is a logical response, and increased surveillance is a prominent part of the solution to the computer crime problem.

- The warfare model evokes the existence of a determined enemy and the critical need for response and reminds the users that individual actions are crucial for collective security.

- Computer security failures can also result in economic failure as they are costly to an organization. So this model would justify convincing users that they have valuable assets and that thieves might target them.

Researchers use different methods to identify mental models, including problem solving, verbal reports, drawing, categorization, and conceptual pattern representation. In the problem solving method, people use their mental models to understand a problem and make inferences and predictions [15], so those with different mental models will understand a problem differently and will come up with different solutions. A verbal report is a direct method of eliciting mental models and can encompass interviews, explanations, or think-aloud protocols [16]. In think-aloud protocols, participants are asked to verbalize their thoughts while performing a task. Think-aloud is useful for analyzing mental models because it provides direct information about the participants' thinking process. Drawing is frequently used in conjunction with verbal reports [17] in user-centered research, and has also been found to assist in elicitation of mental models [18]. The categorization method shows how mental models are developed and categorized, and has usually been used to show the similarities and differences between experts and novices [19]. Finally, conceptual patterns represent the concepts and their relationships [20], [21].

Because mental models are often represented pictorially and using verbal reports has some limitations [17], drawings have been used as complementary methods in several mental model research studies. For example, Raja et al. [22] conducted a study of participants' mental models of the Vista Firewall using a diagramming task. They gave participants a picture of a computer, a firewall, and the internet cloud and asked them to show how the Vista Firewall works by drawing arrows. Subsequently, they designed a new interface with contextual information to improve participants' mental models of the firewall.

Wash [8] used multiple rounds of interviews to understand users' mental models of security threats. He identified eight folk models of malware and attackers. Users employed these models to decide which security software to use and which advice to follow. Wu and Zappala [23]

conducted a series of semi-structured phone interviews using interview techniques and diagramming exercises to capture users' perception of the encryption process. They found four mental models that are different in detail and complexity. They also found that users do not fully understand the decisive role of encryption.

Clearly, understanding user mental models can lead to better communication regarding privacy and security risks [24]. Evidence suggests that deficient mental models of data breaches influence behavior, and people tend to underestimate the consequences and risks of a data breach. Ideally, users need to be able to answer these questions:

- What is a data breach?
- How do data breaches happen?
- What are the consequences of a data breach?
- How can individuals and companies prevent data breaches?
- What are a company's responsibilities regarding securing personal data?
- What can users do after a data breach?

RESEARCH QUESTIONS

The following research questions guided our study.

RQ1. How do users understand data breaches?

RQ2. What are their perceptions of the causes, responsibilities, consequences, as well as possible prevention and appropriate follow up?

The objective of these questions is to form a framework that will inform communication practices and interventions by organizations and other relevant parties aimed at dispelling misconceptions and empowering users when they make security decisions.

METHODOLOGY

The data presented in this article is derived from 35 one-on-one, in-person sessions with participants about their mental models of internet data breaches. Each session lasted 40 to 90 minutes. Participants were compensated with a small monetary payment. Our study was reviewed and cleared by a university Research Ethics Board.

We collected data from a drawing task, as well as open-ended and closed-ended questions administered through LimeSurvey (an open source survey system, hosted on a secure server). We audio-recorded the participants' voice while they were verbally explaining their understanding of internet data breaches. These recordings were transcribed using Otter.ai (https://otter.ai), and the transcriptions were reviewed during our analysis.

Participants Participants were recruited using recruitment posters, and a Facebook page for user study recruitment; known contacts were also emailed. We recruited a total of 35 participants: 18 female and 17 male. They ranged from 18 to 54 years (see Table I). When asked specifically if they have ever experienced any data security problem, 11 said yes, 18 said no, and the remaining six said that they were uncertain. When asked whether they had ever experienced identity theft, 27 said no, five said yes, and the remaining three said that they were uncertain. Of the 35 participants, 34 agreed to be audio-recorded, and one participant did not, so we took notes during that session.

Sessions The sessions took place in a research lab or an off-site location. Participants read and signed a consent form after we explained the tasks. They first completed a basic demographic, and a SeBIS (Security Behavior Intentions Scale) questionnaire [25]. Then participants were asked to draw their understanding of how a data breach happens in response to the following prompt.

> Using a paper and pencil, please draw your understanding of how a data breach happens. In other words, try to draw what is happening when it is said that an attacker has hacked a company's database servers and personal information about you *and many other people has been breached.* (Elements you may need for this drawing: Admin, Data, Customer, Hacker, Access to data, Vulnerability).

We made a change after the first 15 participants' sessions to emphasize the breadth of the attack (see italics) but did not observe any changes in participant responses.

After the drawing task, participants answered open-ended questions and Likert-type questions on a 7-point scale regarding causes, consequences, motivations, and prevention methods of a data breach. After reviewing the result of the Likert-type questions of the early round of study, we speculated that participants answered some questions simply agreeing with anything related to security because we were interested in that topic. So in the second round of study, we added more plausible but inappropriate items as well as clearly wrong answers to check and ensure the validity of their responses.

Data Analysis We addressed participant responses in two sections: qualitative data, and quantitative data stemming from Likert-scale responses. We analyzed the results of the SeBIS questionnaires by aggregating the score of positive questions minus the score of negative ones.

Each question was scored 1-5, where 1 stands for “Never,” 3 for “Sometimes,” and 5 for “Always.” The other closed answers were analyzed by computing the median for the central tendency of our data, as well as analyzing and reviewing graphical representations.

The high-level codes for open questions were associated with our research questions and were focused on the following.

- What is considered a data breach?
- What are the causes of an internet data breach?
- What reasons are given for an internet data breach?
- How do you know whether a user has been affected in an internet data breach?
- What are the consequences and prevention methods?
- Who is responsible for data protection?

These themes are top-level categories, and we created several subcategories based on participants’ responses.

We then conducted a thematic analysis [26] of participants’ think-aloud comments during their drawing task, discussion of their drawings, and responses to open-ended questions. We started by examining the diagrams closely to understand the data as a group. We were looking for key elements, trends, themes, or ideas in the images. We generated a set of codes by comparing the similarities and differences between the participants’ drawings. The codes are representative of the identified themes and are linked to drawings as summary markers [27], [28]. We built an

initial summary of these codes and identified patterns in the ways participants talked about data breaches and their word choices, looking for cases where they had different perceptions. We used the transcriptions as a complementary source for the drawing task to better understand the drawings.

RESULTS

SeBIS Question Results Fig. 1 shows a summary of the results of the SeBIS questionnaire, illustrating the computer security behaviors of participants. Notably, most reported risky behavior regarding password generation: they only sometimes used different passwords for different accounts (37%), they only sometimes used a password that exceeded the site's minimum requirements (37%), and they often did not include special characters in their passwords when not required (51%).

When asked about proactive awareness, they reported risky behavior like sometimes opening a link without first looking to see where it went. They sometimes submitted information to websites without first verifying that it would be sent securely, and if they discovered a security problem, they often (74%) continued what they were doing because they assumed someone else would fix the problem. They reported risky behavior regarding updating software and anti-virus programs (57%). The histogram in Fig. 2 shows their different levels of aggregate security behavior. The possible range of participant scores was between 0 and 80, and the plot illustrates a reasonable distribution, showing that the participants were neither security "advocates" nor security "slackers."

Questionnaire Results At the end of each session, participants were asked to answer another questionnaire consisting of some open-ended questions and a series of 7-point Likert-scale questions that were grouped to represent the following categories:

1. Definition of a data breach and responsibility for data protection
2. Causes of data breaches
3. Consequences of a data breach
4. Motivation for data breaches
5. Prevention methods
6. Actions after a breach

1. Definition of a data breach and responsibility for data protection. In response to being asked what a data breach is, all participants had a general understanding of how an unauthorized party gets access to the secure or private/confidential information. For example, P11 defined a data breach as "… when information is kept privately on the internet and is then accessed by someone who is not supposed to have access to the information."

In response to being asked whether they had ever heard of an internet data breach, 25 participants said yes, three said no, and seven said they were not sure. In response to how they had heard of data breach incidents, they mentioned news media, breach notifications and word of mouth. When asked how they would know whether they had been affected in an internet data breach, participants showed a reasonable understanding of how users become aware of breaches (see Table II).

When asked who is responsible for data protection, 28 participants considered the users responsible for protecting data. When asked the same question in a closed-ended format, 60% of participants believed that government and customers of a company are responsible for data protection. For this and some other questions, early results suggested guessing, so we offered several options with seemingly plausible but inappropriate answers. As a result, more than 40% of participants said that they either believed or were uncertain whether the American National Standard Institute, G7, GAAT, or OECD were responsible. (The G7 is the Group of 7 major advanced nations; GAAT is the General Agreement on Tariffs and Trade; OECD is the Organization for Economic Cooperation and Development.) These answers suggest that a considerable number of participants were not aware of accountability of people whose data had been exposed in a breach (see Fig. 3). It seems clear that many users either have distorted perceptions of accountability or are unsure what to factor into their attributions of blame in data breach episodes.

In our previous study [10] where we analyzed the nature of a company's communication with consumers regarding data breaches, we found the company's approach appeared to deflect responsibility by shifting the blame and using compensation strategies that introduce the company as the users' helper to reduce the reputation and financial damage of their data breaches. This finding may influence user understanding of accountability, which indicates the need for a more systematic approach in communicating information on data security to the public.

2. Causes of data breaches. We asked questions about causes in both an open-ended and a Likert-scale format. Participants generally mentioned the following items in their open-ended answers: negligence, poor passwords, poor security measures, hackers, and vulnerability.

Notably, participants employed the word *vulnerability* in its everyday meaning of "human weakness" rather than its technical use of "system weakness." Other potential causes of data breaches can be seen in Table III. As can be seen in Fig. 4, although the rating seems reasonable for the appropriate answers, more than 40% of our participants were uncertain or rated the inappropriate answers high, indicating that they did not know the causes of data breaches.

3. Consequences of a data breach. When asked what can happen as a consequence of an internet data breach, participants mentioned, in order of importance, financial loss as the main consequence, identity theft, invasion of privacy, fraud, loss of trust, national threat, political consequences, and cyberwar.

Fig. 5 shows the results from Likert-type questions. Participants rated highly or were uncertain about some inappropriate responses such as data-harvesting programs, browser hijacking, pop-up advertisements, and personal safety. This finding suggests that many nonspecialist users are unfamiliar with the actual consequences of data breaches. Although 47% correctly identified the inappropriate consequences, about 50% still showed no knowledge. This result suggests that if users do not know how stolen information is used, they may not consider the consequences of data breaches as serious.

4. Motivation for data breaches. In response to being asked the motivation for an internet data breach, participants mentioned common reasons. Only a few participants had a broader perspective of the factors that can motivate an attacker and mentioned having fun, damaging corporation reputations, spying, proving a weakness in a system, and displaying technical skills.

Participant responses to the Likert-scale questions (Fig. 6), also suggest that they are familiar with common motivations for data breaches. Surprisingly, however, more than 50% agreed or

were uncertain that a data breach can happen to secure electronic data, to stay on top of advancement in security technologies, or to check a company's security measures. These responses suggest an unclear understanding of reasons for data breaches.

5. Prevention methods. When asked what companies should do to protect their data from breaches, participants suggested investing in security measures, educating users and employees, restricting data access and regularly monitoring networks, and encrypting data. Hiring reliable employees and not collecting all data were also considered by one participant as suitable prevention methods. For Likert-scale questions (see Fig. 7), responses were mostly reasonable; however, some responses suggested that participants were simply guessing. For instance, these responses mostly agreed that standardized protocols, high-performance networking, and genetic algorithms can prevent a data breach (all of which show mistaken perceptions). Again, these findings indicate the need for clearer communication in educating users about security.

6. Actions after a breach. In response to being asked what they can do if their personal data has been breached, a few participants talked about freezing their accounts, and only one was aware of an "identity theft protection service." Our results for Likert-scale questions (Fig. 8) show that many users are only partially aware of appropriate after-breach procedures.

Drawing Task Results Our goal in this part of the study was to explore the users' perceptions of how a data breach happens. Morgan et al. [12] discuss the importance of eliciting how elements of mental models *influence* other elements—for example, where some events are causally related to other events or outcomes. We asked them to sketch their understanding of the process, and to get them started, we suggested the following potential elements: Admin, Data,

Customer, Hacker, Access to data, and Vulnerability, and asked them to describe what these elements' roles are in a data breach.

We then conducted a thematic analysis, reviewing the results for each participant and identifying the mechanisms shown that suggested their mental model of the data breach process. Two researchers separately reviewed the diagrams and then discussed their findings to reach agreement on the main themes. The codes identified related the roles involved (e.g., user, administrator, and attacker), the information, location of the attack (e.g., user computer, server, database), and the means by which access was gained (e.g., passwords, special knowledge, vulnerabilities). In some cases, the causal sequence of events depicted needed discussion (e.g., how surveillance found passwords or vulnerabilities). Overall, we identified three major mechanisms in the participants' drawings:

1. That the attacker gains admin access.
2. That the attacker gains user access.
3. That the attacker gains backdoor access.

We also found one more mechanism (database server vulnerability) illustrated by only two participants. The sections below describe these patterns in more detail.

Admin access. Participants depicted their understanding of how an attacker can gain access to the data as attacking the admin system directly and gaining admin level access to the data. In this mechanism, user data are stored on a server that can be unlocked only by an administrator. These participants also believed that accessing the admin system would happen either by a capture attack on the admin password or by guessing the admin's password. A capture attack is the

action of obtaining information such as passwords and other confidential data. It can be accomplished by keyloggers, malicious software or hardware that records keystrokes at a low level, and therefore records any usernames, passwords, or other credentials entered by typing. Participants were not sure about the level of admin access and one mentioned that the admin may have access only to users' identity verification data, so an attacker who targets the admin account will access that data and will then be able to access the server as a normal user (see Fig. 9a).

User access. This group of participants was focused on *when* attackers try to hack an individual's data. They also believed that it could happen by password guessing or password capturing attack. Attackers may attempt to take screen captures of a user's personal computer to gather information over the course of an operation or input capture to steal a user's credit card information while they are shopping online on an apparently legitimate but really fraudulent website (see Fig. 9b).

Backdoor access. In a few cases, participants' drawings of a data breach illustrated an existing backdoor that could be used by attackers. In this case, an attacker sees a protected sign in the frontend that gives access to secured data with the appropriate "key" (customer and admin). Then the attacker looks for the backdoor and "tries the knob." The backdoor can appear as a result of malware or by an intentional manufacturing decision. However, one participant tried to show that attackers can gain access to the backdoor by brute force attack, checking all possible passwords until the correct one is found. The brute force attack is indeed one actual kind of attack, though other actual kinds of attack include exploiting backdoors that are put in place on purpose by manufacturers or cybercriminals to allow access into a system (see Fig. 10a).

Database server vulnerability. In the second round of the study, after changing the drawing prompt, two participants drew an attacker gaining access to the system through database server vulnerabilities. However, they did not show any illustration of the vulnerabilities in their drawings. P27 said that attackers can use different methods to breach customers' data by accessing data through getting administrator credentials, compromising individuals' data by deceiving users to disclose their information (e.g., using phishing attacks), and using database or server vulnerabilities (see Fig. 10b).

Based on the participants' drawings, it is not clear whether users understand what a vulnerability in a system is. Three participants (P2, P10, and P28) drew the vulnerability as an open door, and three as a broken wall (P15, P30, and P34), and the others did not include it in their drawings. Only one participant (P13) added more details about the steps of the attack where the attacker scans the system for confidential information. The drawings of two participants (P8 and P17) had labels about the consequences of a data breach, like loss of resources and invasion of privacy.

The main finding of our picture analysis (in the early round) was that most participants believe that attackers are interested in personal data that they have stored on their devices or shared unintentionally with an unauthorized party. For example, P8 said, "A data breach happens when a stranger gets access to my private pages such as Instagram and … finds my username and password then uploads pictures and information instead of me." P20 said that "A data breach happens when a third party is monitoring your conversations with a server and recording your data without your authorization."

Using elements like customer and data admin did not change their model of how their personal data are disclosed. Even in the second round of study, after we changed the wording of our

drawing task prompt to explicitly state the mass consequences of data breaches, some participants still believed that attackers are interested in accessing individual users' credentials.

DISCUSSION

The extracted themes from participants' drawings and other remarks they made suggest how a data breach is represented in their mental models. We now summarize our key insights and discuss their implications for communicating security procedures to users.

Drawing and Open Questions Analysis

Target of attack. We found that most participants believed that attackers attempt to access their personal information through their social media accounts, emails, or data stored on their personal devices like mobile phones or tablets. During the drawing task, some people illustrated data on their devices and ignored data stored on organizational databases.

Due to this perception of data storage, they believed that because users are entering their data, *they* are the principal people responsible, when it is not true. For example, when asked about data protection responsibility, P8 said, "The most responsible person is us; then it goes to companies we share our information with."

After changing the wording of our drawing task, they were still uncertain about the attack's target. Most participants still believed that attackers are interested in users (vulnerable users), while fewer included the system admin, and even fewer identified the vulnerability of the system itself as a potential target. This may be the reason why many people continue using breached services.

Uncertainty. Participants expressed much uncertainty about how an attacker gains access to data, and their answers were mostly focused on either guessing passwords or capturing the users' credentials while they are using an illegitimate website, especially for online shopping. Another area of uncertainty in people's knowledge was whether protective actions, like encryption, are strong enough to prevent data breaches. We did not ask directly about the strength of encryption algorithms; however, a few participants talked about encryption as a preventive method. Moreover, although they agreed in Likert-scale responses that encryption is a preventive method, they noted that some of the breached companies had used data encryption that had proven to be ineffective. Our findings are consistent with what Wu at al. [23] found regarding the participants' confusion about encryption strength. This result shows the need to communicate to users the significance of encryption's protective capabilities so that they may demand that companies encrypt their data using strong encryption algorithms.

Participants know the term *vulnerability*, but they typically think that it relates to themselves. They used *vulnerability* in the sense that users are more vulnerable to attack because of lack of security knowledge or lack of malware protection. Participants said, "The hacker targets vulnerable users more easily," and "when there is no protection against malware and/or hackers, then the data would be left vulnerable and could potentially be accessed by the attacker." Moreover, only six participants illustrated *vulnerability* as a broken wall or open door in their drawings. This finding highlights clearly the need to define terms to users rather than assuming understanding, especially with terms that have multiple meanings.

Some participants mentioned that users need to know more about the type of data stored on companies' databases and the ways that these data are protected. This finding underscores the need for information flows to be more transparent, for example by making GDPR compliance

clear [29] by stating specifically the purpose of data collection, time period of data storage, permission to access data, and automated decision-making like profiling. This goal can be achieved by improving software design to support users' ability to track access to their data and perhaps giving a user warning when someone accesses their personal data.

Our findings also demonstrate participants' inadequate knowledge of what to do when their data are breached. They did not mention any protection mechanism against the negative impact of data breaches, and it is not clear whether they know that these mechanisms exist. They mentioned changing passwords, deleting accounts, or reporting the incident after-breach.

> Call the police or email/report this incident to the company/Admin or any regulatory body such as investigators.
>
> Talk to police, bank, ISP, depending on the extent.
>
> Change my passwords, delete accounts, and create new ones with a different email.

This finding underscores the need for clear communication on what actions are required after a breach and what can go wrong if these actions are not taken. The study identified a need for information on how to reduce risk of a data breach, for example by placing a credit freeze, and how to respond to a breach depending on the type of information that was compromised (e.g., type of identity protection services that they need to use).

Questionnaire Analysis The results of the questionnaire show that users were exhibiting safe security behavior in securing their devices, but the scores are lower in updating, proactive awareness, and password choice. Participants correctly identified users' and employees' negligence, weak passwords, and inadequate security measures as causes of a data breach. They

understood that financial loss, identity theft, and invasion of privacy are negative impacts of a data breach. A variety of motivations for the attack were mentioned in open-ended questions—for example, attackers displaying their technical skills and political motivations.

Participants tended to rate legislation as less likely to prevent a data breach, and they incorrectly identified answers that we offered such as high-performance networking, and genetic algorithms as prevention methods. This response might be a result of their unfamiliarity with new laws that can force companies to invest more in their security measures but could also underscore the common belief that attackers are competent enough to find a way to penetrate a system. This finding shows an opportunity to communicate to users that many massive data breaches could have been prevented by simple security practices like updating certificates and patching software promptly [4].

Limitations Our work has certain limitations. First, our sample cannot support conclusions about the general population because it is skewed to younger people with higher level of education, and it is possible that this fact influenced our findings.

Second, although we explored participants' mental models about data breaches, we did not explore the reasons for these mental models. Our earlier study [10] did establish a link between messaging and understanding of issues of responsibility for data breaches, and this topic deserves further exploration.

CONCLUSION

Users conceptualize security threats, and they create mental models based on their individual experiences. These models shape their behavior and guide their security-related decisions. In this

article, we have presented our findings drawn from 35 sessions with participants about their perceptions of data breaches.

Results from the questionnaire and the drawing tasks suggested that users have a reasonable basic model of how data breaches happen. Participants showed limited detail in their drawings, and they also illustrated that they are not aware of potential causes of a breach like vulnerabilities in a system that can be prevented remedied.

An important finding in our early round was user perception of the responsibility for data protection. Under the European Union's General Data Protection Regulation regulations, Canada's Protection of Personal Information and Electronic Documents Act, and US Federal Trade Commission restrictions, it is businesses' responsibility to keep personal data safe and protected against unauthorized access. However, many participants attributed blame to their own actions and continued to utilize the services of breached companies.

We also found that users' mental models of data access coincided with the category of network attacks against confidentiality [30]. Users understood that an attacker can capture their credentials using screen capturing or input capturing. Participants had a flawed model of what a vulnerability is, and they referred to the user who can be vulnerable due to lack of awareness and knowledge; only a few of them had an understanding of vulnerability in a system and only two participants illustrated database servers' vulnerability as a target of attack. Participant responses for necessary after-breach actions made it evident that they were concerned about checking their bank transactions and changing their passwords. Although identity crime (for example, identity theft, scam, fraud) is one of the most important potential consequences of a data breach, our participants did not seem to know any way to monitor or stop it [2].

In all, the results of this study indicate that many users are not aware of effective actions to prevent data breaches or of actions to manage them when they do occur. As our discussion showed, this is a communication problem, as no systematic or organized effort seems to exist for instructing users on the pertinent factors in data breach crises based on their existing knowledge and mental models. This gap in user understanding is not only costly to the public but also enables organizations to deflect responsibility from their actions and evade public scrutiny through strategies that have been developed to help them to do so. This study proposes and illustrates a mental models approach for obtaining data from users to design targeted communication protocols that will increase awareness of cybersecurity issues. It is intended as a foundation for further research into user perceptions of data breaches, employing different samples and scenarios, to better identify areas of confusion, which would confirm where focused communication design is required.

REFERENCES

[1] Risk Based Security, "2020 q1 report data breach quick view," [Online]. Available: https://pages.riskbasedsecurity.com/en/2020-q1-data-breach-quickview-report. [Accessed 18 07 2020].

[2] Identity Theft Resource Center, "Identity Theft Resource Center," 2019. [Online]. Available: https://www.idtheftcenter.org/data-breaches/.

[3] A. Lazarevic, J. Kumar and V. Srivatava, “Intrusion Detection: A Survey,” Boston, MA, Springer US, 2005, pp. 19-78.

[4] GAO-18-559, “Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach GAO-18-559,” 2018.

[5] D. Swinhoe, “The 15 biggest data breaches of the 21st century,” 8 January 2021. [Online]. Available: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

[6] C. Mele, “Data breaches keep hapening. So why don't youdo something?,” [Online]. Available: https://www.nytimes.com/2018/08/01/technology/data-breaches.html.

[7] C. Bravo-Lillo, L. F. Cranor, J. Downs and S. Komanduri, “Bridging the gap in computer security warnings: A mental model approach,” *IEEE Security and Privacy,* vol. 9, no. 2, pp. 18-26, 2011.

[8] R. Wash, “Folk Models of Home Computer Security,” in *Proceedings of the Sixth Symposium on Usable Privacy and Security*, New York, NY, USA, 2010.

[9] R. Wash and E. Rader, “Influencing mental models of security: A research agenda,” in *Proceedings of the 2011 New Security Paradigms Workshop*, New York, NY, USA, 2011.

[10] Z. Hassanzadeh, S. Marsen and R. Biddle, “We’re here to help: Crisis communication and user perception of data breaches,” in *Graphic Interface 2020*, Toronto, CA, 2020.

[11] T. Van Djik, "Cognitive Context Models and Discourse," in *M. I. Stamenov (ED.) Language Structure*, Amesterdam, 1997.

[12] M. Granger Morgan, B. Fischhoff, A. Bostrom and C. J. Atman, Risk Communication: A Mental Models Approach, Cambridge: Cambridge University Press, 2001.

[13] P. N. Johnson-Laird, Mental models: Towards a cognitive science of language, inference, and consciousness, Cambridge University Press, 1990.

[14] L. J. Camp, "Mental Models of Privacy and Security," in *IEEE Technology and Society Magazine 28*, 2009.

[15] P. N. Johnson-Laird, "Mental Models and Human Reasoning," *Proceedings of the National Academy of Sciences 107,* vol. 43, no. 18243-50, 2010.

[16] M. T. H. Chi, "Laboratory Methods for Assessing Experts' and Novices' Knowledge," in *The Cambridge Handbook of Expertise and Expert Performance*, Cambridge, Cambridge University Press, 2006, pp. 167-84.

[17] D. Jonassen and Y. H. Cho, "Externalizing Mental Models with Mindtools," in *Understanding Models for Learning and Instruction*, Boston, MA: Springer US, 2008, pp. 145-59.

[18] N. A. Jones, H. Ross, T. Lynam, P. Perez and A. Leitch, "Mental models: an interdisciplinary synthesis of theory and methods," *Ecology and Society,* vol. 16, no. 1, 2011.

[19] M. T. H. Chi, P. J. Feltovich and R. Glaser, “Categorization and Representation of Physics Problems by Experts and Novices,” *Cognitive Science ,* vol. 5, no. 2, pp. 121-52, 1981.

[20] D. H. Jonassen, Computers as Mindtools for Schools: Engaging Critical Thinking, Merrill, 2000.

[21] D. H. Jonassen, “On the Role of Concepts in Learning and Instructional Design,” *Educational Technology Research and Development ,* vol. 2, no. 54, p. 177, 2006.

[22] F. Raja, K. Hawkey and K. Beznosov, “Revealing Hidden Context: Improving Mental Models of Personal Firewall Users,” in *Proceedings of the 5th Symposium on Usable Privacy and Security*, New York, 2009.

[23] J. Wu and D. Zappala, “When Is a Tree Really a Truck? Exploring Mental Models of Encryption,” in *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, Baltimore, 2018.

[24] F. Asgharpour, D. Liu and L. J. Camp, “Mental Models of Security Risks,” in *Financial Cryptography and Data Security*, Berlin, 2007.

[25] S. Egelman and E. Peer, “Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS),” in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, New York, 20015.

[26] G. Guest, K. M. MacQueen and E. E. Namey, “Introduction to Applied Thematic Analysis,” in *Applied Thematic Analysis*, 2012.

[27] J. Check and R. K. Schutt, “Qualitative Data Analysis,” in *Research Methods in Education*, 2012.

[28] U. Flick, “The SAGE Handbook of Qualitative Data Analysis,” in *Research Methods in Education*, 2014.

[29] R. Koch, “Everything you need to know about GDPR compliance,” 2018. [Online]. Available: https://gdpr.eu/compliance/.

[30] I. Sumra, H. Bin Hasbullah and J. L. Ab Manan, “Attacks on Security Goals (confidentiality, Integrity, Availability) in VANET: A Survey,” in *Advances in Intelligent Systems and Computing*, 2014.

Zara Hassanzadeh is

Robert Biddle is

Sky Marsen is

Practitioner Takeaway

- Among the five readability tools tested, scores that should have been the same typically varied by two grade levels.
- Differences resulted from how compound and hyphenated words, numbers, abbreviations and acronyms, URLs, and other punctuation and text elements were counted, because the tools often did not specify how to score them.
- Microsoft Word 2013 for Windows is recommended if the Flesch-Kincaid Grade Level is required.

Note: This table (without a table number or call-out in the text) always appears across both columns at the top of page 2 of the article.

TABLE I
PARTICIPANTS' DEMOGRAPHICS (TOTAL= 35)

Age	**%**	**Education**	**%**	**Field of study**	**%**
18-30	74%	Less than High school	0%	Formal science (Computer Science, Logic, Math)	17%
31-40	20%	High school degree or equivalent	18%	Natural science (Biology, Physics, Chemistry…)	11%
41-50	3%	College/Bachelor's degree	51%	Social science	29%
51-60	3%	Trade or technical degree	3%	Engineering	14%
Over 60	0%	Graduate degree	28%	Arts	17%
				Law	6%
				Other	6%

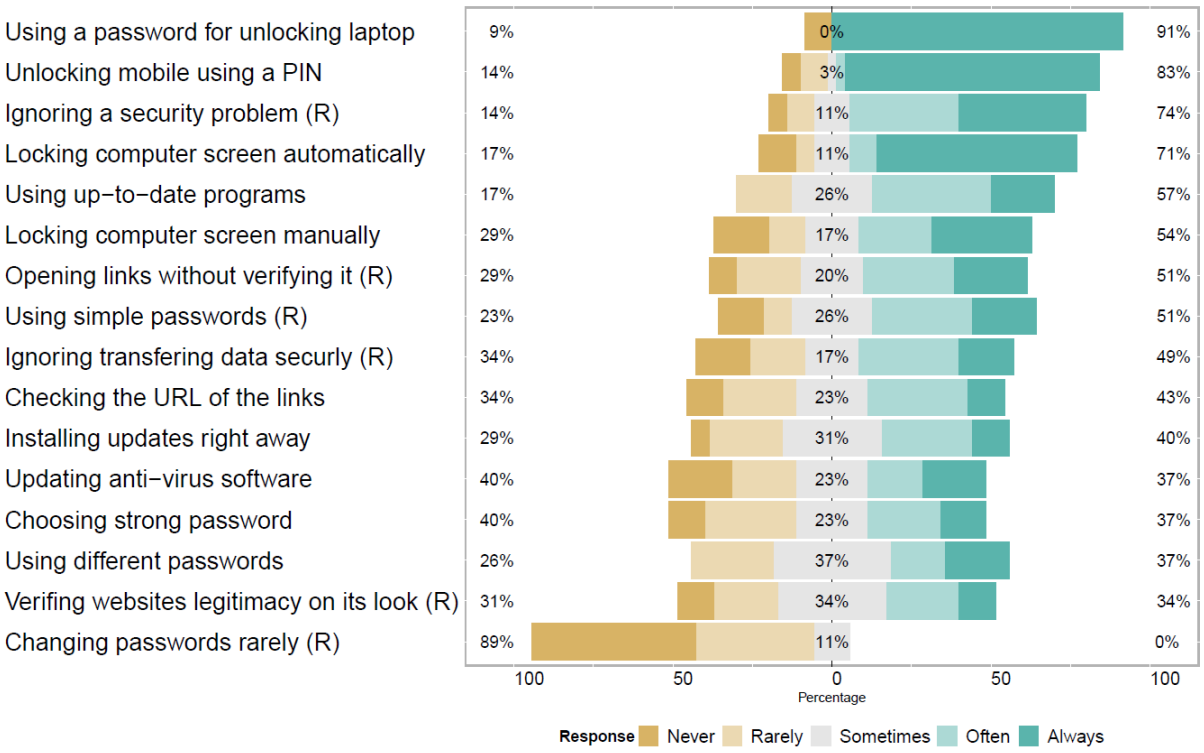


Fig 1. Security Behavior Intentions Scales (SeBIS) results. Statements marked (R) were reverse scored.

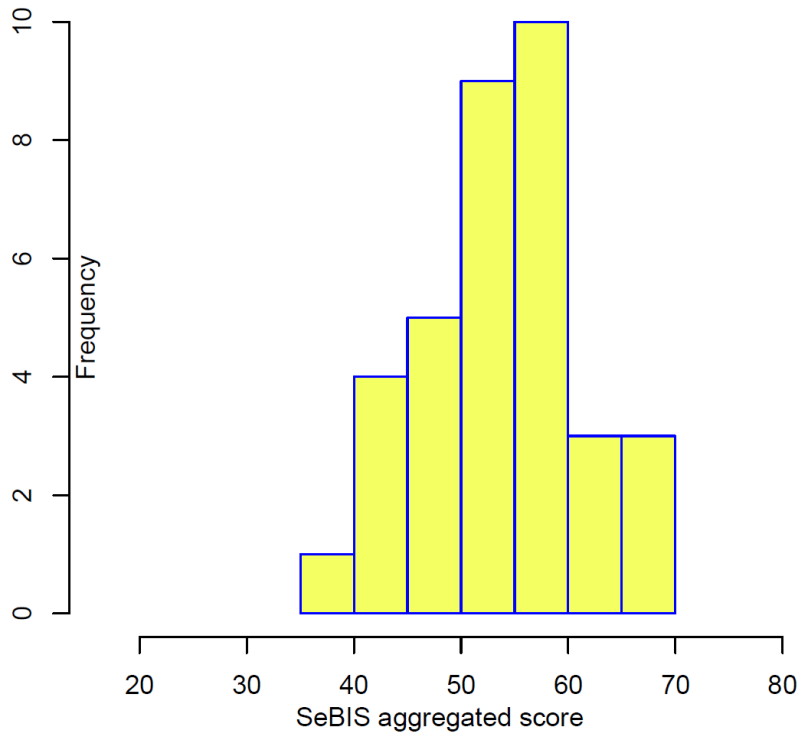


Fig 2. SeBIS histogram; maximum score is 80 and minimum is 16.

TABLE II

HOW WOULD YOU KNOW IF YOU HAVE BEEN AFFECTED IN AN INTERNET DATA BREACH?

Code	Total	Sample of Data Extracted
Company's notifications	13	"I would hopefully be contacted by the company who lost my information and be told what was taken."—P2
Alerts to my accounts	9	"When you are notified about your activities (transactions, logging in, etc.) on internet through SMS or email notification."—P19
Checking my bank transactions	9	"This can be seen in many ways, such as a sudden change in your bank statement that looks bizarre and unusual purchases have taken place." —P15
Never know	7	"You probably wouldn't know if the attackers did a good job."—P5
News	8	"I would know I was affected in an internet data breach because I might hear about it through the media."—P2
Removed info	3	"My information on the phone gets removed."—P8
Blackmailing victim	3	"Maybe noticing data being used in a way you don't remember doing? Or they'll tell you, if they're hoping the breach will make you do something for them."—P5

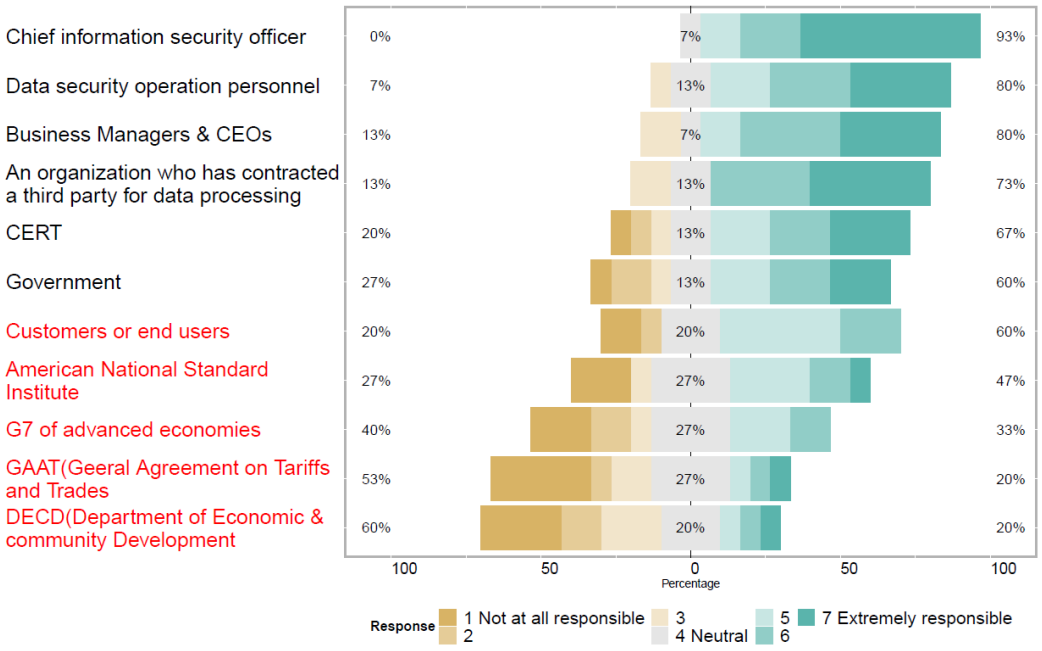


Fig 3. Accountability of people for data protection. Labels in red are inappropriate answers.

TABLE III
SAMPLE PARTICIPANTS COMMENTS FOR CAUSES OF A DATA BREACH

Causes	Total	Sample of Data Extracted
Negligence	7	"Carelessness, on the part of the designer, on the user's part for not behaving safely."—P1
Poor password	5	"When people don't use difficult enough passwords"—P30
Poor security measures	8	"A company may cut corners and just do the bare minimum to get certified."—P18
Vulnerability	6	"Vulnerability, which is having data that is not encrypted. The hacker targets vulnerable users more easily"—P3.
Hackers	9	"I believe that an Internet data breach is caused by a hacker"—P25

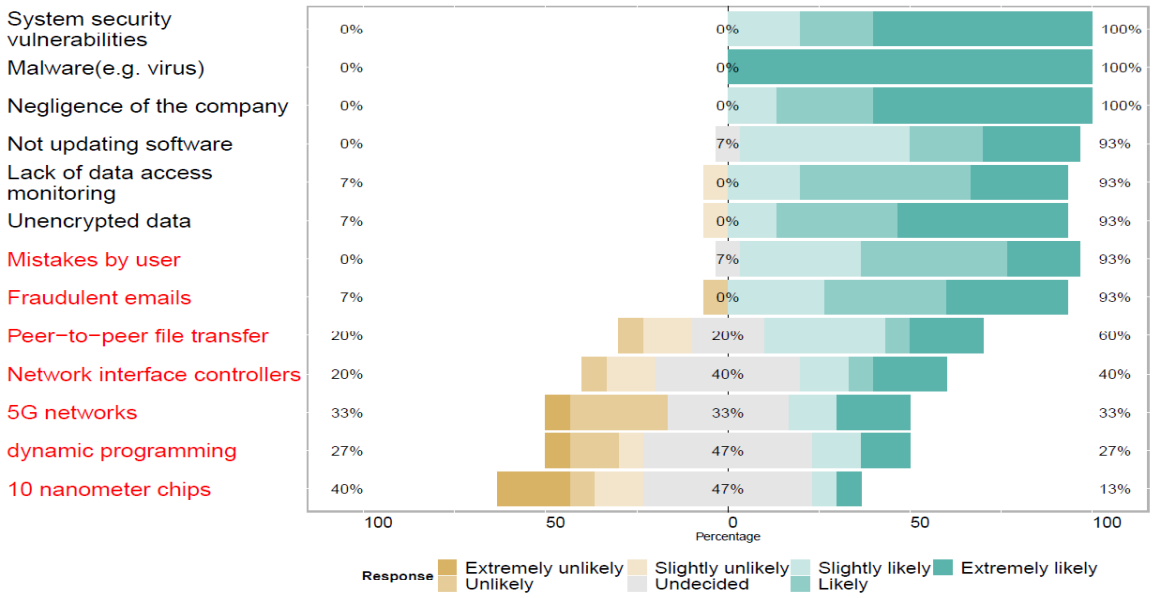


Fig 4. What causes an Internet data breach? Labels in red are inappropriate answers.

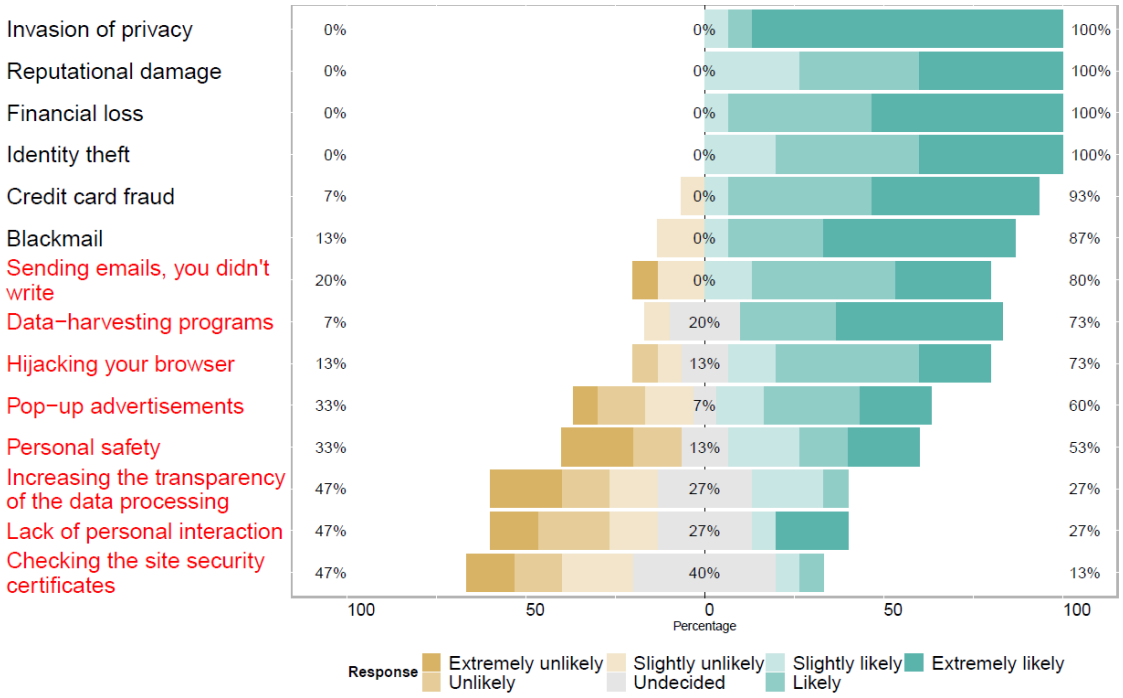


Fig 5. What are the consequences of Internet data breach? Labels in red are inappropriate answers.

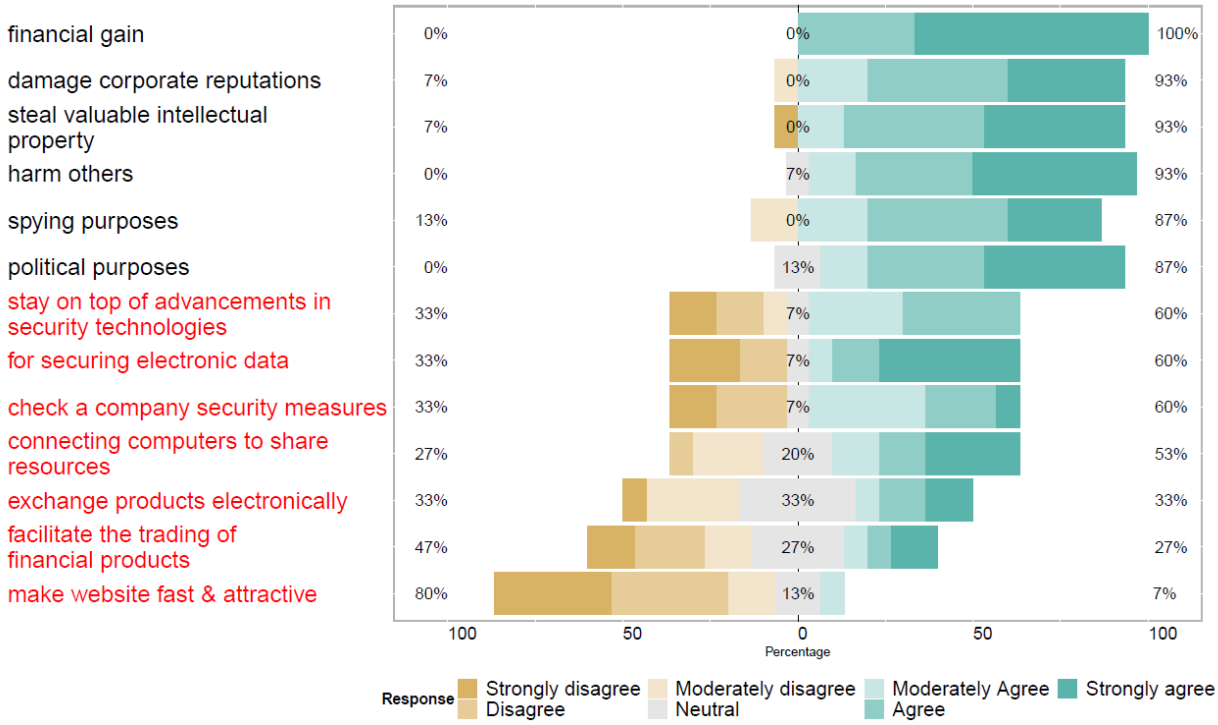


Fig 6. Why do data breaches happen? Labels in red show misleading perceptions.

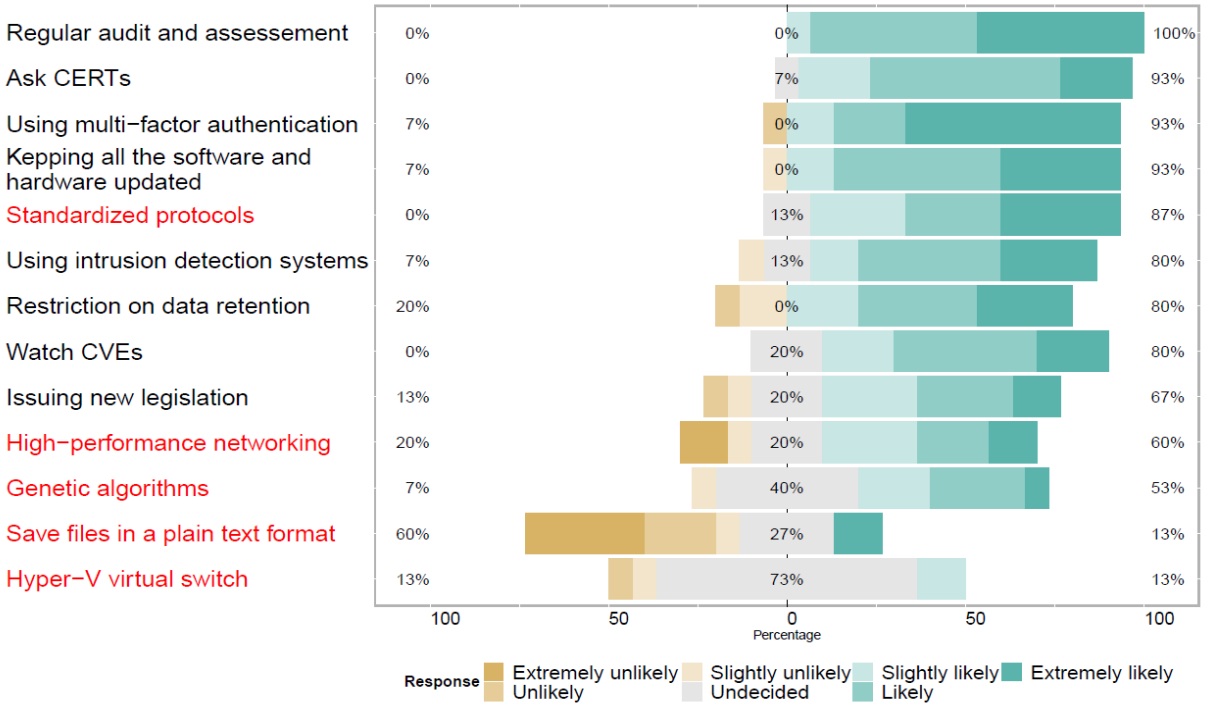


Fig 7. How likely is it to prevent a data breach via the following practices? Labels in red show misleading perceptions.

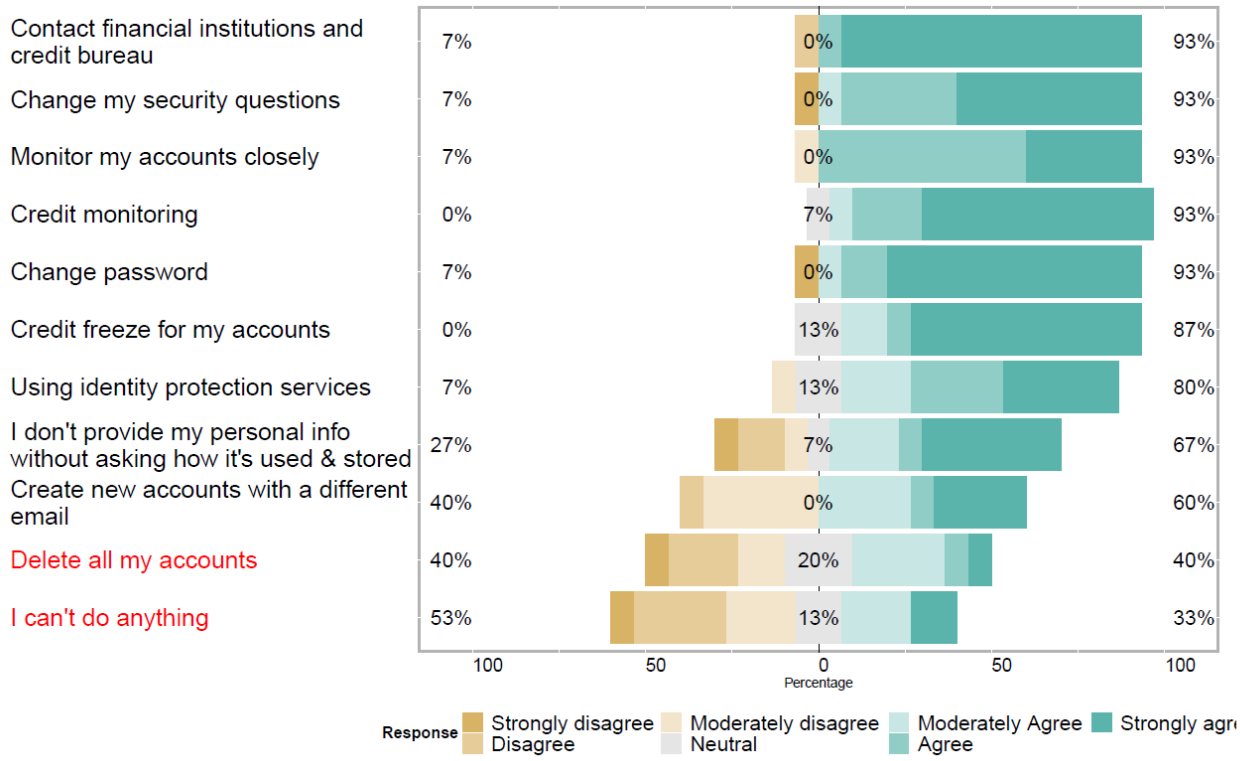
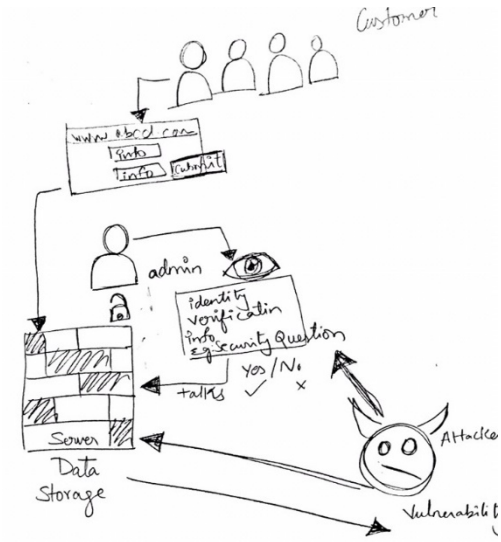
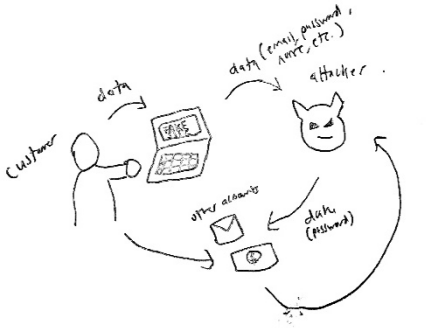


Fig 8. What can you do if your data has been breached? Labels in red show misleading perceptions.

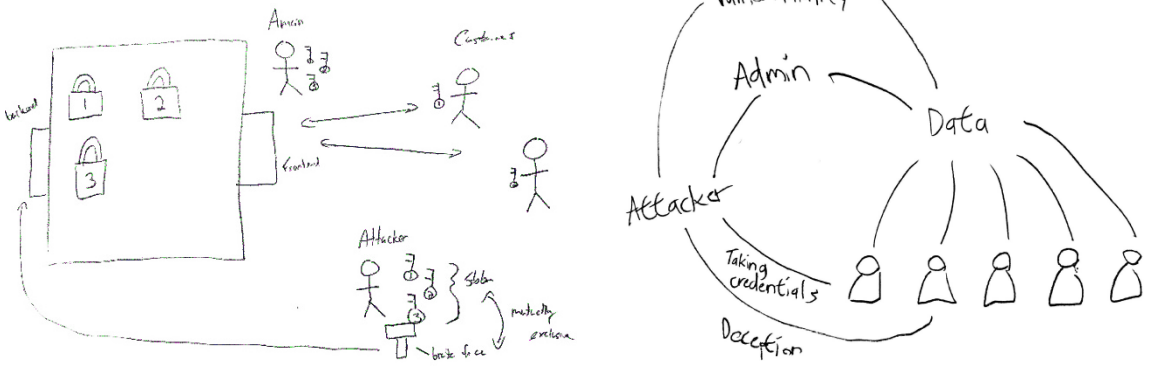


a. P19. Attacker hacks the admin system to steal identity verification data.



b. P14. Attacker hacks the user system to steal personal data.

Fig. 9. Participants' drawing 1.



a. P5. Backdoor access.

b. P27. Different types of attack.

Fig. 10. Participants' drawing 2.