Impact and Significance of Human Factors in Digital Information Security

Monjur Ahmed[1],
[1]Eastern Institute of Technology, Hawke's Bay, New Zealand,
Email: mahmed@eit.ac.nz
Himagirinatha Reddy Kambam[2],
[2]9Spokes International Limited, Auckland, New Zealand,
Email: himagiri.kambam@gmail.com
Yahong Liu[3],
[3]Eroad Ltd., Auckland, New Zealand,
Email: lyhamy2002@outlook.com
Sapna Jaidka[4],
[4]University of Waikato, Waikato, New Zealand,
Email: sapna.jaidka@waikato.ac.nz
Krassie Petrova[5],
[5]Auckland University of Technology, Auckland, New Zealand,
Email: krassie.petrova@aut.ac.nz

***Abstract*—In this paper, we present a study on the impact and significance of human factors in digital information security. The study focuses on digital data breaches and seeks to find out how human factors within the context of data breaches in cyberspace impact information security. Data breach in cyberspace is a major privacy and security concern that affects the integrity of information security, and thus the underlying reasons for such data breaches demand investigation. An incident of data breach may occur due to several reasons. The root cause for a data breach may yield either from technological or human factors, or both. While technological factors are mostly predictable, human factors may not be. Besides, human factors are dynamic and cannot be fully quantified. This opens the opportunity for an attacker to compromise systems by exploiting human factors. The presented study seeks to find the extent to which human factors are contributors for data breaches. Analyses on 101 real life incidents of data breaches are carried out, and the reasons behind those breaches are explored to understand the implications of human factors in these breaches.**

***Index Terms*—Computing Security, Cybersecurity, Data Breach, Digital Data Breach, Human Factors, Information Security, Social Engineering.**

I. Introduction

IN computing, the advantages come with the price of security breaches and its subsequent impact. The malicious act of compromising personal or organizational data is a cybercrime. Prediction exists that cybercrime will cost approximately $6 trillion per year on average through year 2021 [132]. The cost of cybercrime surges by 62% in five years [34]. Thus, security is a major concern in computing. In computing settings, privacy and security are of utmost importance. All kinds of computing approaches are prone to security breaches and attacks. One such example is Cloud Computing [81]. Cloud Computing is a contemporary computing approach that encapsulates all other computing means [3], implying that considering breaches in Cloud Computing essentially means considering breaches in computing holistically. Though recent emergence of Cloud Computing brings many advantages, security threats and concerns also exist [188]. Incidents of massive data breaches took place in the Cloud or other computing settings. Several factors or reasons may act behind an incident of a data breach. Thus, it is important to realise the driving factors for data breaches. In this paper, we present a study focused on human factors as a reason for data breach.

Threat taxonomy helps to understand the facets from which security concerns may emerge. A taxonomy helps in better understanding of threats through which data breaches may take place; and planning upon such understanding to better safeguard data in cyber space. Efforts to develop threat taxonomy for Cloud Computing exist. Human factors, whether mentioned explicitly or not, are addressed in different Cloud threat taxonomies as one of the reasons for data breaches. For example, a Cloud Threat taxonomy proposed in [4] notes human factor as a major contributing one towards threats in Cloud Computing. Several other examples of human factors as a threat metric are mentioned by [63], [61], [64], and

M. Ahmed, Eastern Insitute of Technology, New Zealand (e-mail: mahmed@eit.ac.nz).
H. R. Kambam, 9Spokes International Limited, New Zealand (e-mail: himagiri.kambam@gmail.com).
Y. Liu, Eroad Ltd., New Zealand (e-mail: lyhamy2002@outlook.com).
S. Jaidka, University of Waikato, New Zealand (e-mail: sapna.jaidka@waikato.ac.nz).
K. Petrova, Auckland University of Technology, New Zealand (e-mail: krassie.petrova@aut.ac.nz).

[168]. [117] argues that enough attention to the effect of human factors on information security is not given, and further research is sought in this regard. [73] assert the importance of studying human factors to fully realise cyber security risks.

In this paper, we present a study on the impact and significance of human factors in information security. The study focuses on digital data breaches and seeks to understand the extent to which human factors are a contributing factor for such breaches. In the rest of the article, we use the term 'data breach' to refer to 'digital data breach'. An incident of data breach may occur for several reasons. While technical factors are mostly predictable, the human factors may be unpredictable. This enables the attackers to compromise systems by exploiting human factors, for example, social engineering. We explore the degree to which human factors contribute towards data breaches. Analyses on 101 real life case studies (incidents) on data breaches are carried out; and the reasons behind those breaches are explored to gain an understanding on the implications of human factors in data breaches.

The rest of the paper is structured as follows: Methodology section outlines the approach used to carry out the study. In Literature review, we describe the concepts of several related terminologies and related work. In the Case Studies section, a summary of the considered incidents of data breaches is described. Findings and discussion on the case studies are presented in Findings and Discussion section.

II. Methodology

We follow an ad-hoc methodology [85], [86] to explore and analyse several real-life scenarios of data breaches. The study is carried out by randomly collecting 101 real life incidents of data breaches from different online news sources. The incidents of data breaches were collected from online news portals yielded by searching using Internet search engines. The keywords used to search incidents of data breach are 'data breaches', 'cloud data breaches', and 'data breach incident'. The considered cases are then analysed to find out the percentage of total data breaches that were caused by human factors. The implications of such human factor related breaches are also analysed and then compared to the overall picture of data breaches in cyberspace, to understand the implications of human factors. The findings help to understand two aspects: the emerging trend of human factors as a reason for data breaches, and whether the implications of Human Factors outweigh the implications of those in other factors. Such understanding eventually helps to focus on human factors with proper level of attention.

To select scenarios as samples of data breaches, the total population considered are the breaches in broader operational context of IT and computing. Random links were chosen from search result returned by search engines. Thus, the total population of the news on breaches are those available on the world wide web and searchable by an Internet search engine. Random Sampling method [138] is followed to select the case studies. The random sampling approach we adapted for the study is also loosely described in [121], [153] and [171]. The quantitative approach of the analysis of causal relationship among variables [42] are used to analyse our findings on the case studies considered.

III. Literature Review

Conducted research to connect human factors to data breaches are somewhat inadequate to date. [117] mention the inadequacy of research on the effect of human factors on information security. [141] asserts that human errors remain a major issue despite of researchers have marked it a significant cause of information security. Besides, [139] suggests that human factors are overlooked in software engineering and development areas. We assume this may lead to poor software development resulting in security loopholes that may aid data breach through social engineering.

In computer security, human factor refers to those characteristics of human beings that can be exploited to gain unfair access to computer systems. This is often done by victimizing a human being and the exploitation goes on without the victim's knowledge. For example, a person might use easily guessable password (e.g. 123456) and an attacker might guess this password to gain unauthorized access. A human factor might be lack of knowledge about computer or IT systems, human error, or it might be related to psychological and behavioural traits of human being. Human is a weak link to keep information secure [141]. As mentioned by [68], human is characterised as the weakest link in cybersecurity by [8], [133], [155], [156]. Human is also mentioned as the weakest link of security by [118].

Human factors are linked to and affect information security management [56]. [4] define human factor as the human-centric actions that pose security threats to computing infrastructure. Human factors from which a Cloud threat may emerge are trust, compliance, regulations, competence, Service Level Agreement (SLA) misinterpretation, and social context [4]. The authors term human factor also as 'soft threat'. [69]mentions factors like 'passive engagement, lack of knowledge, misdirected attention as well as engaging in risky cyber security behaviours' to have potential to increase the chance of a security breach to happen. The human factors are described by [126] as the factors that are "concerned with applying what is known about human behaviour, abilities, limitations, and other characteristics to the design of systems, tasks/activities, environments, and equipment/technologies". [139] explains human factors as factor that can be studied from different perspectives such as psychological, cognitive, management and technical aspects. [152] assert that human factors focus on human being and their interaction with information, machines, materials environment and procedures. [94] define human factors as the study of interrelationship between humans, the tools and equipment they use.

Human factors have relevance with errors and the potential for harm is significant if technology is mishandled [185]. [117] argues that human factors play significant role in computer security. Human factors have tremendous effect on business, information, services and systems [91]. Organisations often

overlook human factors though security depends on it [88]. [157] argues that human factors are unaddressed even though information security is largely a human factor problem. [40] reports human error to be greatest weakness in Information Systems failure. Latest technological improvements in security cannot combat security breaches that arise from carelessness or lack of awareness of the users [38]. Though Internet and related technologies are revolutionary, the use the technology also experience employee-related breaches that affects organisations [46]. According to Kulyk and Volkamer (2018), research found that human factors are a barrier to establish proper security practices among end users.

The significance of human factors in computing security is mentioned in [70], [71], [100], and [119]. The approach to attack using human factors is termed as social engineering [176]. [98] describes social engineering and human conducted attacks and the implications of human-centric attacks. [176] mentions social engineering as 'dark art' and discussed the impact of the attacks based on human factors. [125] defines social engineering as a non-technical method of cyber-attacks that entirely depends on human psychology and involves manipulating people into breaching standard security practices'. [179] mentions social engineering to have profound negative impact and is likely to increase over the course of time. Similar discussions are found in [83], [14], and [134]. [158] classifies social engineering as a serious vulnerability that is highly effective with the ability to bypass all technological protection. [117] confirm the wide acknowledgement of the fact that employees in an organisation are often a weak link when it comes to the protection of information assets. Using state-of-the-art security software and hardware is not a measure against human factors. The recent approach towards cyber-attacks intends to exploit human weaknesses instead of trying to break through security software or hardware [66].

IV. Case Studies

101 case studies or real-life incidents of cybersecurity breaches are collected and analysed. List and brief description of the case studies are in appendix. The case studies are the news of security breaches of different organisations in various business domains/sectors. The case studies are analysed to find out the reason for the breaches and whether the reason is a human factor centric.

V. Findings and Analysis

The summary of findings from the case studies are presented in Table I, Table II, Table III, Table IV, Table V, Table VI and Table VII. The table includes the reasons for breaches for the chosen case studies, and whether the breach was human-centric. A justification is also included in the table outlining why the reason is human-centric or not; the justification is provided only for those breaches that, in our opinion, require further note as justification.

In analysing the facts collected from the selected 101 case studies, the reasons for breaches are explored. The reasons for breaches are categorised as external/internal as well as human

TABLE I
Summary of Breaches

Case Study	Source	Reason(s) for Breach	Human Factor involved?	Justification
Microsoft	[27]	Configuration issue within its Business Productivity Online Suite	Uncertain	This could be an application vulnerability, or poorly configured application.
Dropbox	[27], [55], [17]	Employee using the same password for both DropBox and LinkedIn, and the breach on the former one was possible due to a breach on the latter one.	Yes	
National Electoral Institute of Mexico	[27]	Poorly configured database. Data stored on an insecure and illegally hosted Cloud server situated outside of Mexico.	Yes	Choosing the service is a human decision.
LinkedIn	[27], [159]	Using weak passwords and password reuse.	Yes	
Home Depot	[27], [11], [187]	Vendor's stolen log-on credentials.	Uncertain	
iCloud	[27], [57]	Vendor denied breach, claimed it was account specific targeted attack.	Yes	Based on vendor's claim.
Yahoo	[27], [11], [36]	Using forged cookies.	No	
Phony phone-call on iCloud	[50]	Scam calls to victimise people.	Yes	
Verizon	[136]	Using third party vendor.	Uncertain	
eBay	[11]	Hackers used credentials of corporate employees.	Uncertain	
Uber	[11]	Placing Uber's Cloud server (AWS) account username and password on online code repository GitHub.	Yes	
Deloitte	[28], [79]	System compromised through an unsecured administrator password. Weak password strategy used by administrator, no two-factor authentication.	Yes	
Sage	[90]	Internal login was used for unauthorised access.	Uncertain	
Facebook	[163]	Technical glitch, as claimed by the vendor.	No	
Twitter	[87]	Unusual access patterns across the network, and unauthorised attempts to access user data.	Uncertain	
Adult Friend Finder	[11]	Using weak hashing algorithm.	Yes	

TABLE II
SUMMARY OF BREACHES (CONT'D...)

Case Study	Source	Reason(s) for Breach	Human Factor involved?	Justification
Equifax	[11], [162]	Application vulnerability that the organisaiton failed to address in good time.	Yes	While the application vulnerability may not be human-centric factor, failing to address the issue in good time may be.
TJX	[11], [147]	Using weak hashing algorithm.	Yes	
Scottrade	[24]	Inadequate safeguard by third-party vendor.	Yes	
Fashion Nexus	[33]	A white hat hacker breached company's server.	Uncertain	
Saks and Lord & Taylor	[51], [166]	Malicious software has been installed on the case register system of the stores, likely through phishing emails.	Uncertain	Human Factor-centric, if the breach is through phishing email.
Sanrio	[144], [82]	It might be due to the misconfigured database installation.	Uncertain	
Scribd	[44]	Information stored with an outdated hashing algorithm.	Yes	
Sky Brasil	[1]	Not securing the server with a password.	Yes	
Snapchat	[19], [103]	Application vulnerability – was known to the vendor prior to the breach. SnapChat admitted that the occurred breach was theoretically possible.	Yes	
Stanford University	[9]	Possible software vulnerability – updated version of Wordpress but PhP was not the latest version.	Uncertain	
Staples	[149]	Malware	Uncertain	
SVR Tracking	[37]	Unsecured Amazon S3 bucket	Yes	
Swedish Transport Agency	[5], [18]	Sensitive information shared through clear text email.	Yes	
Sutter Medical Foundation	[177]	Various news providers note the reason as negligence in protecting clients' sensitive information.	Yes	
Network solutions	[97]	Hackers have broken into Web servers	Uncertain	

TABLE III
SUMMARY OF BREACHES (CONT'D...)

Case Study	Source	Reason(s) for Breach	Human Factor involved?	Justification
New York State Electric & Gas	[53]	A software consulting firm employee gained unauthorized access to the database.	Uncertain	
New York Taxis	[173]	New York City released detailed information about every yellow cabs in 2013.	Uncertain	
Newegg	[108], [48]	Hackers injected malicious code on payment webpage.	Uncertain	
Nexon Korea Corp	[145], [76]	Backup server for online game-MapleStory was Hacked.	Uncertain	
NHS (National Health Service)	[93], [47]	Stolen laptops.	Yes	
Nintendo	[99], [45]	The service was hacked.	Uncertain	
NMBS	[49]	Storing data on non-secure server.	Yes	
Nival and km.ru	[52]	Hacking	Uncertain	
Ohio State University	[26]	Unauthorised accessed to server to steal information.	Uncertain	
Orbitz	[39]	The system was poorly monitored and put the data vulnerable.	Yes	
Oregon Department of Revenue	[128]	An employee of uploaded work files to personal cloud storage account.	Yes	Organisational data stored on personal space.
Panerabread	[96]	The database designed in very simple way and able to search on phone numbers.	Yes	
PayAsUGym	[21]	One IT servers was accessed by an unauthorized user.	Uncertain	
Premera	[184], [93]	Hacker broken the system.	Uncertain	
Guest Diagnostics	[72]	Hacker gained access through unsecured mobile App.	Yes	
RBS Worldpay	[114]	Servers hacked.	Uncertain	
Red Cross Blood Service	[112]	File was left unsecured on development website by a contractor employee.	Yes	
River City Media (RCM)	[107], [87]	Due to incorrectly configured Rsync backups, forgotten to put password on this repository.	Yes	
RockYou	[182]	Hacker inject SQL query from webpage to the database, due to website's poor input validation mechanism.	Yes	

TABLE IV
SUMMARY OF BREACHES (CONT'D...)

Case Study	Source	Reason(s) for Breach	Human Factor involved?	Justification
AOL	[35], [170]	Illegal access of data warehouse using another employee's ID	Uncertain	
AOL	[129]	Due to unauthorised access to the user accounts.	Uncertain	
Apple	[122], [135], [140]	Atomic Reference Array vulnerability on JAVA	No	
Apple	[92]	Vulnerability in the Java browser plug-in of developer website	No	
AT&T	[154], [183]	Non implementation of cryptography on employee database	Yes	
AT&T	[151], [89]	Improper Access control or inadequate authorization of customer system	Yes	
British Airways	[25], [32], [22]	Piece of malicious code at point of entry	Uncertain	
British Airways	[111], [174]	Automated attempt from third parties to gain access to accounts using information obtained from elsewhere on the Internet.	Uncertain	
Citigroup	[12], [104]	Lack of anti-Spyware programmes on Website	Yes	
Citigroup	[175]	Inadequate security in shipping the computer tapes.	Yes	
Citigroup Inc.	[146], [58], [95]	Limitations in the technology used for redacting the documents.	No	
Countrywide Financial corp.	[23]	An employee stole the information.	Yes	
Facebook	[148]	Users' victim of make money website scam through fraudulent advertising.	Yes	
Twitter	[54], [43]	Problem in the hashing process.	No	
Yahoo	[10]	Unknown	Yes	
European Central Bank	[78], [59]	Unknown	Uncertain	
Evernote	[16]	Attempt to access secure areas of the company was suspected.	Uncertain	
T-mobile	[101]	Hackers gained unauthorized accessed through API.	No	
Experion/T-Mobile	[130]	An unauthorized party accessed T-Mobile data housed in an Experian server	No	
Firebase	[75]	Misconfiguration of the databases by developers.	Yes	
Formspring	[106], [127]	Poorly secured development server configured to a live database.	Yes	
Gamigo	[142]	Hacker sent link & email addresses and hashes were stolen.	Yes	

TABLE V
SUMMARY OF BREACHES (CONT'D...)

Case Study	Source	Reason(s) for Breach	Human Factor involved?	Justification
Gawker.com	[65]	Hackers used 'brute force attack' to gain access to passwords.	Yes	
Global Payments	[82], [80]	Intruders accessed servers holding the merchant application's information.	Uncertain	
Singapore's Health service	[15]	Hacking attempt	Uncertain	
Health net	[62], [181]	Health Net's IT vendor IBM lost server hard drives.	Yes	
Heartland	[105], [2]	Keylogging malware went through the firewall that captured anything typed on a computer and subsequently sniffer was propagated through the system that was capturing the entire data packets on a network.	No	
HSBC Turkey	[7]	Not mentioned	Yes	
Instagram	[131]	A bug in Instagram API disclosed several user's email addresses and phone numbers.	No	
Interpark	[77]	Hackers fooled staff member through email.	Yes	
Internal Revenue Service	[30], [120]	An online program "Get Transcript" is used.	Yes	
Japan Airlines	[60]	Hackers initiated the breach by sending a malicious email that delivered malware and infected 23 computers. Out of the 23 computers, seven were actually sending data to a server in HongKong.	Uncertain	
Korea Credit Bureau	[167]	The worker who had privilege of accessing several databases copied data onto an external drive.	Yes	
KT Corp.	[**?**], [186]	Hackers created a computer program that penetrates through the KT Corp.'s firewall.	Yes	
Lincoln Medical & Mental Health Center	[6]	Seven CDs containing personal and critical data were lost during shipping via FedEx.	Uncertain	
Living Social	[150]	Unknown	Yes	
Localbox	[160]	A researcher at ZDNet, LocalBox left a large amount of personal data on Amazon S3 storage bucket which could be accessed and downloaded by anyone.	Yes	

TABLE VI
SUMMARY OF BREACHES (CONT'D...)

Case Study	Source	Reason(s) for Breach	Human Factor involved?	Justification
Marriot Hotels	[180], [110]	Hackers had gained an unauthorized access to the Starwood reservation system since 2014.	Yes	
Massachusetts Government	[109]	The virus called W32.QAKBOT was designed by hackers to infiltrate computer networks and allow the attackers to gain access to sensitive data.	Yes	
MBM Company	[137]	IT staff that was managing the archive left the backup exposed online through an unsecured Amazon S3 bucket.	Yes	
Medicaid	[143], [67]	Hackers located in Eastern Europe breached the server which had configuration error.	Yes	
Memorial Healthcare System	[74]	Employees impermissibly accessed the electronic protected health information of individuals by using the login credentials of a former employee of an affiliated physician's office.	Yes	
MyHeritage	[31], [123]	A file named myheritage was found on a private server that contained email addresses and hashed passwords of 92,283,889 users.	Uncertain	
MySpace	[41], [113]	None of the passwords were salted, making it easy to decrypt. No strong passwords containing Uppercase were used.	Yes	
NameTests	[169]	The quizzes were developed by the company that collected personal information from Facebook and displayed it in a JavaScript file that could be easily obtained by malicious third parties.	Yes	
NASDAQ	[124]	Suspicious files were found on the U.S. servers during normal security monitoring.	Yes	
National Security Agency	[102]	WannaCry Ransomware malware is installed on the DoublePulsar tool developed by the National Security Agency which gave remote access to hackers.	Yes	

TABLE VII
SUMMARY OF BREACHES (CONT'D...)

Case Study	Source	Reason(s) for Breach	Human Factor involved?	Justification
Neiman Marcus	[93]	The card-scraping malware was used to collect payment card details.	Yes	
Nemours Foundation	[116]	The data backup tapes were lost.	Partially Yes	
Facebook	[164]	Third party Facebook app developers made records publicly available.	Yes	
Capital One Bank	[115]	Hacker exploited a misconfigured web application firewall. The hacker was an ex-employee of Amazon Web Services, the Cloud Service Provider (CSP) the bank was using.	Yes	A misconfiguration is a human error or incompetence, not a vulnerability of the firewall.

factor-centric and non-human factor-centric. Also, the breaches on IT service-related organisations and non-IT organisations are analysed. We define those organisations as IT service that fall in the category of telecom services, software and hardware related services, and e-commerce organisations.

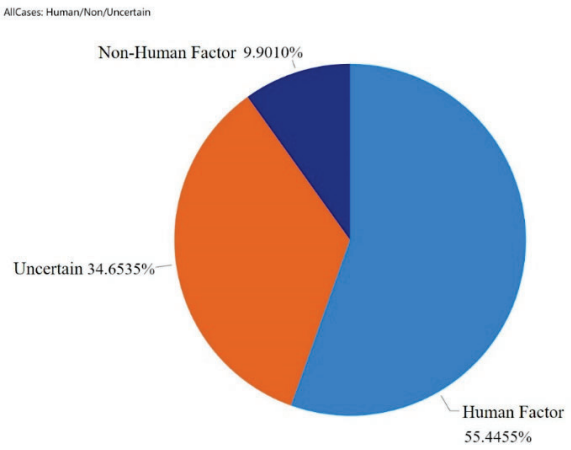

Fig. 1. Human Factor Perspective of Breaches

Fig. 1 shows the reasons for breaches from a human factor-centric perspective. About 55% of all 101 cases are human factor-centric breaches, while about 10% of the cases are due to non-human factor centric reasons. The reasons for about 35% of the breaches are uncertain and requires further information to determine whether they were due to human factor centric causes or not. Fig. 2 illustrates the reasons for breaches for IT service-related organisations of the considered

101 cases. Majority of the breaches (about 57%) in IT organisations are due to human factor related causes, while about 17% of the breaches are due to non-human centric reasons. The reasons for about 26% of the breaches are uncertain and further information is required to decide whether they are due to human factors or not.

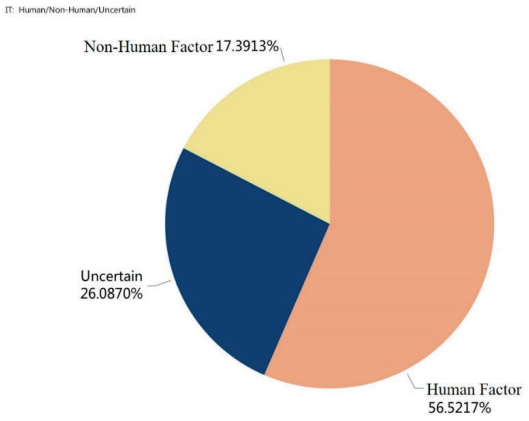

Fig. 2. Human Factor Perspective of Breaches in IT Organisations

For non-IT organisations among the 101 cases considered, about 55% of the cases are due to human factors; while about 4% are due to non-human factors and about 42% of the breaches on non-IT organisations require further information to decide whether the breaches are related to human factors. This is depicted in Fig. 3.

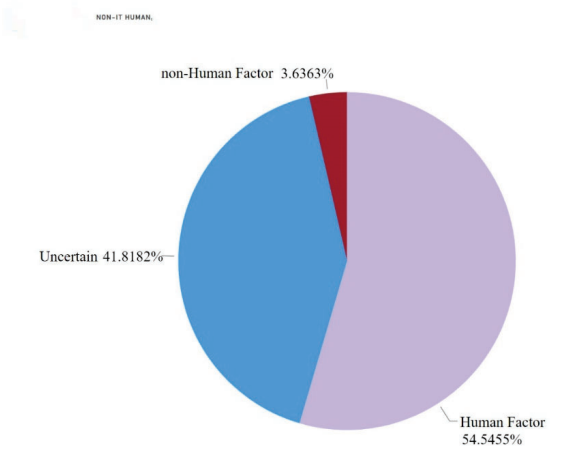

Fig. 3. Human Factor Perspective of Breaches in non-IT Organisations

The reason for a breach for an organisation may emerge from within the context of the respective organisation (internal cause), or from outside sources (external cause). Considering this viewpoint, about 53% of all breaches considered are due to external sources where about 47% of the breaches are for internal causes, as illustrated in Fig. 4.

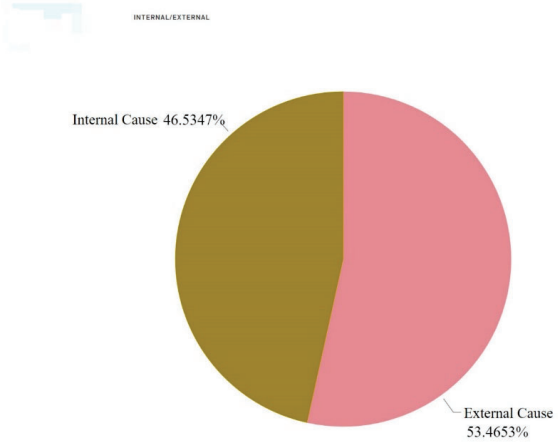

Fig. 4. Ratio of Internal/External Causes for All Breaches

Narrowing down the internal/external causes for human factor-centric breaches only, the findings are that, about 52% of the human factor-centric breaches are due to internal factors and the rest are due to external causes. This is illustrated in Fig. 5.

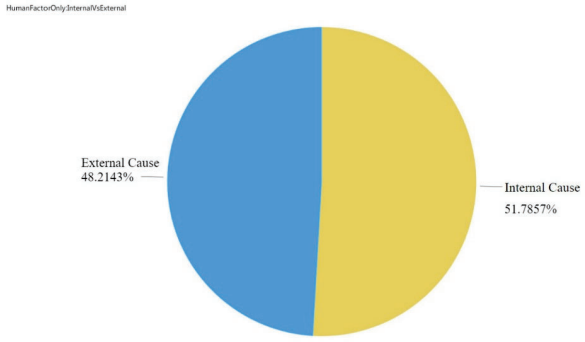

Fig. 5. Ratio of Internal/External causes for Human Factor-centric Breaches Only

Taking the internal/external causes for breaches into account for IT and non-IT organisations, we found about 54% of the breaches in IT organisations are for external causes and the rest are for internal causes. On the other hand, about 53% of the breaches in non-IT organisations are due to external causes and the rest are due to internal causes. The above are illustrated in Fig. 6 and Fig. 7 respectively. Finally, as Fig. 8 shows, about 54% of all the cases considered are non-IT organisations and about 46% are IT organisations.

Table VIII and Table IX summarises the above findings. In Table VIII summarises the percentage of Human Factor centric breaches for all breaches considered in the study (i.e., all 101 case studies), as well as IT and non-IT organisations from the total breaches considered. On the other hand, Table IX summarises the breaches on different categories based on internal or external factors as the perceived causes of breaches

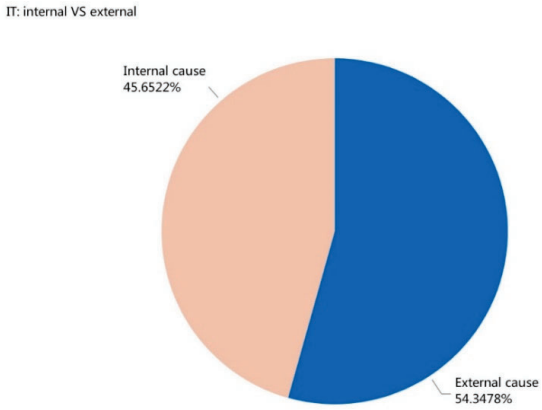

Fig. 6. Ratio of Internal/External causes for Breaches in IT Organisations

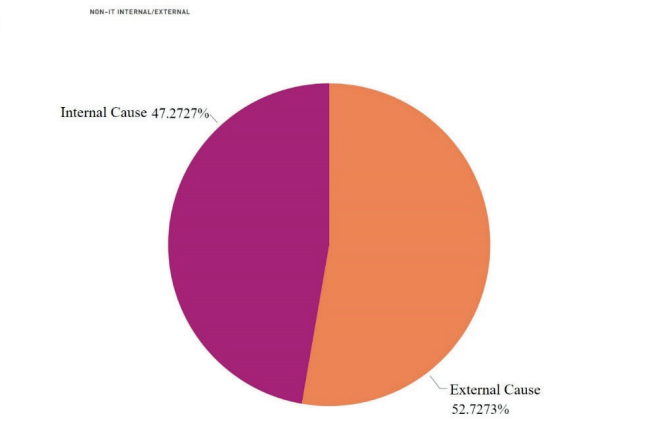

Fig. 7. Ratio of Internal/External causes for Breaches in non-IT Organisations

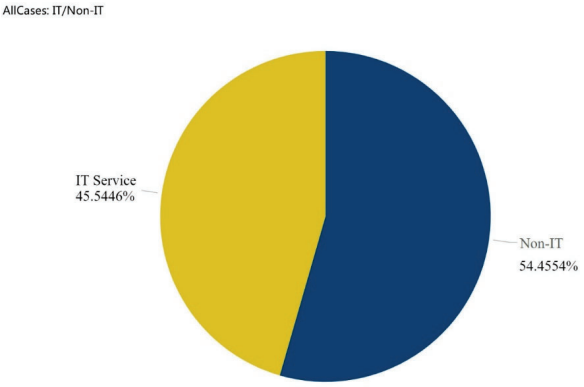

Fig. 8. Ratio of all Breaches in IT and non-IT Organisations

considered.

TABLE VIII
SUMMARY OF FINDINGS ON HUMAN FACTOR CENTRIC BREACHES.

Type of Organisation	Percentage of Human Factor centric Breaches
All (for all 101 case studies)	55.45%
IT	56.52%
Non-IT	54.55%

TABLE IX
INTERNAL AND EXTERNAL CAUSES AS CONTRIBUTING FACTORS FOR THE BREACHES.

Category of Breaches/Industry	% of Breaches (due to Internal cause)	% of Breaches (due to External cause)
All (for all 101 case studies)	46.53%	53.47%
Human Factor centric Breaches	51.79%	48.21%
IT Organisations	45.65%	54.35%
Non-IT Organisations	47.27%	52.73%

VI. DISCUSSIONS

Human Factors are the reasons for majority of the breaches in considered 101 cases. More breaches may be linked to human factors, since a notable portion of breaches need further information and analysis to decide whether they are due to human factors. For both IT and non-IT companies, human factor centric breaches dominate over non-human factor related breaches. The reasons behind some breaches either cannot be determined or there is insufficient information to ascertain the reason for the breach. Both the inability to detect the reason and the lack of sufficient information warrants investigation.

The cause of breaches may be sourced from both internal or external sources and neither of the causes is insignificant when compared to the other. This also holds true when considering only human factor-centric breaches, as well as considering breaches in IT and non-IT organisations. While external factors may not be controllable, the internal factors behind data breaches can be minimised and further research required on this.

Human factors-centric breaches affect across variety of business domain including IT businesses. This may put one under the impression that human factors imply factors well beyond mere incompetence. It is important to find the loophole to minimise human-centric breaches. If competence (or lack of competence thereof) is taken into consideration, could a conclusion be drawn that incompetence results in human related breaches in both large and small organisation that are either IT or non-IT business? If not regardless, is the recruitment process flawed? Is there lack of ample level of training and awareness? If people are competent, what are the reasons for a person to be the reason for human-centric attack? Is it work-life balance, work environment or other

aspects that may lead to people making mistakes (where incompetence is not a factor) that may lead to a security breach? Is the security programme and risk management of an organisation being contributors towards human factor-centric breaches? Finding whether a breach is human related or not is crucial, so is the answers to the above questions. Otherwise, an organisation may result is having flawed security analysis and poor gap analysis resulting in developing an ineffective security programme.

VII. Conclusions and Future Developments

While technological factors may be predictable, human factors are not due to their dynamicity. Human factors are unstructured and entirely context dependent. It may be argued that proper training and awareness can effectively battle with human factor related attacks. But, since it fits into no framework and hard to predict, threats that emerge from human factors are likely to remain as an open challenge in all form of computing.

The findings presented is a preliminary foundation to further research. Seeking answers to the questions mentioned in Discussions section would extend our current study. In the case studies considered, several attacks are due to human errors by the professionals who manage their respective cyberspace and/or their own organisational computer networks, not by the end-users who may not be competent in using IT/IS systems. The reason for unexpected mistakes (negligence? incompetence? other job-related factors?) by the professionals warrant investigation and research. The possibility for such mistakes to be linked with work pressure and overall wellbeing of the employees needs research focus. The cost of cybercrime is significant. Thus, it may be safe to say that, addressing the human factors to any extent required would cost far less than the loss occurs as a result of data breaches.

The research presented may be extended to include a study representing insights into poor handling of smartphone applications and thus exploring significance of human factors in breaches through smartphones. Another future reasearch that may emerger as the motivation from this research is to find mitigating ways to minimise impact of human factors which may include (but not limited to) exploring the option of resilience through using decentralised architecture (e.g. BlockChain). Additionally, research on ways to increase Cyber Security awareness among people to minimise imapct of human factors is another area where the presented research may seerve as a motivational factor.

APPENDIX: List of Case Studies

The randomly selected 101 case studies are real life incidents of Cloud and/or data breaches that are published on online portals. Brief descriptions of the case studies are listed below.

- Microsoft: A breach in 2010 due to a configuration issue in its Business Productivity Online Suite resulting in unauthorised access to employee contact info [27].
- Dropbox: In 2012, hackers accessed DropBox's 68 million user accounts including their email addresses and passwords [27], [55], [17]. The reason for the breach was using same password by an employee for both DropBox and LinkedIn [55].
- National Electoral Institute of Mexico: 93 million of voter of the National Electoral Institute of Mexico were compromised in April 2016. It was due to poorly configured database. The institute stored its data on an insecure and illegally hosted Cloud server situated outside of Mexico [27].
- LinkedIn: In 2012, LinkedIn breach resulted in 6 million user passwords being stolen. In 2016, LinkedIn suffered another breach where 167 million of users' emails and passwords were stolen [27]. The reason for the breaches is claimed to be using weak passwords and password reuse [159].
- Home Depot: DIY retailer Home Depot's point-of-sale terminals at the self-checkout were exploited for months in 2014. This affected 56 million credit cards and was the biggest breach of its kind at that time [27], [11], [187].
- iCloud: The breach in 2014 on Apple's cloud storage iCloud meant leaked pictures of its celebrity users [27]. Apple denied it to be architecture-wide breach, but rather is a targeted attack on celebrity accounts that used weak passwords [57].
- Yahoo: In 2013, a breach on Yahoo's network resulted in disclosing information (e.g. name, email, date of birth) of more than a billion of user accounts [27], [11]. Yahoo claimed that it was carried out using forged cookies [36].
- Phony phone-call: An attempt by fraudsters to capitalise the iCloud breach and launching scam calls to gain advantage by fooling people [50].
- Verizon: Data breach in 2017 (exposed 14 million customer accounts) was due to the management of Verizon data by NICE Systems, a third-party vendor [136].
- eBay: The attack in 2014 exposed 145 million users' names, addresses, dates of birth and encrypted password. According to eBay, the hackers got into their system using credentials of their employees to access to eBay network [11].
- Uber: In 2016, personal information of 600,000 drivers and 57 million users were exposed. The breach was due to placing Uber's Cloud server (AWS) account username and password on online code repository GitHub [11].
- Deloitte: Global consultancy firm Deloitte had its clients' personal information hacked and exposed in 2017. The system was compromised through an unsecured administrator password [28], [79].
- Sage: UK based accounting firm Sage was affected in 2016. An internal login was used for unauthorised access to employees' data of 300 UK firms [90].
- Facebook: Facebook 'exposed 6 million users' phone numbers and email addresses to unauthorized viewers', due to technical glitch (as claimed by Facebook) [163].
- Twitter: Twitter's 250,000 user accounts were hacked in 2013. The company suggested that they were aware on the incident upon detecting 'unusual access patterns

across the network and had identified unauthorised attempts to access user data that had led to accounts being compromised' [87].
- AFF: "Hackers collected 20 years of data … Most of the passwords were protected only by the weak SHA-1 hashing algorithm ..." [11].
- Equifax: An application vulnerability exposed about 147.9 million consumers' data [11]. The reason was a flaw that could be patched weeks before the attack [162].
- TJX: A breach on a portion of its network exposed credit card, debit card, check and merchandise transactions [147]. One claim state that a group of hackers took advantage of a weak data encryption system, though different claims exist [11].
- Scottrade: A third-party data breach inadvertently exposed 20,000 of its customers' non-public information. One of Scottrade's vendors, Genpact's employee uploaded Scottrade's database to an Amazon-hosted SQL server. It is revealed that the worker didn't take adequate safeguards to lock down the server [24].
- Fashion Nexus: 650,000 fashion shoppers' details including email and home addresses was exposed by a white hat hacker who breached company's web server" [33].
- Saks and Lord & Taylor: More than 5 million bank cards exposed. Hackers installed malicious software on payment register systems at affected stores. [51] [166].
- Sanrio: 3.3 million accounts exposed from a database containing information about first and last names, birthday, gender, country of origin, email addresses, hashed passwords, password hint questions and their corresponding answers [144], Rogers, 2015).
- Scribd: Usernames, encrypted passwords and email addresses of 50 million users were accessed [44].
- SKY Brasil: 32 million of its users' data leaked that revealed names, addresses, phone numbers, birth dates, client IP address, payment method and encrypted password [1].
- Snapchat: Usernames, phone numbers of 4.6 million Snapchat accounts had hacked [19]; [103].
- Stanford University: Website of a centre of the university remained compromised for several months [9].
- Staples: 1.16 million customer credit card breach [149]
- SVR Tracking: 540,000 users' data including personal information accidentally made available to the public in its Amazon bucket [37].
- Swedish Transport Agency: Personal information and data related to defence plans exposed online [5], [18].
- Sutter Medical Foundation: Computer containing about 3.3 million patients' information was stolen [177].
- Network solutions: In 2009, about 50 sites of the company hosts have been comprised. Hackers took accounts information of more than 573,000 debit and credit cards [13].
- New York State Electric & Gas: The companies' customer information system has been accessed by unauthorized software consulting firm employee in 2012. It exposed 1.8 million customers' information [53].
- New York Taxis: New York City has release data of 173 individual taxi trips in 2013 without proper anonymise of drivers' license number and taxi number [173].
- Newegg: In 2018, hackers injected 15 lines of code on Newegg's payment webpage. The hackers stayed on the webpage for more than one month. On average more than to skim the credit card information of customer [108], [48].
- Nexon Korea Corp: Hacker attacked the database of South Korea's leading game developer-Nexon Korea Corp in 2011. That caused breach of personal data of its online game Maple Story's 13.2 million subscribers [145], [76].
- NHS (National Health Service): A senior hospital manager lost a laptop computer containing unencrypted Health Service records of more than 20,000 patients when he was on holiday in 2008. Followed by several laptops stolen from St George's hospital in London and Wolverhampton. A disc containing almost 1,000 emergency call went missing by courier company [47].
- Nintendo: Japan's Club Nintendo service was hacked in 2013. Customer information compromised in the attack includes full name, phone numbers and home & email address [45].
- NMBS: Due to mistake of a data worker in 2013, thousands of customer information from rail authority NMBS open online [49].
- Nival and km.ru: In 2016, a teenage hacker breached random Russian websites as revenge for the MH17 crash. The victims were about 1.5 million [52].
- Ohio State University: In 2010, hackers had broken into their server that stored about 760,000 people's personal information. That could cost the university USD$4 million [26].
- Orbitz: Credit information of 880,000 customers breached that belongs to Travel booking website Orbitz in 2018 [39].
- Oregon Department of Revenue: In 2018, due to a mistake of an employee, 36,000 people's information of Revenue includes names, addresses and Social Security numbers might be exposed [128].
- Panerabread: In 2018, the web site of American chain restaurants, Panerabread, leaked millions of customer records [96].
- PayAsUGym: Their servers was hacked in 2016, the organization admitted that 300,000 members' financial details were stolen [21].
- Premera: Premerra announce a major breach in 2015, 11 million customers' medical and financial data may have exposed due to this attack [184].
- Guest Diagnostics: Digital intruders stole about 34,000 people's personal and medical information from this medical laboratory company in 2016 [72].
- RBS Worldpay: Royal Bank of Scotland admitted that its computer system was hacked in 2008. About 1.5 million cardholders may have been affected by this breach [114].

- Red Cross Blood Service: Due to mistake of a third-party provider in 2016, Australia Red Cross Blood Service experienced data breach that affected 550,000 donors [112].
- River City Media (RCM): RCM is notorious spam operator. Due to the incorrectly configured Rsync backup, 1.37 billion identity were leaked in 2017 [107].
- RockYou: In 2009, the social network App company Rockyou suffered a major security breach due to attack. That exposed 30 million accounts' information [182].
- AOL: 92 million AOL customer account "screen names", zip codes, telephone numbers were stolen by former AOL employee. With his inside knowledge of AOL system accessed data warehouse using another employee's ID [35], [170].
- AOL: Up to 2 percent of AOL's millions of user's information were hacked in 2014. User's accounts were compromised by unauthorised access to send out spam messages [129].
- Apple: In 2012, Antisec claims to have snatched 12 million Apple device ID's from FBI Agent. Posted 1 million of identifiers to the web. During the shell session a file was downloaded from FBI Agent's Desktop folder using the Atomic Reference Array vulnerability on JAVA [122], [135], [140].
- Apple: In 2013, Apples' Developers portal hacked and about 270,000 registered third-party developers information stolen. Hacker able to install malware on developer Mac computers through the vulnerability in the Java browser plug-in of developer portal [92].
- AT&T: In 2007, a laptop was stolen from a car that holds information of unspecified number of current and former employees of AT&T comprise of Social Security numbers, names and other personal details [154]. Employee data exposed because of unencrypted information [183].
- AT&T: During 2013 and 2014, employees at three call centres used by AT&T accessed more than 68,000 accounts that had without adequate authorization. This leads to the breach of about 280,000 US customers' names and Social Security Numbers(fully/partially) [151], [89].
- British Airways (BA): BA website and mobile app hacked in 2018, compromised 380,000 British Airways passengers' personal information and financial information including credit card numbers, expiry dates, CVV numbers [25]. Hackers run the malicious code at point of entry on to the BA website [32], [22].
- British Airways: In 2015, thousands of British Airways frequent -flyer executive club accounts had breached. Attack was due to an automated computer program that searches for vulnerabilities, Guardian claimed [111], [174].
- Citigroup: In May 2011, cyber-attack on Citigroup bank compromised 360,083 credit card accounts which is 1 percent of its North American accounts. This attack resulted in a loss of $2.7 million. Hackers used spyware for hacking, Experts said [12], [104].
- Citigroup: 3.9 million U.S customers personal data was lost from CitiFinancial, the consumer finance division of CitiGroup Inc. in 2005. It was occurred while shipping the computer tapes in a box through UPS Inc. This personal data includes account information, Social Security numbers and payment histories [128], [175].
- Citigroup Inc: In 2013, the Citigroup exposed the personal information (that includes date of birth and Social Security Numbers) of around 150,000 customers who had filed for bankruptcy between 2007 and 2011 due to a limitation in the technology they have been using for editing the documents [58], [95], [146].
- Countrywide Financial corp.: Former senior financial advisor of Countrywide Financial Corporation stolen confidential information of millions of customers and sold it to a third party for marketing purposes [23].
- Facebook: Facebook Inc was hacked by a spammer to gain access to the personal information of 30 million users. Hackers made use of 400,000 accounts to gain the access tokens that are used by Facebook users to log into their accounts without typing passwords [148].
- Twitter: 330 million Twitter users were asked to change their passwords because the passwords were saved in plain text instead of random string of characters [43]; [54].
- Yahoo: In a 2014 data breach, 500 million user's information was exposed [10].
- European Central Bank: Approximately 20,000 email addresses, phone numbers and addresses in unencrypted format were stolen from the European Central Bank's database website that was used by people to register for events in bank [78], [59].
- Evernote: In 2013, Evernote revealed a breach in which user names, email addresses and password in encrypted format were accessed by a hacker [16].
- T-mobile: Upto 2 million customers' information that included their name, billing zip code, contact number and mobile account type was leaked in 2018 [101].
- Experion/T-mobile: Personal information of about 15 million T-mobile customers was exposed by a data breach at Experion in 2015 [130].
- Firebase: Over 100 million people's personal data records were exposed that included passwords and usernames, GPS records, Bitcoin transactions and Facebook and LinkedIn tokens. This happened due to poor configuration of online databases by the application developers [75].
- Formspring: 420,000 encrypted passwords were posted online ([106], [127].
- Gamigo: Over 8 million email addresses and encrypted passwords were leaked [142].
- Gawker.com: Company's website was hacked and a file containing company's source code, hundreds of thousands of email addresses and passwords and internal conversations between staff members was uploaded on 4Chan [65].
- Global Payments: 1.5 million payment cards information

was hacked in 2012. Company had to pay heavy fines and provide insurances to affected customers [82], [80].

- Singapore's Health service: About 1.5 million people's personal information including their names, national ID card number, address, gender, race and date of birth were stolen from Singapore's health service. The target of the hacker was Prime Minister Lee Hsien Loon's particulars and information about his medications [15].
- Health net: In 2011, nine server drives were found missing that contained 1.9 million customers personal and health data. The data center was managed by IBM [62], [181].
- Heartland: In 2008, Heartland Payments Systems suffered a breach as Intruders manages to get access to the system. Around 130 million customers were affected [105], [2].
- HSBC Turkey: About 2.7 million HSBC Turkey customers' credit cards were compromised in a breach in 2014 [7].
- Instagram: In 2017, around 6 million Instagram user's email addresses and phone numbers were hacked due to a bug in the API [131].
- Interpark: In 2016, over 10 million user's personal information that included the names, addresses, email addresses, date of births and phone numbers was compromised as hacker managed to get access of an employee's computer [77].
- Internal Revenue Service (IRS): More than 700,000 social security numbers and other sensitive data were stolen as hackers managed to get access to the "Get Transcript" application of the IRS which was used by taxpayers to look and download their last few years' tax filing information. This feature was suspended after discovering the beach [30], [120].
- Japan Airlines: In 2014, personal data of approximately 190,000 customers were stolen that included names, date of births, genders, home addresses, work addresses, job titles, phone numbers, fax numbers, email addresses, Japan Airline Mileage Bank membership numbers and enrolment dates [60].
- Korea Credit Bureau: 20 million South Koreans' personal data that included identification numbers, addresses and credit card numbers was stolen by a worker who got access to various databases of the company [167].
- KT Corp.: Personal information of 8.7 million KT Corp. users was stolen and sold. Stolen information included names, mobile phone numbers, membership numbers, personal identification number and mobile phone serial number of each subscriber [**?**], [186].
- Lincoln Medical & Mental Health Center: Seven CDs containing personal and critical data that included name, address, Social Security Number, medical record number, patient number, health plan information, date of birth, dates of admission and discharge, diagnosis information and some driver licence numbers were lost in transport [6].
- Living Social: Personal information of more than 50 million people was compromised as the servers got hacked. The hacked information included the names, email addresses, birthdates and encrypted passwords of LivingSocial customers [150].
- Localbox: In 2018, a Weshington-bases data firm company, LocalBox was held responsible for breaching personal data for 48 million user profiles [160].
- Marriot Hotels: Around 500 million guest's personal and financial data was compromised. The Starwood reservation system was hacked since 2014 but was not identified till 2018 [180], [110].
- Massachusetts Government: In 2011, 1500 computer systems belonging to the departments of Unemployment Assistance and Career Services of the Massachusetts Executive Office of Labor and Workforce Development were compromised. Personal information of 210,000 people was exposed. The exposed information included names, Social Security numbers, employer identification numbers, email addresses, home addresses and bank information [109].
- MBM Company: Personal information of more than 1.3 million customers was made public. Information included customers' names, addresses, zip codes, phone numbers, email addresses, IP addresses, passwords in plain text, internal company mailing lists, credit card details in encrypted format, payment details, promo codes and item orders [137].
- Medicaid: In 2012, 500,000 personal records with less sensitive data and 280,000 personal records with Social Security numbers were stolen. The affected customers are those who had visited the healthcare in the past four months of this breach [143], [67].
- Memorial Healthcare System: Protected health information of 115,143 individuals had been compromised by the employees. The information included individuals' names, date of births and Social Security numbers. Former employee's login credentials had been used to access the electronic protected health information maintained by Memorial Healthcare System [74].
- MyHeritage: Email addresses and hashed passwords of 92,283,889 users of MyHeritage was discovered on a private server outside of MyHeritage [31], [123]
- MySpace: A social networking website MySpace suffered a breach in 2016. 360 million credentials containing 427 million encrypted passwords were compromised [41], [113].
- NameTests: Facebook quizzes developer NameTests exposed personal information of 120 million Facebook users. The quizzes were collecting personal information of users, like names, date of births, photos and friend lists and displaying then in a JavaScript file, one that could be easily accessed by malicious third parties [169].
- NASDAQ: Nasdaq OMX group that owns the Nasdaq stock market got their servers hacked in the U.S. [124].
- National Security Agency: Individuals and organization from more than 150 countries were affected by WannaCry

RansomWare malware. National Security Agency was one of them. Hacker steal their cyber security tool and installed the malware by which hackers got control over their systems [102].

- Neiman Marcus: 40 million payment card details were compromised. Out of those 9200 cards were used to make fraudulent purchases. Hacker got access to the names, contact information, purchase histories and the last four digits of payment card numbers [93].
- Nemours Foundation: The Nemours Foundation, a health care organization that runs children's hospitals has lost 1.05 million records [116].
- FaceBook: In one of the breaches in 2019, more than 540 million records were publicly exposed. Third-party Facebook app developers exposed users' data including account names, details about comments and reactions to posts [164].
- CapitalOne Bank: The 2019 breach at Capital bank resulted in unauthorized access to 100 million credit card applications and accounts [115]. According to the bank, the exposed customer data are credit scores, credit limits, balances, payment history, contact information, and other data in credit card application [29].

REFERENCES

[1] R. Abel. Sky Brasil exposes data of 32M customers on ElasticSearch — SC Media. Retrieved from https://www.scmagazine.com/home/security-news/sky-brasil-one-of-the-biggest-subscription-television-services-in-brazil-is-the-latest-elasticsearch-server-user-to-leave-its-customers-exposed-after-not-securing-the-server-with-a-password/, 2018.

[2] B. Acohido. Hackers breach heartland payment credit card system. Retrieved from https://abcnews.go.com/Business/PersonalFinance/story?id=6695611page=1 2009

[3] M. Ahmed. Ki-Ngā-Kōpuku: A Decentralised, Distributed Security Model for Cloud Computing. PhD Thesis. Auckland University of Technology, New Zealand, 2018.

[4] M. Ahmed, and A. T. Litchfield. Taxonomy for Identification of Security Issues in Cloud Computing Environments, Journal of Computer Information Systems (JCIS), DOI: 10.1080/08874417.2016.1192520, 2016.

[5] C. Anderson. Swedish Government Scrambles to Contain Damage From Data Breach - The New York Times. Retrieved from https://www.nytimes.com/2017/07/25/world/europe/ibm-sweden-data-outsourcing.html, 2017

[6] H. Anderson. Breach stems from lost fedex shipment. Retrieved from https://www.healthcareinfosecurity.com/breach-stems-from-lost-fedex-shipment-a-2709, 2010.

[7] Ankara. HSBC turkey hacked for credit card information. Retrieved from http://www.hurriyetdailynews.com/hsbc-turkey-hacked-for-credit-card-information-74274, 2014.

[8] M. Anwar, W. He, I. Ash, X. Yuan, L. Li, and L. Xu. Gender difference and employees' cybersecurity behaviors. Computers in Human Behavior, 69, 437–443. doi:10.1016/j.chb.2016.12.040, 2016.

[9] I. Arghire. Stanford University Site Hosted Phishing Pages for Months. Retrieved from https://www.securityweek.com/stanford-university-site-hosted-phishing-pages-months, 2017.

[10] L. Armasu. Yahoo data breach exposed 500 million accounts in 2014. Retrieved From https://www.tomshardware.com/news/yahoo-data-breach-500-million,32745.html, 2016.

[11] T. Armerding. The 17 biggest data breaches of the 21st century, https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html, 2018.

[12] M. Aspan, and K. Soh. Citi says 360,000 accounts hacked in May cyber attack - Reuters. Retrieved from https://www.reuters.com/article/us-citigroup-hacking/citi-says-360000-accounts-hacked-in-may-cyber-attack-idUSTRE75F17620110616, 2011

[13] B. Kerb. Security Fix – Network Solutions Hack Compromises 573,000 Credit, Debit Accounts. Retrieved from http://voices.washingtonpost.com/securityfix/2009/07/network_solutions_hack_comprom.html, 2009.

[14] T. Bakhshi, M. Papadaki, and S. M. Furnell. A Practical Assessment of Social Engineering Vulnerabilities, Proceedings of the Second International Symposium on Human Aspects of Information Security & Assurance (HAISA 2008), pp. 12–23, 2008.

[15] C. Baynes. Hackers steal 1.5 million people's personal data in cyber-attack on singapore's health service. Retrieved from https://www.independent.co.uk/news/world/asia/singapore-personal-data-hack-health-database-government-millions-people-a8456111.html, 2018.

[16] BBC. Evernote says security has been breached by hackers. Retrieved from https://www.bbc.com/news/technology-21644317, 2013.

[17] BBC. Dropbox hack 'affected 68 million users', http://www.bbc.com/news/technology-37232635, 2016.

[18] BBC. Sweden Data Leak 'a disaster', says PM. Retrieved from: https://www.bbc.com/news/technology-40705473, 2017.

[19] BBC News. Snapchat hack affects 4.6 million users - Retrieved from https://www.bbc.com/news/technology-25572661, 2014.

[20] BBC News. World-Check terrorism database exposed online -Retrieved from https://www.bbc.com/news/technology-36662612 , 2016.

[21] BBC News. PayAsUGym hack exposes members' card details - Retrieved from https://www.bbc.com/news/technology-38382687, 2016.

[22] BBC News. British Airways breach: How did hackers get in? - BBC News. Retrieved 20 August 2019, from https://www.bbc.com/news/technology-45446529, 2018.

[23] L. Bell. Countrywide notifies customers of data breach with direct mail. Retrieved from https://www.dmnews.com/data/news/13063971/countrywide-notifies-customers-of-data- breach-with-direct-mail, 2008.

[24] D. Bisson. Scottrade Confirms Third-Party Data Breach Exposed 20,000 Customers' Private Data, https://www.tripwire.com/state-of-security/latest-security-news/scottrade-confirms-third-party-data-breach-exposed-20000-customers-private-data/, 2017.

[25] J. Bishop. 380,000 Passengers Affected By 'Malicious' British Airways Hack. Retrieved 20 August 2019, from https://www.forbes.com/sites/bishopjordan/2018/09/09/british-airways-hacked/#1918b83c67ae , 2018.

[26] R. Book, J. Jurich, and A. Marotti. Hacked: Data breach costly for Ohio State, victims of compromised info, The Lantern. Retrieved from https://www.thelantern.com/2010/12/hacked-data-breach-costly-for-ohio-state-victims-of-compromised-info/, 2010.

[27] C. Bradford. 7 Most Infamous Cloud Security Breaches, https://www.storagecraft.com/blog/7-infamous-cloud-security-breaches/, 2018.

[28] M. Burgess. That Yahoo data breach actually hit three billion accounts, http://www.wired.co.uk/article/hacks-data-breaches-2017, 2017.

[29] CapitalOne. Information on the Capital One Cyber Incident. Retrieved from: https://www.capitalone.com/facts2019/, 2019.

[30] CBC. Massive irs data breach much bigger than first thought. Retrieved from https://www.cbsnews.com/news/irs-identity-theft-online-hackers-social-security-number-get-transcript/ , 2016.

[31] A. Chen. Why a DNA data breach is much worse than a credit card leak. Retrieved from https://www.theverge.com/2018/6/6/17435166/myheritage-dna-breach-genetic-privacy-bioethics, 2018.

[32] R. Chirgwin. British Airways: If you're feeling left out of our 380,000 passenger hack, then you may be one of another 185,000 victims • The Register. Retrieved 20 August 2019, from https://www.theregister.co.uk/2018/10/25/british_airways_september_hack_update/, 2018.

[33] T. Clark. Data hacked at web provider Fashion Nexus. https://www.drapersonline.com/news/data-hacked-at-web-provider-fashion-nexus/7031553.article, 2018.

[34] CIO New Zealand. Cost of Cybercrime Surges by 62 Percent in 5 years. Available at: https://www.cio.co.nz/article/643097/cost-cybercrime-surges-by-62-per-cent-5-years/, 2018.

[35] CNN Money. AOL worker arrested in spam scheme. Retrieved from: https://money.cnn.com/2004/06/23/technology/aol_spam/, 2004.

[36] J. Condliffe. A History of Yahoo Hacks, https://www.technologyreview.com/s/603157/a-history-of-yahoo-hacks/, 2016.

[37] H. Daitch. SVR Tracking Leak - 500,000 Vehicles Left Unsecured — IdentityForce®. Retrieved from https://www.identityforce.com/blog/svr-tracking-leak, 2017.

[38] D. Danchev. Reducing "Human Factor" Mistakes. Available at: http://techgenix.com/reducing_human_factor_mistakes/ , 2006.

[39] D. Deahl. Orbitz says a possible data breach has affected 880,000 credit cards - The Verge. Retrieved from https://www.theverge.com/2018/3/20/17144482/orbitz-data-breach-credit-cards, 2018.

[40] Deloitte. Protecting what matters. 6th Annual Global Security Survey. available at: https://www.iasplus.com/en/binary/dttpubs/2009securitysurvey.pdf , 2009.

[41] A. Dellinger. More than 427 million myspace passwords might have just been leaked. Retrieved from https://www.dailydot.com/debug/myspace-database-hack-leakedource/, 2016.

[42] N. K. Denzin, and Y. S. Lincoln. Collecting and interpreting qualitative materials (Vol. 3). Sage, 2008.

[43] N. Douglas. How twitter's password screwup might have happened. Retrieved from https://www.lifehacker.com.au/2018/05/how-twitters-password-screwup-might-have-happened/ , 2018.

[44] P. Ducklin. Scribd, "world's largest online library," admits to network intrusion, password breach – Naked Security. Retrieved from https://nakedsecurity.sophos.com/2013/04/05/scribd-worlds-largest-online-library-admits-to-network-intrusion-password-breach/ , 2013.

[45] Emilygera. Club Nintendo hacked in Japan. Retrieved from https://www.polygon.com/2013/7/5/4495374/club-nintendo-hacked-in-japan, 2013.

[46] M. Evans, L. A. Maglaras, Y. He, and H. Janicke. Human Behaviour as an aspect of Cyber Security Assurance. Security and Communication Networks, Volume 9 Issue 17, November 2016, Pages 4667-4679, 2016.

[47] J. Fernandez. NHS manager suspended after losing laptop — Digital Health. Retrieved from https://www.digitalhealth.net/2008/07/nhs-manager-suspended-after-losing-laptop/, 2008.

[48] J. Fingas. Newegg fell victim to month-long card skimming hack. Retrieved from https://www.engadget.com/2018/09/19/newegg-credit-card-skimming-hack/ , 2018.

[49] Flanders Today. NMBS data leak was breach of privacy — Retrieved from http://www.flanderstoday.eu/business/nmbs-data-leak-was-breach-privacy , 2013.

[50] Fleishman, G. (2017). Ignore that call from "Apple" about an iCloud breach, https://www.macworld.com/article/3185485/security/ignore-that-call-from-apple-about-an-icloud-breach.html, 2017.

[51] T. Foltýn. Saks and Lord &; Taylor stores suffer data breach exposing five million bank cards — WeLiveSecurity. Retrieved 20 July 2019, from https://www.welivesecurity.com/2018/04/05/saks-lord-taylor-stores-breach-cards/ , 2018.

[52] F. Lorenzo. A Teen Hacker Is Targeting Russian Sites as Revenge for the MH17 Crash - VICE. Retrieved from https://www.vice.com/en_us/article/pgkp57/a-teen-hacker-is-targeting-russian-sites-as-revenge-for-the-mh17-crash, 2016.

[53] GCN. Data breach exposes info on NY utility customers – Retrieved from https://gcn.com/articles/2012/01/25/agg-ny-utilities-data-breach.aspx , 2012.

[54] C. Gartenberg. Twitter advising all 330 million users to change passwords after bug exposed them in plain text. Retrieved from https://www.theverge.com/2018/5/3/17316684/twitter-password-bug-security-flaw-exposed-change-now , 2018.

[55] S. Gibbs. Dropbox hack leads to leaking of 68m user passwords on the internet, https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach, 2016.

[56] H.W. Glaspie, and W. Karwowski. Human Factors in Information Security Culture: A Literature Review. Advances in Human Factors in Cybersecurity, Advances in Intelligent Systems and Computing 593, DOI 10.1007/978-3-319-60585-2_25 , 2018.

[57] J. Goldman. Apple Admits Celebrity Accounts Were Hacked, But Denies iCloud Breach, https://www.esecurityplanet.com/network-security/apple-admits-celebrity-accounts-were-hacked-but-denies-icloud-breach.html, 2014.

[58] J. Goldman. Citigroup acknowledges massive data breach. Retrieved from https://www.esecurityplanet.com/network-security/citigroup-acknowledges-massive-data-breach.html , 2013.

[59] J. Goldman. European central bank hacked. Retrieved from https://www.esecurityplanet.com/network-security/european-central-bank-hacked.html , 2014.

[60] J. Goldman. Japan Airlines Breach Exposes 750,000 People's Personal Data. Retrieved from https://www.esecurityplanet.com/hackers/japan-airlines-breach-exposes-750000-peoples-personal-data.html , 2014.

[61] Grobauer, B., Walloschek, T., Stocker, E.: "Understanding Cloud Computing Vulnerabilities," IEEE CLoud Computing, pp. 14–20, 2012.

[62] G. L. Group. Health net ibm privacy breach settlement. Retrieved from https://www.classlawgroup.com/health-net-ibm-privacy-breach/ , 2011.

[63] N. Gruschka, and M. Jensen. Attack Surfaces: A Taxonomy for Attacks on Cloud Services, 3rd International Conference on Cloud Computing, IEEE, pp. 276–279, DOI: 10.1109/CLOUD.2010.23, 2010.

[64] S. Gupta, and P. Kumar. Taxonomy of Cloud Security, International Journal of Computer Science, Engineering and Applications, Vol. 3, No. 5, pp. 47–67, 2013.

[65] S. Gustin. Gawker media websites hacked, staff and user passwords leaked. Retrieved from https://www.wired.com/2010/12/gawker-hacked/ , 2010.

[66] B. Gyunka, and O. C. Abikoye. Analysis of Human Factors in Cyber Security: A Case Study of Anonymous Attack on Hbgary. Computing and Information Systems Journal, Vol 21, No 2, 2017, pp 10-18 , 2017.

[67] E. Hacker. Breached server at the utah department of health gives hackers access to medicaid records. Retrieved from http://www.livehacking.com/2012/04/10/breached-server-at-the-utah-department-of-health-gives-hackers-access-to-medicaid-records/ , 2012.

[68] L. Hadlington. The "Human Factor" in Cybersecurity: Exploring the Accidental Insider. Chapter 3. IGI Global. DOI: 10.4018/978-1-5225-4053-3.ch003 , 2018.

[69] L. Hadlington. Employees Attitude towards Cyber Security and Risky Online Behaviours: An Empirical Assessment in the United Kingdom. International Journal of Cyber Criminology. ISSN: 0973-5089, January – June 2018. Vol. 12(1): 269–281. DOI: 10.5281/zenodo.1467909, 2018.

[70] D. J. Haniff, and C. Baber. Wearable Computers for the fire service and police force: Technological and human factors, ISWC'99 Proceedings of the 3rd IEEE International Symposium on Wearable Computers, ACM, pp. 185–186, 1999.

[71] Hawkey, K., Gagne, A. Botta, D., Beznosov, K., Werlinger, R., Mukdner, K.: "Human, Organizational and Technological Factors of IT Security," CHI 2008 Proceedings, Florence, Italy, pp. 3639–3644, April 5–10, 2008.

[72] Hackett, R. (2016). Quest Diagnostics Data Breach: Health Info of 34,000 Customers Exposed — Fortune. Retrieved from http://fortune.com/2016/12/13/quest-diagnostics-data-breach-health/ , 2016.

[73] Henshel, D., Cains, M.G., Hoffman, B., & Kelley, T. (2015). Trust as a human factor in holistic cyber security risk assessment. Procedia Manufacturing 3 (2015) 1117 – 1124, 2015.

[74] HHS. (2017). $5.5 million hipaa settlement shines light on the importance of audit controls. Retrieved from https://www.hhs.gov/about/news/2017/02/16/hipaa-settlement-shines-light-on-the-importance-of-audit-controls.html , 2017.

[75] Hildenbrand, J. (2018). Thousands of android and ios apps are leaking your data through their firebase backend (update). Retrieved from https://www.androidcentral.com/thousands-apps-are-leaking-your-data-through-their-firebase-backend , 2018.

[76] Hill Owen. (2011). Maple Story server hacked. 13.2 million Korean accounts compromised — PC Gamer. Retrieved from https://www.pcgamer.com/maple-story-server-hacked-13-2-million-korean-accounts-compromised/ , 2011.

[77] Ho Jung, W. (2016). Interpark apologizes for massive data leak. Retrieved from http://www.koreaherald.com/view.php?ud=20160726000748 , 2016.

[78] Honan, B. (2015). European central bank hacked. Retrieved from https://www.csoonline.com/article/2955278/european-central-bank-hacked.html , 2015.

[79] Hopkins, N. (2017). Deloitte hit by cyber-attack revealing clients' secret emails. https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails, last accessed 2018/06/13. 2017.

[80] ISMG, (2018). Global payments breach tab: $94 million. Retrieved from https://www.bankinfosecurity.com/global-payments-breach-tab-94-million-a-5415 , 2018.

[81] Jaeger, P., Lin, J., Grimes, J.: Cloud computing and information policy: Computing in a policy cloud? Journal of Information Technology & Politics, 5(3), 269-283. doi: 10.1080/19331680802425479, 2008.

[82] James, R. (2018). Major credit card processor hacked – is the sky falling? Retrieved from https://privacysniffs.com/crime-talk/major-credit-card-processor-hacked-is-the-sky-falling/ , 2018.

[83] Jagatic, T.N., Johnson, N.A., Jakobsson, M., Menczer, F.: "Social Phishing," Communications of the ACM, Vol. 50, No. 10, October, 2007.

[84] Ji-sook, B. (2012). 8.7 million kt mobile customers' data hacked in s. korea. Retrieved from https://www.databreaches.net/8-7-million-kt-mobile-customers-data-hacked-in-s-korea/ [**?**]

[85] Johnson, R. B., & Onwuegbuzie, A. J. (2004). Mixed methods research: A research paradigm whose time has come. Educational researcher, 33(7), 14-26, 2004.

[86] Johnson, R. B., Onwuegbuzie, A. J., & Turner, L. A. (2007). Toward a definition of mixed methods research. Journal of mixed methods research, 1(2), 112-133, 2007.

[87] Jones, C. (2013). Twitter says 250,000 accounts have been hacked in security breach, https://www.theguardian.com/technology/2013/feb/02/twitter-hacked-accounts-reset-security, last accessed 2018/05/28, 2013.

[88] Kahraman, E. Evaluating IT security performance with quantifiable metrics. Master's thesis, DSV SU/KTH. Available at: http://citeseerx.ist.psu.edu /viewdoc/download?doi=10.1.1.102.4000&rep=rep1&type=pdf, 2005.

[89] Kastrenakes, J. (2015). FCC fines AT&T a record $25 million for customer data thefts - The Verge. Retrieved 20 August 2019, from https://www.theverge.com/2015/4/8/8370515/att-fcc-settlement-data-thefts-25-million-fine , 2015.

[90] KCOM. (2017). Cloud: The Data Breach Scapegoat, https://business.kcom.com/media/blog/2017/november/cloud-the-data-breach-scapegoat/, 2017.

[91] Kearney, P. (2010). Security: The Human Factor. Cambridgeshire: IT Governance Publishing. 2010.

[92] Kelly, H. (2013). Apple: We were hacked, too - CNN. Retrieved 20 August 2019, from https://edition.cnn.com/2013/02/19/tech/web/apple-hacked/index.html , 2013.

[93] Kirk, J. (2019). Neiman marcus settles lawsuit over payment card breach. Retrieved from https://www.bankinfosecurity.com/neiman-marcus-settles-lawsuit-over-payment-card-breach-a-11923 , 2019.

[94] Kohn, L.T., Corrigan, J.M., & Donaldson, M.S., (eds.). (1999) To err is human - building a safer health system. Washington, DC, Committee on Quality of Health Care in America, Institute of Medicine, National Academy Press, 1999.

[95] Kovacs, E. (2013). Citi exposes details of 150,000 individuals who went into bankruptcy. Retrieved from https://news.softpedia.com/news/Citi-Exposes-Details-of-150-000-Individuals-Who-Went-into-Bankruptcy-369979.shtmlhttps://fortune.com/2016/12/13/quest-diagnostics-data-breach-health/ , 2013.

[96] Krebs, B. (2018). Panerabread.com Leaks Millions of Customer Records — Krebs on Security. Retrieved from https://krebsonsecurity.com/2018/04/panerabread-com-leaks-millions-of-customer-records/ , 2018.

[97] Krebs. B. (2010). Hundreds of Network Solutions Sites Hacked. Retrieved from https://krebsonsecurity.com/2010/01/hundreds-of-network-solutions-sites-hacked/ , 2010.

[98] Krombholz, K., Hobel, H., Huber, M., Weippl, E.: "Social engineering attacks on the knowledge worker," In Proceedings of the 6th International Conference on Security of Information and Networks, SIN '13, ACM, pp. 28–35, New York, NY, USA, 2013.

[99] Kubba Sinan. (2013). Club Nintendo Japan hacked. Retrieved from https://www.engadget.com/2013/07/05/club-nintendo-japan-hacked/?guccounter=1 , 2013.

[100] Kueppers, S., Schilingno, M.: "Getting our act together: Human and technological factors in establishing an online knowledge base," SIGUCCS 99, ACM, Denver, Colorado, pp. 135–139, 1999.

[101] Kumar, M. (2018). T-mobile hacked — 2 million customers' personal data stolen. Retrieved from https://thehackernews.com/2018/08/t-mobile-hack-breach.html , 2018.

[102] Langde, R. (2017). Wannacry ransomware: A detailed analysis of the attack. Retrieved from https://techspective.net/2017/09/26/wannacry-ransomware-detailed-analysis-attack/, 2017.

[103] Lawler, R. (2013). Snapchat database leak claims to contain 4.6 million phone numbers and usernames. Retrived 23 August 2019, from https://www.engadget.com/2013/12/31/snapchat-user-info-leak/ , 2013.

[104] Lee, A. (2011). Citigroup: $2.7 Million Stolen from Customers As Result Of Hacking — HuffPost. Retrieved 20 August 2019, from https://www.huffpost.com/entry/citigroup-hack_n_885045 , 2011.

[105] Lewis, D. (2015). Heartland payment systems suffers data breach. Retrieved from https://www.forbes.com/sites/davelewis/2015/05/31/heartland-payment-systems-suffers-data-breach/#6a61f7b2744a , 2015.

[106] Leyden, J. (2012). Formspring springs a leak: 28 million passwords reset after raid. Retrieved from https://www.theregister.co.uk/2012/07/11/formspring_security_breach/ , 2012.

[107] Leyden, J. (2017). That big scary 1.4bn leak was 100s of millions of email, postal addresses • The Register. Retrieved from https://www.theregister.co.uk/2017/03/07/rcm_email_megaleak/ , 2017.

[108] Liao Shannon. (2018). Newegg users' credit card info was exposed to hackers for a month - The Verge. Retrieved from https://www.theverge.com/2018/9/19/17879630/newegg-user-credit-card-info-data-breach-hack , 2018.

[109] Liebowitz, M. (2011). Huge data breach pots 200,000 at risk. Retrieved from http://www.nbcnews.com/id/43086769/ns/technology_and_science-security/t/huge-data-breach-puts-risk/#.XXB3tOMzbb1 , 2011.

[110] Loudenback, T. 500 million marriott customers have had their data hacked. here's what you should do instead of freaking out. Retrieved from https://www.businessinsider.com.au/marriott-breach-data-hack-personal-information-what-to-do-2018-11?r=US&IR=T%22 , 2018.

[111] Martin, A. (2015). British Airways suffers frequent flyer account hacking — WeLiveSecurity. Retrieved 20 August 2019, from https://www.welivesecurity.com/2015/03/30/british-airways-suffers-frequent-flyer-account-hacking/ , 2015.

[112] Mascarenhas, H. Red Cross Blood Service data breach that affected 550,000 donors caused by 'one-off human error'. Retrieved from https://www.ibtimes.co.uk/red-cross-blood-service-data-breach-that-affected-550000-donors-caused-by-one-off-human-error-1633977 , 2017.

[113] McGee, M. K. Did a myspace hack compromise 427 million passwords? Retrieved from https://www.bankinfosecurity.com/did-myspace-hack-compromise-470-million-passwords-a-9151 , 2016.

[114] McGlasson, L. RBS WorldPay Hacked; 1.5 Million Cardholders at Risk. Retrieved from https://www.bankinfosecurity.com/rbs-worldpay-hacked-15-million-cardholders-at-risk-a-1150 , 2009.

[115] McLean, R. A hacker gained access to 100 million Capital One credit card applications and accounts. Retrieved from: https://edition.cnn.com/2019/07/29/business/capital-one-data-breach/index.html, Accessed on: 20 September, 2019.

[116] Mearian, L. 'wall of shame' exposes 21m medical record breaches. Retrieved from https://www.computerworld.com/article/2505546/-wall-of-shame–exposes-21m-medical-record-breaches.html , 2012.

[117] Metalidoua, E., Marinagic, C., Trivellasc, P., Eberhagen, N., Skourlasd, C., & Giannakopoulos, G.. The Human Factor of Information Security: Unintentional Damage Perspective. Procedia - Social and Behavioral Sciences 147 (2014) 424 – 428, 2014.

[118] Mitnick, K. D., Simon, & L., W. The art of deception: controlling the human element of security. Indiana: John Wiley & Sons. ISBN: 978-0-471-23712-9 , 2011.

[119] Mohamadi, M., Ranjbaran, T.: "Effective factors on the success or failure of the online payment systems, focusing on human factors," 7th International Conference on e-Commerce in Developing Countries with Focus of e-Security, IEEE, Iran, pp. 1–12, April 17–18, 2013.

[120] Morgan, S. (2016). Irs reports 700,000 U.S. taxpayers hacked and 47 million 'get transcripts' ordered. Retrieved from https://www.forbes.com/sites/stevemorgan/2016/02/28/irs-reports-700000-u-s-taxpayers-hacked-and-47-million-get-transcripts-ordered/#2ec249fe7b93, 2016.

[121] Morse, J. M. (1991). Strategies for sampling. In, Morse JM, ed. Qualitative Nursing Research-A Contemporary Dialogue, 1991.

[122] Musil, S. (2012). AntiSec claims to have snatched 12M Apple device IDs from FBI - CNET. Retrieved 20 August 2019, from https://www.cnet.com/news/antisec-claims-to-have-snatched-12m-apple-device-ids-from-fbi/ , 2012.

[123] MyHeritage. (2018). Myheritage statement about a cybersecurity incident. Retrieved from https://blog.myheritage.com/2018/06/myheritage-statement-about-a-cybersecurity-incident/ , 2018.

[124] Naraine, R. (2011). Nasdaq confirms servers hacked via web-facing application. Retrieved from https://www.zdnet.com/article/nasdaq-confirms-servers-hacked-via-web-facing-application/ , 2011.

[125] Nate, L. (2018). What is Social Engineering? Defining and Avoiding Common Social Engineering Threats. Available at: https://digitalguardian.com/blog/what-social-engineering-defining-and-avoiding-common-social-engineering-threats , 2018.

[126] National Research Council: Health Care Comes Home: The Human factors. Committee on the Role of Human factors in Home Health Care, Board on Human-Systems Integration, Division of Behavioural and Social Sciences and Education. Washington DC: The National Academies Press, 2011.

[127] NBC. Formspring site hacked, passwords leaked to web. Retrieved from http://www.nbcnews.com/id/48150149/ns/technologyandscience-security/t/formspring-site-hacked- passwords-leaked-web/.XWcEqeMzY 2x , 2012.

[128] NBC. Security incident exposed at Oregon Department of Revenue - KOBI-TV NBC5 / KOTI-TV Retrieved from https://kobi5.com/news/security-incident-exposed-at-oregon-department-of-revenue-74399/ , 2018.

[129] NBCNews (2014). You've Got Hacked: AOL Confirms 'Significant Number' of Mail Users Hit. Retrieved from https://www.nbcnews.com/tech/security/youve-got-hacked-aol-confirms-significant-number-mail-users-hit-n91701 , 2014.

[130] Newcomb, A. (2015). T-mobile customers hacked in experian breach: What you need to know. Retrieved from https://abcnews.go.com/Technology/experian-hack-exposes-mobile-customers/story?id=34200279 , 2015.

[131] Newton, C. (2017). An instagram hack hit millions of accounts, and victims' phone numbers are now for sale. Retrieved from https://www.theverge.com/2017/9/1/16244304/instagram-hack-api-bug-doxagram-selena-gomez , 2017.

[132] Nick Eubanks, Jul 13, 2017. The True Cost of Cybercrime for Businesses. Available at: https://www.forbes.com/sites/theyec/2017/07/13/the-true-cost-of-cybercrime-for-businesses/#44a947234947, 2017.

[133] Nurse, J. R. C., Creese, S., Goldsmith, M., and Lamberts, K. (2011). Trustworthy and effective communication of cybersecurity risks: A review. Proceedings - 2011 1st Workshop on Socio-Technical Aspects in Security and Trust, STAST 2011, 60–68. doi:10.1109/STAST.2011.6059257 , 2011.

[134] Odaro, U.S., and Sanders, B.G. Social Engineering: Phishing for a Solution. Proceedings of the IT Security for the Next Generation, Erfurt, Germany, 2011.

[135] Olson, P. FBI Agent's Laptop 'Hacked' To Grab 12 Million Apple IDs - UPDATED. Retrieved 20 August 2019, from https://www.forbes.com/sites/parmyolson/2012/09/04/fbi-agents-laptop-hacked-to-grab-12-million-apple-ids-anonymous-claims/#26896f6126b5 , 2012.

[136] O'Sullivan, D. Cloud Leak: How A Verizon Partner Exposed Millions of Customer Accounts, https://www.upguard.com/breaches/verizon-cloud-leak, 2018.

[137] Paganini, P. (2018). Unsecured aws s3 bucket managed by walmart jewelry partner exposes data of 1.3m customers. Retrieved from https://securityaffairs.co/wordpress/70381/data-breach/walmart-jewelry-partner-leak.html , 2018.

[138] Patton, M. Q. Qualitative evaluation and research methods. SAGE Publications, inc. 1990.

[139] Pirzadeh, L. (2010). A Systematic Literature Review, Master of Science Thesis in Computer Science and Engineering. Department of Computer Science and Engineering, Chalmers University of Technology. 2010.

[140] Phys.org (2012). App firm say it may be source of Apple breach. Retrieved from: https://phys.org/news/2012-09-app-firm-source-apple-breach.html, 2012.

[141] Pollock, T. (2017). Reducing human error in cyber security using the Human Factors Analysis Classification System (HFACS). KSU Proceedings on Cybersecurity Education, Research and Practice. 2. available at: http://digitalcommons.kennesaw.edu/ccerp/2017/research/2, 2017.

[142] Protalinski, E. (2012a). 8.24 million gamigo passwords leaked after hack. Retrieved from https://www.zdnet.com/article/8-24-million-gamigo-passwords-leaked-after-hack/ , 2012.

[143] Protalinski, E. (2012b). Medicaid hacked: over 181,000 records and 25,000 ssns stolen. Retrieved from https://www.zdnet.com/article/medicaid-hacked-over-181000-records-and-25000-ssns-stolen/, 2012.

[144] Ragan, S. (2015). Database leak exposes 3.3 million Hello Kitty fans — CSO Online. Retrieved 20 July 2019, from https://www.csoonline.com/article/3017171/database-leak-exposes-3-3-million-hello-kitty-fans.html , 2015.

[145] Reuters. (2011). Data of 13 million South Korean online game subscribers hacked - -Retrieved from https://www.reuters.com/article/us-korea-hacking-nexon/data-of-13-million-south-korean-online-game-subscribers-hacked-idUSTRE7AP09H20111126 , 2011.

[146] Riedy, M. K., and Hanus, B. (2016). Yes, your personal data is at risk: Get over it. SMU Sci. & Tech. L. Rev., 19, 3. 2016.

[147] Roberts, P. (2007). Massive TJX Security Breach Reveals Credit Card Data, https://www.csoonline.com/article/2121609/malware-cybercrime/massive-tjx-security-breach-reveals-credit-card-data.html, 2007.

[148] Rodriguez, S. (2018). Facebook says hackers were able to access millions of phone numbers and email addresses. Retrieved from https://www.cnbc.com/2018/10/12/facebook-security-breach-details.html , 2018.

[149] Roman, J. (2014). Staples: 1.2 Million Cards Breached - BankInfoSecurity. Retrieved from https://www.bankinfosecurity.com/staples-12-million-cards-breached-a-7704 , 2014.

[150] Rosenblatt, S. (2013). Livingsocial hacked; 50 million affected. Retrieved from https://www.cnet.com/news/livingsocial-hacked-50-million-affected/ , 2013.

[151] Rosenfeld, E. (2015). AT&T data breaches revealed: 280K US customers exposed. Retrieved 20 August 2019, from https://www.cnbc.com/2015/04/08/att-data-breaches-revealed-280k-us-customers-exposed.html , 2015.

[152] Sanders, M.S. and McCormick, E.J. (1992). "Human factors in engineering and design", McGraw-Hill, Inc., 7th edition, 1992.

[153] Sandelowski, M. (1995). Sample size in qualitative research. Research in nursing & health, 18(2), 179-183. 1995.

[154] Santo, M. (2007). AT&T Laptop Theft Exposes Employee Data. Retrieved 20 August 2019, from https://hothardware.com/news/att-laptop-theft-exposes-employee-data , 2007.

[155] Sasse, M., Brostoff, S., and Weirich, D. (2001). Transforming the "weakest link": A Human-Computer Interaction Approach for Usable and Effective Security. BT Technology Journal, 19(3), 122–131. doi:10.1023/A:1011902718709 , 2001.

[156] Sasse, M., and Flechais, I. (2005). Usable Security: Why Do We Need It? How Do We Get It? Retrieved from http://discovery.ucl.ac.uk/20345/ , 2005.

[157] Schultz, E. (2005). The human factor in security. Computers & Security, 24, 425-426, 2005.

[158] Schneier, B. (2000). Secrets and Lies, New York: John Wiley & Sons, 2000.

[159] Schuman, E. (2016). LinkedIn's disturbing breach notice, https://www.computerworld.com/article/3077478/security/linkedin-s-disturbing-breach-notice.html, 2016.

[160] Scott. (2018). 48 million user profiles potentially leaked by washington-based data firm localbox. Retrieved from https://spyware-techie.com/48-million-user-profiles-potentially-leaked-by-washington-based-data-firm-localbox , 2018.

[161] Security on NBC News. (2005). Citi notifies 3.9 million customers of lost data - Technology & science. Retrieved 20 August 2019, from http://www.nbcnews.com/id/8119720/ns/technology_and_science-security/t/citi-notifies-million-customers-lost-data/?hasFlash=true&#.XVuJ03tS9yx, 2005.

[162] Sharwood, S. (2017). Missed patch caused Equifax data breach, https://www.theregister.co.uk/2017/09/14/missed_patch_caused_equifax_data_breach/, 2017.

[163] Shih, G.: Facebook admits year-long data breach exposed 6 million users, https://uk.reuters.com/article/net-us-facebook-security/facebook-admits-year-long-data-breach-exposed-6-million-users-idUSBRE95K18Y20130621, last accessed 2018/05/28, 2018.

[164] Silverstein, J. Hundreds of millions of Facebook user records were exposed on Amazon cloud server. Retrieved from:

https://www.cbsnews.com/news/millions-facebook-user-records-exposed-amazon-cloud-server/ , 2019.
[165] Smith, D., and Bee, S. (2011). Sutter Health sued over theft of computer containing patient data – The Mercury News. Retrieved from https://www.mercurynews.com/2011/11/23/sutter-health-sued-over-theft-of-computer-containing-patient-data/ , 2011.
[166] Smith. M. (2018). Saks, Lord & Taylor hacked; 5 million payment cards compromised. Retrieved from: https://www.csoonline.com/article/565016/saks-lord-taylor-hacked-5-million-payment-cards-compromised.html , 2018.
[167] Sophia Yan, K. (2014). Massive data theft hits 40% of south koreans. Retrieved from https://money.cnn.com/2014/01/21/technology/korea-data-hack/ , 2014.
[168] Srinivasan, M.K., Sarukesi, K., Rodrigues, P., Manoj, S., and Revathy, P. State–of–the–art Cloud Computing Security Taxonomies – A classification of security challenges in the present cloud computing environment, ICACCI '12, ACM, Chennai, India, pp. 470-476, August 03 – 05, 2012.
[169] Statt, N. Maker of popular quiz apps on facebook exposed personal data of 120 million users. Retrieved from https://www.theverge.com/2018/6/28/17514822/facebook-data-leak-quiz-app-nametests-social-sweetheart-exposed-user-info , 2018.
[170] Stout, D. AOL Engineer Sold 92 Million Names to Spammer, U.S. Says - The New York Times. Retrieved from https://www.nytimes.com/2004/06/23/technology/aol-engineer-sold-92-million-names-to-spammer-us-says.html , 2004.
[171] Strauss, A., and Corbin, J. (1990). Basics of qualitative research. Sage publications. 1990.
[172] The Guardian. (2013). Apple Developer site hack: Turkish security researcher claims responsibility. Retrieved from: https://www.theguardian.com/technology/2013/jul/22/apple-developer-site-hacked, 2013.
[173] The Guardian. (2014). New York taxi details can be extracted from anonymised data, researchers say — Technology. Retrieved from https://www.theguardian.com/technology/2014/jun/27/new-york-taxi-details-anonymised-data-researchers-warn , 2014.
[174] The Guardian. (2015). British Airways frequent-flyer accounts hacked. Retrieved from https://www.theguardian.com/business/2015/mar/29/british-airways-frequent-flyer-accounts-hacked, 2015.
[175] The New York Times. (2005). Citigroup unit's data tapes lost - The New York Times. Retrieved from https://www.nytimes.com/2005/06/07/business/worldbusiness/citigroup-units-data-tapes-lost.html , 2005.
[176] Thornburgh, T.: "Social Engineering: The "Dark Art"," InfoSecCD Conference04, Kennesaw, GA, USA, October 8, 2004.
[177] Trend Micro. Sutter Health sued for $1 billion following data breach. Retrieved from: https://blog.trendmicro.com/sutter-health-sued-for-1-billion-following-data-breach/, 2011.
[178] Tsukayama, H. AOL probing security breach - The Washington Post. Retrieved 20 August 2019, from https://www.washingtonpost.com/business/economy/aol-probing-security-breach/2014/04/28/efbfb3ca-cf0e-11e3-a6b1-45c4dffb85a6_story.html?noredirect=on , 2014.
[179] Twitchell, D.P.: Social Engineering in Information Assurance Curricula, InfoSecCD Conference 06, Kennesaw, Georgia, USA, September 22-23, 2006.
[180] Valinsky. Marriott reveals data breach of 500 million starwood guests. Retrieved from https://edition.cnn.com/2018/11/30/tech/marriott-hotels-hacked/index.html , 2018.
[181] Vijayan, J. Health net discloses loss of data to 1.9 million customers. Retrieved from https://www.computerworld.com/article/2506615/health-net-discloses-loss-of-data-to-1-9-million-customers.html , 2018.
[182] Vijayan, J. RockYou hack exposes names, passwords of 30M accounts. Retrieved from https://www.computerworld.com/article/2522045/rockyou-hack-exposes-names–passwords-of-30m-accounts.html , 2009.
[183] Vijayan, J. AT&T Laptop Theft Exposes Employee Data. Retrieved from https://www.pcworld.com/article/136636/article.html , 2007.
[184] Vinton, K. Premera Blue Cross Breach May Have Exposed 11 Million Customers' Medical and Financial Data. Retrieved from https://www.forbes.com/sites/katevinton/2015/03/17/11-million-customers-medical-and-financial-data-may-have-been-exposed-in-premera-blue-cross-breach/#6538e1575d90 , 2015.
[185] Walton, M. National Patient Safety Education Framework. Canberra, Commonwealth of Australia, 2005.
[186] Whitney, L. Hackers accused of stealing data from 9M korean mobile users. Retrieved from https://www.cnet.com/news/hackers-accused-of-stealing-data-from-9m-korean-mobile-users/, 2012.
[187] Winter, M. Home Depot hackers used vendor log-on to steal data, e-mails, https://www.usatoday.com/story/money/business/2014/11/06/home-depot-hackers-stolen-data/18613167/, last accessed 2018/05/26, 2014.
[188] Zissis, D., Lekkas, D. Addressing cloud computing security issues. Future Generation Computer Systems, 28, 583–592, 2012.