Cloud Computing Data Breaches in News Media: Disclosure of Personal and Sensitive Data

David Kolevski
School of Computing and Information Technology
University of Wollongong
Wollongong, Australia
dk616@uowmail.edu.au

Katina Michael
School for the Future of Innovation in Society
Arizona State University
Tempe, Arizona
katina.michael@asu.edu

Roba Abas
School of Business
University of Wollongong
Wollongong, Australia
roba@uow.edu.au

Mark Freeman
School of Computing and Information Technology
University of Wollongong
Wollongong, Australia
mfreeman@uow.edu.au

2022 IEEE International Symposium on Technology and Society (ISTAS) | 978-1-6654-8410-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/ISTAS55053.2022.10227100

***Abstract*—Cloud computing has changed how businesses adopt information and communication technology (ICT) services that can be provisioned dynamically, providing more capacity and capability as required without the huge upfront capital expenditure. As consumers continue to use more and more online self-service portals, they increasingly leave digital footprints and personally identifiable information (PII) behind. Hackers, cloud configuration vulnerabilities, insider attacks, and accidental information security leaks are commonplace today, affecting tens of millions, if not hundreds of millions of end-users. This article recounts the story of three of the most significant data breaches internationally, Sony PSN (2011), eBay (2014) and Yahoo! (2014), through the lens of news media at the height of the data breaches. The article captures a variety of cloud computing stakeholder perspectives, identifying key socio-technical considerations that need to be addressed over the longer term for the protection of the end-user, and the continuous improvement of cloud services.**

Keywords— cloud computing, data breaches, consumers, identity theft, fraud, disclosure, misuse of data, privacy, security, personally identifiable information, value chain, stakeholders, Sony, eBay, Yahoo!

I. Introduction

Cloud computing services have undergone rapid growth since their inception and this trend is only set to continue in the coming decade, and potentially beyond, as business and government continue to undergo digital transformation. Organizations and governments (i.e., cloud customers) that otherwise would have in-house data centers, are increasingly outsourcing their processing and storage requirements to cloud providers. Cloud architecture comprises four service delivery models: software as a service (SaaS), platform as a service (PaaS), infrastructure as a service (IaaS) and Anything as a Service (XaaS) [1, 2]. Cloud providers provision ad hoc computing resources to facilitate these services, enabling cloud customers to process and store data and applications. These characteristics allow for self-service functionality that operates on a broad spectrum of devices and is hardware and software independent [3]. The higher the level of service (i.e. SaaS), the greater the functionality of the cloud provider [4]. In more recent studies, cloud computing service delivery models have converged and as a result, XaaS is growing in its use and adoption [2, 5]. Outsourced solutions, based around cloud computing services, now mean that cloud customers are operating with greater dependencies on external third-party organizations. In fact, the fulfilment of any service offering requires the availability of resources of the third party, and is reliant on the complex cloud computing value chain, which necessitates disparate stakeholders to work more closely together [6]. Responsibility is shared between an entity leasing ICT services and a supplier of those ICT services through what is known as a service level agreement (SLA). When one party is in breach of the legal contractual agreement of exchange for ICT provision or acceptable use of ICT services, then the "at-fault" party has to pay the other for damages. SLAs for the greater part are defined on measurable metrics.

Unsurprisingly, as cloud services have become embedded in our everyday lives, data breaches have increased commensurately. Most recently, Australia suffered what is arguably its biggest data breach in history when its alternate operator, Optus, a Singapore Telecom company, had 10 million records compromised. It was estimated that 40% of Australia's population had their personal information stolen, including: names, birthdates, home addresses, phone and email contacts, and passport and driving license numbers. A further 10,000 individuals had their Medicare details stolen, and about 2.8 million were deemed to be in "quite significant" risk of identity theft and fraud. While the company has maintained the attack was "sophisticated", the Australian Government is saying that the attack was anything but sophisticated, rather akin to a "kid in a garage" attack using a freely accessible software interface [31]. The hacker demanded 1.5 million Australian dollars, and the company was fined 2.1 million dollars. Operation Guardian has been launched by the Australian Federal Police working together with the private sector and industry to ensure that these individuals will not be affected through criminal activities on the dark web, through a partnership between law enforcement, the private sector and industry [32].

Security defenses of many of the world's global organizations and government agencies have been challenged. Hackers and criminal cyber groups are finding ways to penetrate the defenses that cloud services employ, either through brute force or social engineering attacks focused on a vulnerable user of the cloud service. Data breaches typically expose weaknesses and can be carried out via a series of attacks, starting from the weakest link in terms of an insider threat (e.g., employees of cloud providers), through to external, technology-driven attacks. As such, there is a pressing need to understand the socio-technical

considerations, stakeholder perspectives and effects of data breaches to enhance existing cloud services, which can be achieved through reviewing prominent data breach case studies.

This article is divided into six parts. Section II describes the cloud computing value-chain, and the various stakeholder roles involved in a typical data breach. Section III provides a brief overview of the methodology of the study. Sections IV-VI present three mini data breach cases providing a step-by-step media account of events as they unraveled after each data breach, and the prevalent socio-technical considerations that were observed. The mini cases include the Sony Play Station Network (PSN) (2011), eBay (2014) and Yahoo! (2014) data breaches as depicted in the news media. Secondary sources of evidence are used to present stakeholder perspectives of key socio-technical considerations, offering a unique point of view of the effects of data breaches, and their corresponding unintended consequences. Section VII provides a discussion on the findings from the case studies and Section VIII a conclusion.

II. Literature Review

A. Cloud Computing Value-Chain

The cloud computing value-chain is an integral component in understanding the dynamics and interaction between key stakeholders. Kolevski et al. [6] state there are operational and non-operational stakeholders within the cloud value-chain, after [24]. Operational stakeholders include cloud providers, customers, enablers, resellers, and third-party providers [24]. Non-operational stakeholders in the cloud computing value-chain include regulators, legislators, and the courts that provide oversight for organizations and end-users. Non-government organizations (NGOs), law enforcement and industry-standards bodies are other non-operational stakeholders that offer support and technical standards to cloud users and providers. End-users are non-operational as they are passive recipients of a cloud computing service offering. End-users provide their information to initialise a service using the cloud customer's portal, which is branded to the direct supplier with which an end-user conducts business. For example, suppose a utility company uses cloud computing to deliver online payment services. In that case, the end-user will interact with a website that has the branding (e.g., logo and color scheme) of that utility. Often, consumers are unaware of how a service has been provisioned, they are merely concerned with access and functionality.

B. Cloud Computing Data Breaches

It is important to define what a data breach is, before delving into the theme of cloud computing data breaches [29]. Daly [7, p. 477] explains that traditionally "data breaches involve security breaches, which lead to the disclosure, access, or acquisition of information." Similarly, Mills and Harclerode [8, p. 777] define a data breach as "when information is stolen or misappropriated." Data breaches are a result of unauthorised access to private and sensitive information [9]. Riedy and Hanus present common causes of data breaches to include an "intentional malicious activity or hacking; accidental publication; insider jobs; lost or stolen computers or media and patently malfunctioning security measures" [9, p. 12].

A cloud computing data breach is defined as a breach that discloses end-user or business data stored on a cloud service [10]. Hackers penetrate the defenses of a cloud provider or customer's cloud network and remain undetected. Hackers then retrieve the end-user or business data and disclose it for financial gain on the dark web [11]. Kumar, Raj and Jelciana [12] state that hackers can bypass basic cloud security in many cloud ecosystems. At the same time, the authors note that securing cloud services reduces the likelihood of data breaches, attack vectors through virtualization, and data at rest (i.e. unencrypted data). Logesswari et al. [13] discuss attack vectors such as distributed denial of service (DDOS) attacks, SQL attacks and virtual machine (VM) hacks and the increased incidence of these types of attacks on cloud services.

According to Mandal and Khan [14], hackers target the cloud provider or customer's weakest link to penetrate the cloud service. For instance, employees are targeted through social engineering attacks in many situations. Social engineering attacks target employees with front-facing interfaces (e.g., email) and expose them to malicious programming code or embedded malicious attachments. Hackers also target both technology vulnerabilities and human weaknesses through exploitation techniques [15]. This study aims to investigate cloud data breaches as they are presented in the media over time to garner a better understanding of the socio-technical considerations most pertinent to the public, in addition to the mechanisms of accountability that might resonate with cloud providers and cloud customers (i.e., businesses that utilize cloud services to facilitate end-user interactions).

C. Landmark Data Breach Cases

Peer-reviewed literature has reported significant data breaches, particularly from a legal context. With each data breach, vast amounts of personally identifiable information (PII) and at times other sensitive information have been exposed [30]. PII is generally considered to be any data that can identify a specific individual (e.g., name, address, email or even an IP address). Sensitive data is data denoting one's personal state, characteristics, or preferences. For example, sensitive data is deemed to be genetic, health or financial information about someone, their racial or ethnic origin, and political or religious beliefs, among other details.

In 2005, the TJX data breach impacted over 45 million end-users, disclosing credit and debit card information [16]. The hackers were able to bypass TJX's existing security protocols through the retail chain's outdated wireless network. TJX did not notify its end-users until more than 18 months after the initial discovery of the breach. In another example, Newman [17] analyzed the 2013 Target data breach that disclosed more than 100 million end-users' credit and debit card details. The hackers were able to bypass Target's vendor security and planted malware on Target's point of sale (POS) system. Target was able to patch their POS system. End-users were notified about the breach, but this occurred more than four weeks after the security attack, which was during the 2013 Christmas period.

In 2015, Anthem Healthcare was the victim of a data breach impacting 80 million end-users. The breach disclosed names, mail addresses, social security numbers (SSNs), and healthcare information [18]. The Anthem Healthcare data breach occurred when an employee opened an email containing a malicious file, and security systems were slow to detect the attack. Anthem Healthcare delayed notifying its end-users for four weeks. In 2017, the Equifax data breach affected over 145 million end-users, disclosing private,

sensitive, and financial information [19]. The disclosed data included names, physical addresses, financial information, and SSNs. The Equifax data breach resulted from the security team's delay in patching Apache's Struts systems, and hackers were able to identify the vulnerability and exfiltrate end-user data. Equifax delayed notifying end-users for four months [19]. The Anthem Healthcare and Equifax data breaches demonstrated that employees and information systems (IS) are susceptible to attacks, and showed that organizations delayed notifying end-users, which further exacerbated end-user identity (ID) theft issues.

D. Research Contribution

News media plays an important role in society, covering stories related to the public interest. Official news media outlets may be influenced by politics, but typically recount events corroborated through primary sources, such as key informants. Investigative reporting usually seeks primary evidence from the source, e.g., a company representative in the cloud computing context. Unsurprisingly, large-scale data breaches are top stories ("front page") of news publications. According to Bunker [20], one of the reasons that this has occurred is information security has transitioned from an IT-only departmental issue to a matter that affects everyone (i.e., end-users and society at large). In other words, when a significant security breach occurs within a prominent company, it is everyone's problem. The scale of a single data breach of a transnational company can now be measured at up to 700 million individuals, meaning that a breach will affect people beyond a single jurisdiction. For example, in 2021 Facebook [33] had 500 million records compromised and in the same year LinkedIn had 700 million records leaked [34]. Bunker [20] also questioned the responsibilities of the businesses (i.e., cloud customers) related to storing end-user data, pointing to the need for information assurance. The author concluded that these responsibilities lay with the cloud customer (i.e., the business) and emphasized that "the solution needs to be more; people and processes are a critical piece of the solution as technology is not enough" [20, p. 20]. This points to socio-technical considerations that necessitate further attention within the cloud computing context. Furthermore, with even greater numbers of data breaches being reported in the news media, the breaches are gaining particular attention from all types of cloud computing stakeholders in the value chain.

For instance, the study by Cross, Parker and Sansom [21] examines the 2015 Ashley Madison data breach that was front-page news and affected over 37 million subscribers (i.e. end-users). The authors applied discourse analysis to investigate the controversial breach using the Factiva database. Factiva is an online database that aggregates and stores news media content from across the globe, allowing users to search and locate news articles. The outcomes of the study [21] indicated that in the Ashley Madison data breach, the subscribers were targeted. In contrast to the discourse analysis by Cross, Parker and Sansom [21], Sinanaj [22] employed a quantitative approach to understand the implications of data breaches using news media articles. Sinanaj identified the news media outlets and categorized them into "newspapers (e.g. *The New York Times*), broadcasting channels (e.g. Bloomberg) and press agencies (e.g. Reuters)" [22, p. 1]. These two studies demonstrate that the use and emphasis on news media is a valid and important methodological approach for the study of cloud computing data breaches.

III. Methodology

A. Unit of Analysis

The three cases that will be examined in this study include: Sony PSN (2011), eBay (2014), and Yahoo! (2014), given the prominence and scale of the data breaches. The unit of analysis is a single data breach event of the respective organization that relies on cloud computing services.

B. Data Collection

Data collection for the three data breach events consisted of news media articles, primarily online newspapers. This data collection was used to investigate the socio-technical considerations associated with data breaches with a particular emphasis on the end-user. Monahan [23] notes that news media serves two functions: first, as a mechanism to bring issues to the public and second, to influence readers by raising awareness of data breaches and what they might signify. As previously stated, studies from Bunker [20] and Cross, Parker and Sansom [21] have applied news media as a valid data collection technique to investigate data breach cases.

The data collection process consisted of four parts. The first was defining the search terms, which were: "[case name]" and "privacy" and "security" and "breach*". The second part outlined the search dates, as determined from when the data breach first appeared on the news and continuing for a one-year period. The third part determined the media outlets to be searched. The media outlets chosen were: *The Australian, The Australian Financial Review, The Sydney Morning Herald, The Guardian U.K., The New York Times, The Wall Street Journal and The Washington Post.* The final component consisted of data validation, ensuring that each article fulfilled the above-mentioned data collection criteria.

C. Data Analysis

Once all the news media had been gathered using the explicit search criteria, each article was screened for inclusion based on relevance. Duplicate sources were also removed. This was especially the case for articles that had been syndicated. Articles were then numbered in the data collection corpus using a sequential numbering scheme ([article #N]) (see Appendix A). From the clean list of articles, based on date, summaries were made, extracting the most important elements of each article. Key points pertaining to socio-technical considerations, defined as those considerations that relate to either social or technological issues, were extracted. A significant stage within the data collection process was to scrutinize the interplay between stakeholders in the cloud computing value-chain to deduce patterns or trends that could be considered "lessons learned" and shared with stakeholders of relevance. The element of *time* also plays an important role in the descriptive narrative presented in the case studies, illustrating how various stakeholders in the cloud computing value chain became aware of the respective data breaches.

IV. Case one: The 2011 Sony Playstation Network Data Breach

A. Case Overview

The Sony PSN data breach occurred on April 26, 2011, with more than 100 million end-users impacted (Appendix A, Part A). Sony immediately took down the PSN. It was not until several weeks later that Sony began restoring the network and that availability of the online service was fully restored. While the service was offline, speculation arose that Sony had suffered a data breach and on May 2, 2011, Sony notified all end-users their personally identifiable information was disclosed with financial information also potentially at risk. Finally, the news media reported on key events, including service availability and restoration, and the media also published direct stakeholder comments on ID theft and fraud issues.

B. Key Socio-Technical Considerations

The news media articles focused on issues surrounding end-user access to Sony's PSN between April 26, 2011, and May 14, 2011, as well as the disclosed end-user data, including PII and financial information. The articles reported that Sony shut down its PSN without notifying its end-user base. Several articles used phrases such as "gaming network has been offline for six days" (article #1), "network was unavailable for several days" (article #83) and "the company was forced to shut down its PlayStation Network" (article #93). These phrases informed readers that the PSN was inaccessible. Furthermore, Sony announced that the shutdown of its PSN was due to an attack by an unauthorized group. Regarding the unauthorized access, several articles also confirmed that hackers disclosed end-user PII containing attributes such as names, dates of birth, email addresses, login credentials and passwords (articles #2; #3; #20). As a result, the articles reported issues related to Sony's network security and end-users' PII protection. The excerpts below present the timeline of important reported events that occurred in the days following the data breach.

• April 27, 2011: Sony highlighted that "certain players' account information, including names, birthdates, e-mail addresses and login information, was compromised" (article #3).

• April 28, 2011: Sony warned that end-users "should be alert for fraudulent activity on their credit cards" (article #5).

• April 29, 2011: Sony determined "there was a difference in timing between when the company identified an intrusion and when it learned that users' data was potentially compromised" (article #9).

• April 30, 2011: Sony said the data breach "resulted in the loss of names, addresses and possibly credit card numbers associated with 77 million accounts on its online game network" (article #11).

• May 2, 2011: Sony asked, "all users to change their passwords" (article #20).

News media articles reported on the large number of affected end-users and implied that their PII was disclosed. While the initial news coverage indicated 24.6 million end-users were affected, articles later confirmed between 77 and 100 million end-users were impacted by the breach. The articles also emphasized that the disclosed end-users' PII was valuable, and that its exposure posed an increased likelihood of ID theft. This was highlighted with terms such as "personal information" (articles #28; #56; #90; #109) and "sensitive data" (article #87), associating the end-user's ID to PII. The excerpts below highlight the effects related to the end-users and their PII in the weeks following the data breach.

• May 4, 2011: Sony "attempts to piece together who stole personal information from more than 100 million accounts on the company's online game networks" (article #28).

• May 10, 2011: Sony discovered that the data breach "occurred between April 17 and 19" (article #37).

• May 28, 2011: "Network and computer-security issues have taken on heightened importance in recent weeks after a high-profile hack of several Sony Corp. systems led to a breach of personal information" (article #56).

• June 23, 2011: "Break-ins into computer systems, potentially giving access to sensitive data such as customer information and internal emails" (article #87).

Several stakeholders stated that the end-users' disclosed passwords could be used on other online services sharing similar log on credentials. These same stakeholders stated that end-users should change their passwords or use alternative passwords for their other online services. Furthermore, the articles portrayed that the disclosed passwords produced exactly the same response, the need for end-users to change their passwords, offering limited immunity to ID theft and fraud. The stakeholder responses below demonstrate the issues with disclosed end-user passwords:

• June 23, 2011, Michael Barrett, the Chief Information Security Officer (CSIO) of PayPal, a unit of eBay Inc. said: "Having the same password for everything is like having the same key for your house, your car, your gym locker, your office" (article #88).

• September 27, 2011, Alastair MacGibbon, the then University of Canberra Centre for Internet Safety Director said: "One of the report's most relevant findings for corporates was that 90 per cent of people said their password couldn't be easily guessed. However, the recent Sony PlayStation security breach revealed that hackers could obtain the passwords of millions of users around the world" (article #113).

V. Case Two: The 2014 eBay, Inc. Data Breach

A. Case Overview

The e-commerce giant eBay, Inc. suffered a catastrophic data breach impacting 145 million end-users during February and March of 2014. eBay did not notify end-users until more than two months later, on May 22, 2014, when the news media began reporting on the data breach (Appendix A, Part B). It was speculated that an adversary targeted an eBay employee with what appeared to be a social engineering attack. This was later confirmed by numerous stakeholders, including the company. The data breach contained end-users' PII such as names, email addresses, physical addresses, telephone numbers, date of birth (DOB) and passwords.

B. Key Socio-Technical Considerations

The eBay case study focused on ID theft and the issues relating to the disclosure of end-users' PII. The news media articles reported that the eBay data breach exposed a significant number of end-users' PII. This is established

through phrases such as "what may have been the biggest ever cyber-attack" (article #1), "hackers stole encrypted passwords and other personal information" (article #4) and "the massive data breach that affected 145 million registered users worldwide" (article #6). These phrases informed the readers about the scale of the data breach and the increased risk of ID theft.

Several articles reported that the disclosed end-users' PII included names, physical addresses, email addresses, phone numbers and dates of birth (articles #1; #4; #5; #6). The articles stated that the hackers could use the disclosed end-users' PII to commit ID theft and leave end-users fending for themselves. These issues are highlighted through phrases such as "the stolen information would make eBay customers easy targets for phishing attacks" (article #5) and "once that information is no longer private, verification checks become easier to fake, leaving people at risk of identity theft and phishing attacks" (article #16). These phrases emphasized that the disclosed end-users' PII is valuable and that its availability to cybercriminals makes end-users extremely vulnerable. The issue of ID theft requires active conversations from the perspective of end-users, businesses, and governments (article #42). The excerpts below present a timeline of eBay's and other notable stakeholders' responses on ID theft, and the consequences of disclosure of end-users' PII, following the reporting of the data breach.

• May 22, 2014, Rik Ferguson, Global Vice-President of Security Research at Trend Micro said: "It should not have taken them three months to notice a break-in like this. Exposure of personal information such as postal addresses and dates of birth puts users at risk of identity theft, where the data is used to claim ownership of both online and real-world identities" (article #1).

• May 22, 2014, Alan Marks, Senior Vice President (SVP) of Global Communications at eBay said: "In eBay's case, the company stored users' names, email and physical addresses and birth dates in plain text but encrypted their passwords. Most states would not have required eBay to disclose the breach" (article #5).

• May 23, 2014, Kaman Tsoi, partner at Herbert Smith Freehills said: "If hackers could not decrypt the passwords, they might have had access to personal information that could be used for cyber-attacks" (article #6).

• May 24, 2014, Gerard Lommel, the President of the Luxembourg Data Protection Authority said: "The growth of online data would most likely lead to more privacy breaches, as individuals increasingly upload personal information onto services run by some of the world's largest tech companies. We will have more and more nightmares" (article #7).

• May 27, 2014, Mark Hurd, President of Oracle Corp. said: "We are in an era because of all the data around, there is no shortage of people wanting to attack. It's a constant battle and I don't think it will let up" (article #11).

• June 3, 2014, David Schoenberger, Chief Innovation Officer of Secure Cloud Systems said: "They are finding more clever ways of breaking into the perimeter security and, more importantly, finding someone on the inside to sell them their credentials to get the data" (article #15).

• June 4, 2014, Christopher Graham, the U.K. Information Commissioner said: "This sort of thing is going to go on and on and on until businesses wake up and realize that personal information is not their plaything; it's our information and it needs to be protected" (article #16).

News media articles reported that the disclosed passwords could have negative consequences on end-users. For example, end-users that use the same password for multiple online services are vulnerable to hackers accessing those services. Shortly following the reporting of the data breach, eBay issued a notice to end-users notifying them that they needed to change their passwords on its platform. The notice was then reported in the news media for some months. The continuous reporting of eBay's notice informed readers that action needed to be taken. However, these communications deflected attention from the severity of the situation, given all the other PII disclosed in the data breach. Once again, the end-user is left with the responsibility to apply quick-fix measures in response to data breaches, though the accountability should be spread between stakeholder types. The excerpts below present the news media coverage on end-users' disclosed passwords.

• May 22, 2014: "eBay Inc. urged its 145 million users to change their passwords because of a data breach. But if the past is a guide, few people will heed the warning" (article #3).

• May 23, 2014: "eBay has urged users to immediately change their passwords, even though they were encrypted" (article #6).

• May 25, 2014: "eBay wants its 145 million users to change their passwords after a cyberattack on the site" (article #9).

• June 4, 2014: "To what has been described as the biggest ever hack against eBay, which forced 145 million users to change their passwords" (article #16).

• June 10, 2014: "Online auction giant eBay recently urged customers to update their passwords because of a massive security breach" (article #17).

• July 17, 2014: "All eBay users were asked to reset their passwords" (article #24).

Several news media articles reported that biometrics should replace passwords. While positive affirmation on biometrics was reported, several stakeholders indicated the problems associated with disclosed biometric data. For example, Stuart Geiger, a then Doctoral Student at the University of California, Berkeley's School of Information, said: "putting the password out of its misery would require collaboration from a gaggle of Silicon Valley companies that compete against each other in everything from online shopping to chats to television" (article #3). Similarly, Gregg Stefancik, an Engineering Director at Facebook, Inc., commented on biometrics and said, "the reason I hate it is because I can't change them" (article #17). Stefancik also said, "once his biometric data was compromised, his fingerprints or retina could not be amended unlike other forms of authentication like passwords." The two stakeholders articulated the hidden dangers with biometric data, and that while it is another form of authentication, it should be used carefully. It is in fact, as already stated, highly sensitive data.

VI. Case Three: The 2014 Yahoo! Inc. Data Breach

A. Case Overview

The third case focused on the 2014 Yahoo!, Inc. data breach, without a specific date of intrusion identified. The 2014 data breach was not reported until September 22, 2016, more than two years after the intrusion (Appendix A, Part C). The data breach impacted over 500 million end-users and disclosed names, email addresses, telephone numbers, DOB, passwords and security questions and answers (Q&A). Following the trend of the previous two cases, the news media immediately began reporting on the data breach and key stakeholders were interviewed by journalists. On December 14, 2016, the news media began reporting that Yahoo! was subject to another data breach in 2013 that exposed the data of one billion end-users.

B. Key Socio-Technical Considerations

The Yahoo! case study focused on end-user ID theft and the size of the data breaches reported. It is important to note that the case study investigated the 2014 data breach. However, during data collection, Yahoo! announced that an earlier data breach occurred in 2013. Therefore, the case study presents issues surrounding the size of the 2013 and 2014 data breaches and the disclosed end-user data. Several articles reported that the 2014 data breach was one of the largest data breaches to be ever reported. For example, the articles reported phrases such as "hackers stole the personal data associated with at least 500m Yahoo accounts" (article #2) and "largest data breach in history - affecting at least 500 million user accounts" (article #6). These phrases emphasized the sheer size of the 2014 data breach. The news media articles also reported that the 2013 data breach, which was announced in December 2016, exposed the data of one billion end-users (articles #41; #49; #83). This is described with phrases such as "a newly discovered data breach exposed the private information of more than one billion Yahoo users" (article #40) and "we thought the previous breach of 500 million user accounts was huge, but 1 billion is monumental" (article #41). These phrases signified the magnitude of the 2013 data breach.

In addition, the articles reported that the disclosed end-user data contained PII. The articles stated names, email addresses, telephone numbers, dates of birth, passwords and security questions and answers (Q&A) were disclosed (articles #2; #40; #51; #76). Some articles also reported that organizations could have provided better security for Q&A. Article (#4) reported that "Yahoo did not encrypt all the security questions it stored, and so some [we]re readable in plain text." Similarly, article (#46) reported that security Q&As are troubling for end-users, as they are commonly used to answer questions such as "the maiden name of the user's mother, the user's high school or place of birth." These questions are often unique and do not change which pose continued risks to end-users. Moreover, the exposed PII could allow hackers to access other of the end-users' online services. The excerpts below present the timeline of reporting on disclosed end-user PII.

• September 23, 2016: "Details including names, passwords, email addresses, phone numbers and security questions were taken" (article #2).

• September 23, 2016, Alex Holden, Founder of Hold Security LLC said: "The stolen Yahoo data is critical because it not only leads to a single system but to users' connections to their banks, social media profiles, other financial services and users' friends and family" (article #5).

• December 15, 2016: "The hackers stole data including names, email addresses, telephone numbers, dates of birth and passwords" (article #40).

• December 15, 2016, Bruce Schneier, a cryptologist and one of the worlds most respected security experts stated: "Yahoo badly screwed up. They weren't taking security seriously and that's now very clear. I would have trouble trusting Yahoo going forward" (article #41).

• December 16, 2016, Sachin Kansal, Vice President (VP) for Consumer Products at Lookout, Inc. said: "Anyone can guess most of the answers to these things by a quick scan of your Facebook and LinkedIn profiles" (article #45).

• December 16, 2016, Tatu Ylonen, CEO at SSH Communications Security, Inc. said: "It doesn't matter if you haven't used your Yahoo account for 10 years, your mother's maiden name or where you met your spouse is likely to stay the same. Or even if your spouse changes, your mother's maiden name still stays the same" (article #46).

• January 18, 2017, Chris Gatford, Director of Hacklabs, a PS&C company said: "You can never get back your date of birth when that information is stolen and that is something we use as an authenticator to gain access to account information" (article #57).

VII. Discussion

A. Cross-Case Comparison of Data Breach Cases and Key Outcomes

In the Sony PSN case in 2011, several articles reported that ID theft was a concern (articles #1; #9). The same occurred in the eBay case, as it was shown that stakeholders highlighted that the disclosed PII posed significant ID theft issues, that could lead end-users to become victims of cybercrime. In the Yahoo! case study, the news media articles also reported that the disclosed end-users' PII could expose them to ID fraud. Likewise, stakeholders said the disclosed PII could allow hackers to access other online services and retrieve sensitive and private information. The articles in the Sony PSN case reported that the disclosed end-users' PII included their names, addresses, dates of birth, email addresses, login credentials and passwords, and that the exposure affected an estimated 100 million end-users. Similarly, in the eBay data breach of 2014, news media articles reported that the breach affected over 145 million end-users and exposed their names, physical addresses, email addresses, phone numbers and dates of birth.

The effects of the Sony PSN data breach were immediate and imposed a higher probability of an end-user falling victim to ID theft. Stakeholders noted that end-users who had followed instructions to change their password still gained minimal ID theft protection, given that most people used similar passwords across platforms. So, one single data breach in effect, meant that individuals had to change all their passwords across a variety of online platforms. In the eBay case study, the responsibility was also placed on end-users to change their passwords. End-users were notified repeatedly of the benefits that the changing of their password would yield. But again, it was noted that end-users who changed their passwords gained minimal ID theft protection. In the case of the two Yahoo! data breaches, commentaries in the media by

security experts emphasized that it was the biggest hack of all time. In this case, it was not just essential PII that were disclosed but also security-related Q&A presented far greater challenges compared to other PII. End-users would have a hard time changing their security Q&A each time a data breach occurred. Finally, the ID theft issue portrays a common problem in cloud data breach studies; the more PII exposed, the greater the risk of ID theft.

The articles reported that Sony, eBay, and Yahoo! had experienced significant data breaches, resulting in end-user data disclosure. Each data breach case had in-depth coverage, including stakeholder representation outlining their views and opinions. There are three key outcomes emanating from this detailed case study analysis. The first was the way in which each company dealt with the hacking and data disclosure. Sony took their gaming service offline, while eBay and Yahoo! kept their services available. The second key outcome was noting the diverse responses by stakeholders (operational and non-operational), with respect to end-user data that was disclosed. The consistent response indicated that end-user data was invaluable, and organizations needed to do better in protecting data. The third key outcome pertains to the absence almost wholly of cloud computing providers in the news media. These providers seldom acknowledge publicly their security shortcomings, and this may be for several reasons, some of them legal or contractual as related to service level agreements (SLAs).

B. The Disclosure of End-User Identity (ID) Information

The three data breach case study incidents disclosed different types of end-user PII, including names, physical addresses, email addresses, DOB, passwords, and secret Q&As. It is important to note that these attributes contain the essential details of identity of end-users. At the same time, they are used to sign on to online services. These attributes are essential to organizations providing services. However, they also are the single reason most hackers target organizations. The same can be said about the financial information collected and stored by cloud stakeholders. End-users are handing out their financial information to organizations to pay for service consumption. The stored credit or debit card data is lucrative for hackers.

The central issue of ID theft was the concept of ID fraud. Some news media articles even reported that ID fraud would always be a pressing issue, and that it would continue to be an inevitable risk of conducting business online. End-users will also be at risk of future harm as the disclosed PII was used to gain access to other online services and could be used in the future for various nefarious purposes. Operational stakeholders (e.g., cloud providers) viewed ID theft as posing significant risks to end-users and even suggested that users need to be vigilant in identifying risks. However, any attempt to address these risks is an increasingly arduous task for stakeholders. Non-operational stakeholders (e.g., public sector organizations), on the other hand, viewed ID theft as a significant issue facing end-users, and condemned businesses for the lack of data protection. They too, expressed that enterprises need to act in response to the holistic issues at hand, and provide support to end-users in the time of crisis. There has been relative silence on the matter by the biggest cloud computing providers, such as Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, Alibaba Cloud, and IBM [25].

C. Disclosure of End-User Passwords and Biometrics

Based on the outcomes of the case studies, end-users are utilising more cloud services for everyday tasks, without even realizing they are using the cloud. This is particularly true of government agencies taking essential citizen services online [26]. Yet citizens continue to use the same password for various online services, exposing them to password reuse dangers. Already, high profile data breaches have shown the consequences of such events occurring, including targeted attacks locking individuals out of their own online web services [27]. Password use for account access continues and, even though two-factor authentication (i.e., a password and additional security token) is widely available, users often proceed without it. Importantly, each case study demonstrated that the resetting of end-user passwords did not protect them from further ID theft. Instead, it masked the problem until another data breach appeared in the news media. Finally, two prominent stakeholders in the eBay data breach indicated that biometric data, that would no doubt be touted as a more secure solution in the future, could not be amended like passwords and should only ever be collected with caution. Today, we have the increased incidence of two-factor authentication which requires a password to be used in tandem with a secondary token, such as a mobile phone SMS secure code, to enable a service, making online systems harder to penetrate.

D. Data Breach Milestones and Stakeholder Engagement

The news media allowed important events that occurred during reporting to be time-stamped. For example, in the Sony PSN case study, immediate reporting of service disruption and the number of end-users impacted took place in the days following the data breach. The eBay case study displayed similar reporting in that the media covered eBay's response to the disclosure and noted the number of end-users having data disclosed. At the time, the Yahoo! data breach was one of the largest, but today we have data breaches where there are over 1 billion end-users that have been compromised. In all case studies, stakeholders of diverse expertise and backgrounds were included in the reporting to the public when they were asked to comment. They each had their opinion voiced on how end-users had their ID stolen and were at a heightened risk of ID theft. Finally, news media allows for stakeholders to actively participate in a discussion of the breach events even if they are indirectly involved in the cloud computing value chain, promoting better mitigation strategies and the potential of engaging with the public regarding hidden dangers of disclosed end-user data that would otherwise not be reported. Overall, an important role of the media is in raising awareness and creating knowledge that can in turn help end-users become more informed about secure online practices, more broadly.

E. The Consequences of Cloud Computing Data Breaches

For the future, data breaches are here to stay so long as PII and sensitive data are collected by organizations. The breaches generally involve large numbers of stakeholders and have the potential to cause extensive harm which is usually asymmetric in its consequences. Data breaches have a significant impact on direct stakeholders, but the onus continues to be on the end-user to try to cope with compromised credentials while needing to continue to transact online. The transition from on-premise computing, storage and processing has seen a dramatic shift to cloud computing. However, along with this shift, we have witnessed an unprecedented number of data

breaches from remote locations. We have also witnessed in the three data breach cases discussed here that users (i.e., end-users) are significant cloud stakeholders in the value-chain. The end-user is an integral member of the cloud computing value chain and must not be sidelined or given inadequate consideration because the consequences of data breaches are personal. Whether this issue is noticed by end-users, or by other operational stakeholders, end-user data disclosure is an urgent growing concern.

F. Key Recommendations

1) Creating and Promoting More Privacy Advocacy Groups to Represent End-Users

The three case studies have demonstrated that more end-user representation is needed. We propose that privacy advocacy groups become more involved in representing end-users when data breaches occur. These groups could be primary advocates for end-users in the media, representing all those who have been subject to a breach. It is equally important that privacy groups advocate for organizations to better protect end-user data and publicize the implications of exposed data. They can do this by actively engaging stakeholders in privacy impact assessments or risk assessments, potentially providing guidelines for big data governance. These groups should seek support from governments, to further educate end-users about issues related to stolen credentials being used at a later date to open bank accounts and commit ID fraud. Finally, the principal focus of privacy advocacy groups should be to acknowledge and promote understanding of the socio-technical implications of cloud data breaches, placing pressure on operational stakeholders of cloud computing providers to seek continuous improvement in their security practice. Corporations also have a duty to protect end-user data, and the role of the media along with non-government organizations (NGOs) is to apply commensurate pressure until industry change is enacted.

2) Continued Use of Passwords and a Tiered Approach in the Rollout of Biometric Authentication

Passwords have endured throughout the decades and are still the most used type of authentication service to facilitate access to a technology-based system. The preference is for two-factor authentication that requires the use of a password and a secondary token such as a code sent to a mobile phone via SMS. The use of biometrics might seem like an ideal technology to adopt because of its unique attributes but biometrics that cannot be changed are perhaps the most sensitive data that could be exchanged online by an end-user. While biometrics are still considered a future technology to invest in, many end-users remain reluctant to use these authentication techniques despite having uploaded facial biometrics to social media sites. Already we are witnessing organizations rolling out biometric options for authentication, including, voice, face, and other forms. Over time and with sustained succession plans, biometrics could be rolled out to support advanced online services. Future headlines could read: "data breach discloses biometrics, end-users asked to do the impossible, change their credentials". But this is already a real scenario [28].

G. Learning from Past Data Breaches

The news media is continuing to report data breach cases that have impacted millions of end-users. While there is an increase in reporting, there has been little response from organizations and governments to better protect those that had their data disclosed. The immediate response from news media is to change passwords and to sign up to credit monitoring services. The reality of the situation is far greater than just applying a band aid fix. The problem begins with our design principles, in that privacy and security needs are overlooked [35, 36]. From there, employee training, tasks and processes need to be reviewed but are neglected. These learning outcomes have been avoided, and as a result, organisations are not improving their defences against cybercriminals from launching sophisticated attacks. An organisation may be reluctant to change from their traditional system designs; however, as the data breach cases have shown us, resistance to change and moving to cloud services have consequences. The short answer to this data breach implication is: no, we have not learned from our past mistakes, and the inability to do so creates profound issues for all cloud stakeholders.

The three data breach cases investigated in this study not only provide an historical perspective on cloud data breaches, but also allow critical events to be revisited, and for further dialogue on consequences that were not apparent during the reporting period. Revisiting past data breaches allows researchers to investigate the breaches with alternative data collection and analysis methods. For instance, in this study, the socio-technical approach was applied to enable an investigation of the breaches through the socio-technical lens. Trends and patterns have emerged that otherwise would had been neglected. Considering the progress in technical and regulatory aspects of data protection, the three data breach cases have shown us we have progressed, however, at glacial rate. The learnings from the continued news media reporting on data breaches have not been fully considered from organizations for the purpose of better improving their security defenses. Simultaneously, governments have not taken end-user data protection needs, apart from the European Union and their General Data Protection Regulation (GDPR), and California Consumer Protection Act (CCPA), into account.

VIII. Conclusion

Cloud computing services have facilitated a massive shift in how businesses and governments manage their ICT infrastructure. At the same time, we are witnessing hackers eager to expose cloud providers and penetrate end-users' security defences. This study has two main outcomes. The first is related to the news media reporting of cloud data breaches. The case studies have demonstrated that news media reporting is an essential data collection technique to portray important events that occurred over a historical timeline, incorporating diverse voices from the cloud computing value chain through informative reporting. News media articles have been shown in this study to have raised awareness about data breaches. The second outcome is that recent data breaches have demonstrated that organizations and governments are repeatedly failing to learn from past data breaches. Possibly the risk appetite stemming from successive data breaches is still negligible, allowing organisations to continue to absorb the brand damage without significant long-term financial losses. The Sony PSN data breach did not apply sufficient security protocols to overcome intrusion and eBay failed to train their employees to recognize social engineering attacks. Yahoo! did not apply up-to-date data security. The news media portrayed key stakeholder opinions in identifying ID

theft issues, however, cloud providers and customers have not been extensively cited in the media publicly speaking about data breaches they have experienced. Greater accountability is still necessary by operational stakeholders through advocacy for industry failings.

A. Future Research

The increasing number of cloud computing data breaches has shown that there is an urgent need to research all types of ICT hacks. For example, research that captures data breach reporting over multi-year periods could be used to present the socio-technical and other consequences of data breaches, revealing common considerations and lessons to inform future cloud computing data security practices. Key voices in data breach reporting that would otherwise be missing in limited time scale studies could be heard and factored into discussions, subject to non-disclosure agreements (NDA). In addition, finding evidence that "injury-in-fact" has occurred to end-users would help in proving the financial, time and other losses incurred by end-users. It is one thing to study the large-scale disclosure, and another to find tangible evidence that individuals have been impacted by the misuse of data or identity theft, and to then quantify that impact appropriately [29].

ACKNOWLEDGMENT

We would like to thank Terri Bookman for her editorial support.

REFERENCES

[1] Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J., Brandic, I., 2009, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility", *Future Generation Computer Systems*, vol. 25, no. 6, pp. 599-616.

[2] Varghese, B., Buyya, R. 2018, "Next generation cloud computing: New trends and research directions", *Future Generation Computer Systems*, vol. 79, pp. 849-861.

[3] Xiao, Z., Xiao, Y. 2013, "Security and privacy in cloud computing", *IEEE Communications Surveys & Tutorials*, vol. 15, no. 2, pp. 843-859.

[4] Spring, J. 2011, "Monitoring cloud computing by layer, Part 1", *IEEE Security & Privacy*, vol. 9, no. 2, pp. 66-68.

[5] Zhang, Y., Lan, X., Ren, J. & Cai, L. 2020, "Efficient computing resource sharing for mobile edge-cloud computing networks", *IEEE/ACM Transactions on Networking*, vol. 28, no. 3, pp. 1227-1240.

[6] D. Kolevski, K. Michael, R. Abbas, M. Freeman, "Stakeholders in the cloud computing value-chain: A socio-technical review of data breach literature", 2020 *International Symposium on Technology and Society*, Phoenix, Arizona, 2020, pp. 290-293.

[7] Daly, A. 2018, "The introduction of data breach notification legislation in Australia: A comparative view", *Computer Law & Security Review*, vol. 34, no. 3, pp. 477-495.

[8] Mills, J.L. & Harclerode, K. 2017, "Privacy, mass intrusion, and the modern data breach", *Florida Law Review*, vol. 69, no. 3, pp. 771-830.

[9] Riedy, M. K. & Hanus, B. 2016, "Yes, your personal data is at risk: Get over it!", *SMU Science & Technology Law Review*, vol. 19, no. 1, pp. 3-52.

[10] Rahulamathavan, Y., Rajarajan, M., Rana, O.F., Awan, M.S., Burnap, P., Das, S.K. 2015, "Assessing data breach risk in cloud systems", *2015 IEEE 7th International Conference on Cloud Computing Technology and Science (CloudCom)*, pp. 363-370.

[11] Wang, C., Jan, S.T.K., Hu, H., Bossart, D., Wang, G. 2018, "The next domino to fall: Empirical analysis of user passwords across online services", *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy*, Tempe, AZ, USA, pp. 196–203.

[12] Kumar, P.R., Raj, P.H., Jelciana, P. 2018, "Exploring data security issues and solutions in cloud computing", *Procedia Computer Science*, vol. 125, pp. 691-697.

[13] Logesswari, S., Jayanthi, S., KalaiSelvi, D., Muthusundari, S., Aswin, V. 2020, "A study on cloud computing challenges and its mitigations", *Materials Today: Proceedings*.

[14] Mandal, S., Khan, D.A. 2020, "A study of security threats in cloud: Passive impact of COVID-19 pandemic", *2020 International Conference on Smart Electronics and Communication (ICOSEC)*, pp. 837-842.

[15] Kolevski, D., Michael, K. 2015, "Cloud computing data breaches a socio-technical review of literature", *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, Greater Noida, India, pp. 1486-1495.

[16] Fisher, J.A. 2013, "Secure my data or pay the price: Consumer remedy for the negligent enablement of data breach", *William & Mary Business Law Review*, vol. 4, no. 1, pp. 215-239.

[17] Newman, B.V. 2015, "Hacking the current system: Congress' attempt to pass data security and breach notification legislation", *University of Illinois Journal of Law, Technology & Policy*, vol. 2015, no. 2, pp. 437-460.

[18] Kass, E.M. 2015, "Do federal regulations help or hinder patient data security?", *Health Data Management*, vol. 23, no. 4, pp. 24, 26, 28.

[19] Kenny, C. 2018, "The Equifax data breach and the resulting legal recourse", *Brooklyn Journal of Corporate, Financial & Commercial Law*, vol. 13, no. 1, pp. 215-238.

[20] Bunker, G. 2012, "Technology is not enough: Taking a holistic view for information assurance", *Information Security Technical Report*, vol. 17, no. 1–2, pp. 19-25.

[21] Cross, C., Parker, M., Sansom, D. 2019, "Media discourses surrounding 'non-ideal' victims: The case of the Ashley Madison data breach", *International Review of Victimology*, vol. 25, no. 1, pp. 53-69.

[22] Sinanaj, G. 2014, "News media sentiment of data breaches", *20th Americas Conference on Information Systems (AMCIS 2014),* Savannah, GA, pp. 1-9.

[23] Monahan, B.A. 2010, *The shock of the news: Media coverage and the making of 9/11*, New York University Press, NY.

[24] Abbas, R., Michael, K., Michael, M.G. (2014), "The regulatory considerations and ethical dilemmas of location-based services (LBS): A literature review", *Information Technology & People*, vol. 27 no. 1, pp. 2-20. https://doi.org/10.1108/ITP-12-2012-0156

[25] L. Dignan, "Top cloud providers in 2021: AWS, Microsoft Azure, and Google Cloud, hybrid, SaaS players", *ZDNet*.com, 2 April 2021, https://www.zdnet.com/article/the-top-cloud-providers-of-2021-aws-microsoft-azure-google-cloud-hybrid-saas/

[26] Chanthadavong, Aimee, “NSW government sets public cloud as default standard for agencies”, *ZDNet.com*, October 2, 2020, https://www.zdnet.com/article/nsw-government-sets-public-cloud-as-default-standard-for-agencies/
[27] Honan, Mat, “Hacked: Passwords have failed and it's time for something new”, *Wired*, 17 January 2003, https://www.wired.co.uk/article/hacked
[28] Peterson, Andrea, “OPM says 5.6 million fingerprints stolen in cyberattack, five times as many as previously thought”, *Washington Post*, 23 September 2015, https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/
[29] Kolevski, D., Michael, K., Abbas, R., Freeman, M. (2021, October). “Cloud computing data breaches: A review of US regulation and data breach notification literature”. In *2021 IEEE International Symposium on Technology and Society (ISTAS)* (pp. 1-7). IEEE.
[30] Kolevski, D., Michael, K., Abbas, R., Freeman, M. (2021, July). “Cloud data breach disclosures: the consumer and their personally identifiable information (PII)?” In *2021 IEEE Conference on Norbert Wiener in the 21st Century (21CW)* (pp. 1-9). IEEE.
[31] Turnbull, Tiffanie, “Optus: How a massive data breach has exposed Australia”, *BBC News*, 29 September 2022, https://www.bbc.com/news/world-australia-63056838.
[32] AFP. “Operation Guardian delivers specialised protection for Optus customers”, *Australian Federal Police*, 30 September 2022, https://www.afp.gov.au/news-media/media-releases/operation-guardian-delivers-specialised-protection-optus-customers.
[33] Newman, Lily H. “What really caused Facebook's 500M-User data leak?” *Wired*, 6 April 2021, https://www.wired.com/story/facebook-data-leak-500-million-users-phone-numbers/
[34] Morris, Chris. “Massive data leak exposes 700 million LinkedIn users’ information”, *Fortune*, 30 June 2021, https://fortune.com/2021/06/30/linkedin-data-theft-700-million-users-personal-information-cybersecurity/
[35] Cavoukian, A. 2008. Privacy in the clouds. *Identity in the Information Society*, 1(1), pp. 89-108.
[36] Cavoukian, A., 2012. Privacy by design. *IEEE Technology and Society Magazine*, 31(4), pp. 18-19.

IX. Appendix A

A. Sony Media Data Set

#1 N. Wingfield, I. Sherr & B. Worthen, Hacker Raids Sony Videogame Network, Dow Jones & Company, Inc., The Wall Street Journal, April 27, 2011. Accessed on: October 12, 2017.
#2 B. Quinn & C. Arthur, Personal data of 77m PlayStation users hacked, Guardian Newspapers Limited The Guardian, April 27, 2011. Accessed on: October 12, 2017.
#3 M. Censer, Sony PlayStation user data compromised, Washington Post The Washington Post, April 27, 2011. Accessed on: October 12, 2017
#5 C. Arthur & K. Stuart, Identity theft fear for 3m PlayStation users in UK: Personal details stolen by hackers in major data leak System shut down as Sony issues worldwide alert, Guardian Newspapers Limited The Guardian, April 28, 2011. Accessed on: October 12, 2017.
#9 D. Guest, F. Foo, C. Griffith, Sony sat on cyber breach for days, News Ltd. The Australian, April 28, 2011. Accessed on: October 12, 2017.
#11 N. Wingfield, I. Sherr & B. Worthen, Corporate News: U.S. Officials Quiz Sony on Data Theft, Dow Jones & Company, Inc. The Wall Street Journal, April 30, 2011. Accessed on: October 12, 2017.
#20 Sony bosses apologise over theft of data from PlayStation network, Guardian Newspapers Limited The Guardian, May 02, 2011. Accessed on: October 12, 2017.
#28 N. Wingfield & I. Sherr, Sony Brings In High-Tech Sleuths, Dow Jones & Company, Inc. The Wall Street Journal, May 04, 2011. Accessed on: October 12, 2017.
#37 C. Griffith, Sony class action `difficult', News Ltd. The Australian, May 10, 2011. Accessed on: October 12, 2017.
#56 N. Hodge & I. Sherr, Corporate News: Lockheed Martin Hit By Security Breach, Dow Jones & Company, Inc. The Wall Street Journal, May 28, 2011. Accessed on: October 12, 2017.
#83 B. Worthen & A. Troianovski, Firms Come Clean on Hacks --- Armed With Crisis Plans, Companies More Readily Disclose Computer-Security Incidents, Dow Jones & Company, Inc. The Wall Street Journal, June 17, 2011. Accessed on: October 12, 2017.
#87 C. Bryan-Low & S. Gorman, Inside the Anonymous Army Of 'Hacktivist' Attackers, Dow Jones & Company, Inc. The Wall Street Journal, June 23, 2011. Accessed on: October 12, 2017.
#88 By Stu Woo, What Makes a Password Stronger --- With Concern About Hackers, Tools for Remembering So Many Codes; No More Pet Names or 123456, Dow Jones & Company, Inc. The Wall Street Journal, June 23, 2011. Accessed on: October 12, 2017.
#90 I. Sherr, Corporate News: Hackers Hit Videogame Maker Electronic Arts, Dow Jones & Company, Inc. The Wall Street Journal, June 25, 2011. Accessed on: October 12, 2017.
#93 H. Tabuchi, Sony Names New Management for Global PlayStation Unit, The New York Times Company The New York Times, June 30, 2011. Accessed on: October 12, 2017.
#109 D. Wakabayashi, Sony Names Top Online-Security Executive, Dow Jones & Company, Inc. The Wall Street Journal, September 07, 2011. Accessed on: October 12, 2017.
#113 M. Sharma, Loose password policies sink ships, and corporates `must take the lead', News Ltd. The Australian, September 27, 2011. Accessed on: October 12, 2017.

B. eBay Media Data Set

#1 S. Gibbs, Change your password, says eBay after 'biggest ever hack': Database with names and addresses is compromised: Financial information not divulged, auction site says, Guardian Newspapers Limited The Guardian, May 22, 2014. Accessed on: October 12, 2017.
#3 D. Yadron & K. Rosman, Despite Data Thefts, The Password Endures, Dow Jones & Company, Inc. The Wall Street Journal, May 22, 2014. Accessed on: October 12, 2017.
#4 A. Peterson, EBay data breached; users cautioned, Washington Post The Washington Post, May 22, 2014. Accessed on: October 12, 2017.
#5 N. Perlroth, EBay Urges New Passwords After Breach, The New York Times Company The New York Times, May 22, 2014. Accessed on: October 12, 2017.

#6 F. Foo, Warning after eBay passwords ‘stolen’, News Ltd. The Australian, May 23, 2014. Accessed on: October 12, 2017.
#7 M. Scott, European Regulators to Start Inquiry Into eBay Data Breach, The New York Times Company The New York Times, May 24, 2014. Accessed on: October 12, 2017.
#9 AT&T buys DirecTV to take on cable rivals, Washington Post The Washington Post, May 25, 2014. Accessed on: October 12, 2017.
#11 J. Kehoe, How Chinese hacking attack felled Nortel, Fairfax Media Management Pty Limited The Australian Financial Review, May 27, 2014. Accessed on: October 12, 2017.
#15 J. Kehoe, Firewalls are no longer the solution, Fairfax Media Management Pty Limited The Australian Financial Review, June 3, 2014. Accessed on: October 12, 2017.
#16 S. Gibbs, Analysis After cryptolocker, how do we make data safe?, Guardian Newspapers Limited The Guardian, June 4, 2014. Accessed on: October 12, 2017.
#17 F. Foo, Biometrics ‘worse than passwords’, News Ltd. The Australian, June 10, 2014. Accessed on: October 12, 2017.
#24 M. Isaac, Despite Security Breach, eBay Posts Profit and Sees Steady Growth, The New York Times Company The New York Times, July 17, 2014. Accessed on: October 12, 2017.
#42 D. Bradbury, How can privacy survive in the era of the internet of things?, Guardian Newspapers Limited The Guardian, April 7, 2015. Accessed on: October 12, 2017.

C. Yahoo! Media Data Set

#2 O. Solon, Yahoo confirms 'state-sponsored' hackers stole personal data from 500m accounts, Guardian Newspapers Limited The Guardian September 23, 2016. Accessed on: October 12, 2017.
#4 A. Hern, Yahoo faces questions after hack of half a billion accounts, Guardian Newspapers Limited The Guardian September 23, 2016. Accessed on: October 12, 2017.
#5 N. Perlroth, Yahoo Hackers Plundered Data on 500 Million, The New York Times Company The New York Times September 23, 2016. Accessed on: October 12, 2017.
#6 H. Tsukayama, C. Timberg & B. Fung, Yahoo hit in world's biggest data breach, Washington Post The Washington Post September 23, 2016. Accessed on: October 12, 2017.
#40 R. McMillan, R. Knutson & D. Seetharaman, New Yahoo Breach Hits 1 Billion Users, Dow Jones & Company, Inc. The Wall Street Journal December 15, 2016. Accessed on: October 12, 2017.
#41 S. Gibbs, Security experts: 'No one should have faith in Yahoo at this point', Guardian Newspapers Limited The Guardian December 15, 2016. Accessed on: October 12, 2017.
#45 N. Olivarez-Giles, Some Steps to Protect Yourself From Hackers, Dow Jones & Company, Inc. The Wall Street Journal December 16, 2016. Accessed on: October 12, 2017.
#46 G. Wells & R. Knutson, Yahoo's Move May Put Deal At Risk, Dow Jones & Company, Inc. The Wall Street Journal December 16, 2016. Accessed on: October 12, 2017.
#49 H. Tsukayama, Yahoo's lag in disclosing hack may come down to lack of knowledge, Washington Post The Washington Post December 17, 2016. Accessed on: October 12, 2017.
#51 S. Solomon, Yahoo, Stable Despite Hacking, Is Still Worthy of Verizon Deal, The New York Times Company The New York Times December 21, 2016. Accessed on: October 12, 2017.
#57 Y. Redrup, Hackers snare MPs in Yahoo breach, Fairfax Media Management Pty Limited The Australian Financial Review January 18, 2017. Accessed on: October 12, 2017.
#76 E. Nakashima, Hackers, Russian spies indicted in Yahoo heist, Washington Post The Washington Post March 16, 2017. Accessed on: October 12, 2017.
#83 S. Adhikari, Firms on notice: no silver bullet for tech werewolves, News Ltd. The Australian March 21, 2017. Accessed on: October 12, 2017.