Cracking Customer Confidentiality

Morgan Davies

COMP3011 – Ethical Hacking

In 2018, GDPR came into force in the EU. Prior, the UK had the Data Protection Act 1998 alongside various other countries that possessed their own interpretations of the legislation. These laws imply that citizens in the modern digital world hold privacy of their personal effects to be a fundamental right [1].

However, that right is under threat from those who wish to exploit this information for financial, competitive or political gain [2, 8]. This is even more so during the COVID-19 pandemic, where vaccine manufacture and distribution assets are highly sought after for national pride or the theft of intellectual property [3].

In this report, I will be highlighting the recent trends in attacks against customer and business data, as well as the potential future direction of these tendencies.

CONTEXTUAL BACKGROUND

Commonly, when the topic of data breaches and privacy is brought up, the consensus appears to be focused on the companies rather than the techniques used to capture the data. This makes sense as legal ramifications against companies can be more publicly significant than the methods of which they were instigated [9]. Considering the extent that customer and business data is shared, not always amongst the most trustworthy organisations, this fear is justified [5]. While the causes and continuations of said sharing are various [6], this fear of personal or business data being shared with undesirable parties is perhaps what catapulted moves towards the previously mentioned legislations in recent years [7].

So what techniques have attackers used in the past to obtain this valuable data? The 2016 Target Data Breach [4] has shown that credential stuffing was used to obtain access to the unsegmented payment network, allowing attackers to scrape credit card details, possibly to escalate cryptocurrency mining efforts [10]. In the context of a Figure 1 attack flow, the Target attackers likely conducted this cycle both against Fazio Mechanical Services AND Target [11], beginning with a phishing email campaign [12] against Fazio. It would be then possible for the perpetrators to perform vulnerability analysis reconnaissance Target's systems, subsequently identifying the misconfigured web service that allowed for the uploading of executable files [13].

Target's case is not unique. Further attacks, such as the 2017 Equifax Breach [14], shows a similar trend of a vulnerability [15] being exposed by a misconfigured web update [16]. Modern trends seem to indicate that these initial footholds are used to further the position of privilege escalation and malware deployment, especially if the goal is to hold organisational assets to ransom [17]. In the case of the health sector, this type of attack has only been growing during the coronavirus crisis [18]. Even vaccine development is under threat from rival nation APT's [19].

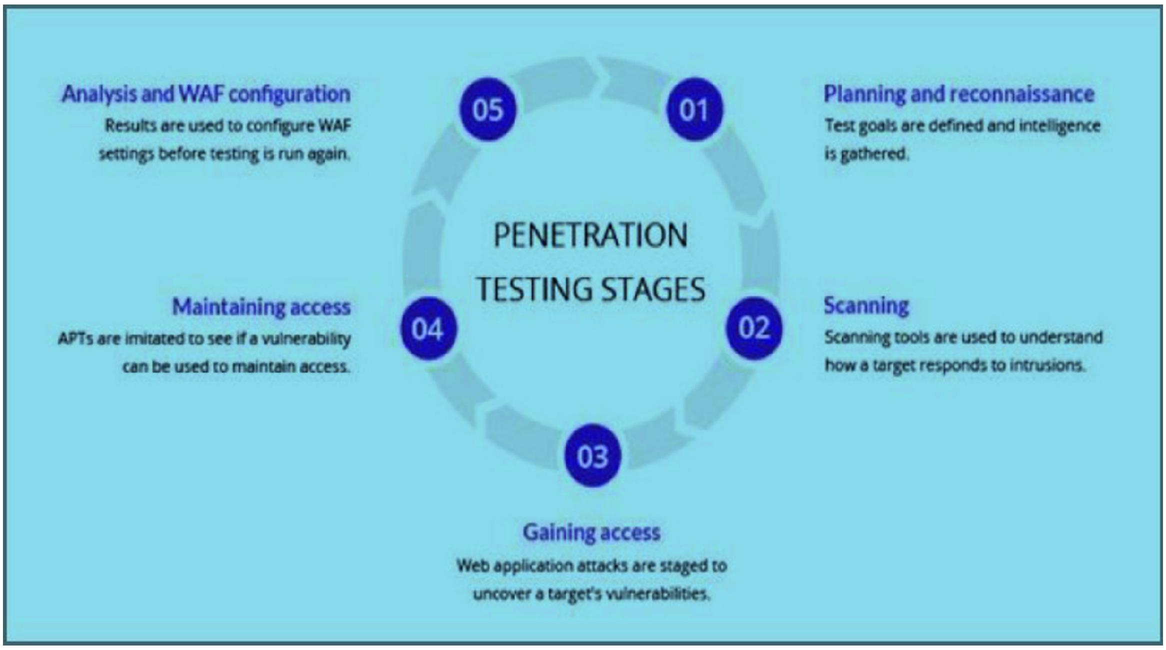
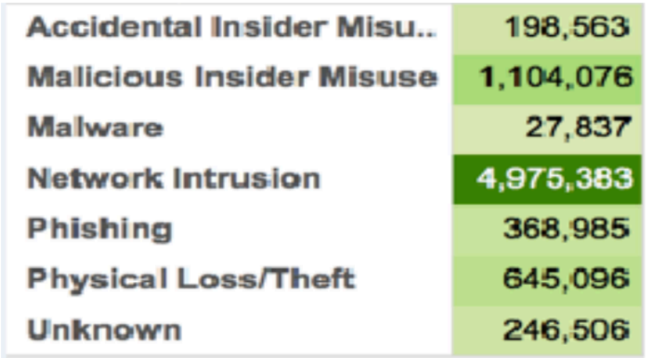

PENETRATION TESTING STAGES
01
Planning and reconnaissance
Test goals are defined and intelligence is gathered.
02
Scanning
Scanning tools are used to understand how a target responds to intrusions.
03
Gaining access
Web application attacks are staged to uncover a target's vulnerabilities.
04
Maintaining access
APTs are imitated to see if a vulnerability can be used to maintain access.
05
Analysis and WAF configuration
Results are used to configure WAF settings before testing is run again.

Figure 1: Flow of an Ethical Hack based on actual techniques used by malicious offensive actors.

TREND ANALYSIS

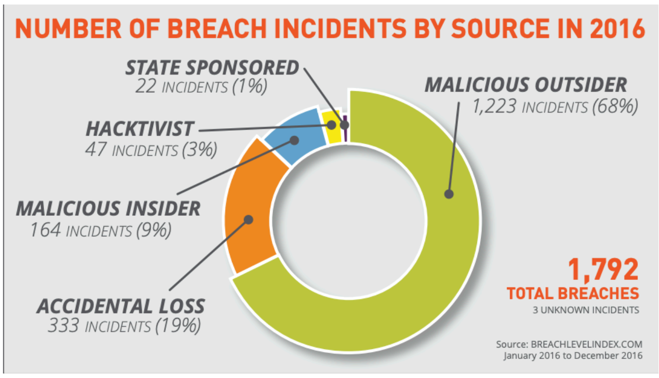
Before the coronavirus pandemic, groups looking to harvest data tended to be skewed towards network intrusion attacks. Figure 2 reflects this, showing network attacks were more successful when speaking in terms of records obtained [20]. This matches the following year (Figure 3). Furthermore, this was not a type of crime that was expected to expire at the time (Figure 4) or into the future considering the first half of 2017 [22] and subsequent years after [23].

Evaluating whose data exactly is being regularly attacked (businesses vs consumers), I have analysed a dataset of breaches from July 2019 – July 2020 (Appendix 1). Based off the results of the analysis, I can confidently claim that attacks on customer data are increasing, both in the chronological and proportional sense. However, attacks on business data can be just as quantifiably devasting (as seen in the 5 billion records attack). Of the business groups, IBM appears to infer that corporations who cannot afford extended periods of downtime are more likely to be attacked by ransomware, an alternative strategy when it comes to data theft [31].



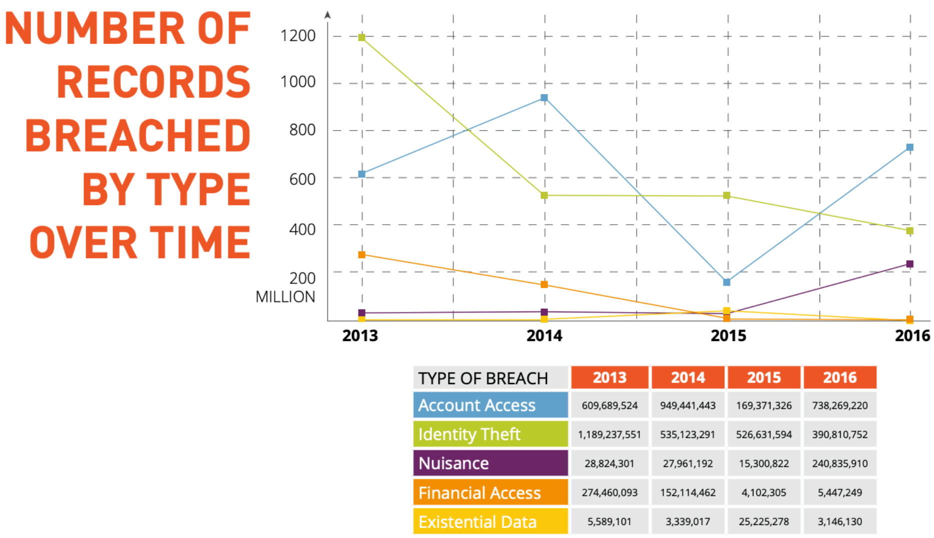
Accidental Insider Misu..	198,563
Malicious Insider Misuse	1,104,076
Malware	27,837
Network Intrusion	4,975,383
Phishing	368,985
Physical Loss/Theft	645,096
Unknown	246,506

Figure 2: Records stolen between 2005 and 2015 in the medical sector [20].



Source: BREACHLEVELINDEX.COM
January 2016 to December 2016

Figure 3: Only malicious insider and accidental loss sections do not fit into the category of network exploitation of data [21]

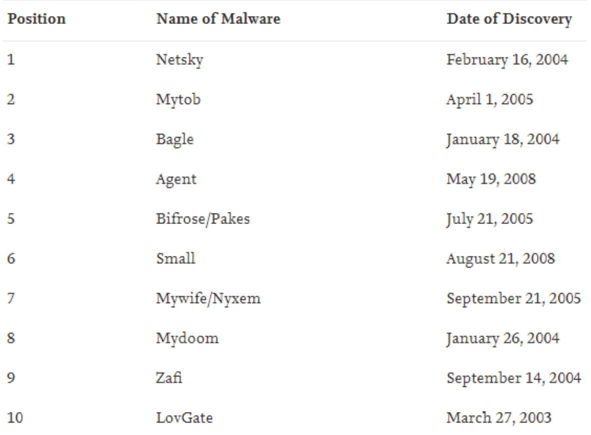


TYPE OF BREACH	2013	2014	2015	2016
Account Access	609,689,524	949,441,443	169,371,326	738,269,220
Identity Theft	1,189,237,551	535,123,291	526,631,594	390,810,752
Nuisance	28,824,301	27,961,192	15,300,822	240,835,910
Financial Access	274,460,093	152,114,462	4,102,305	5,447,249
Existential Data	5,589,101	3,339,017	25,225,278	3,146,130

Figure 4: All of these types come under the term "data", but some are a means to an end. I.e. Account Access by password cracking an intercepted admin credential hash to obtain records for identify thievery for financial purposes, would be leveraging privileged access to a system as a means to an end [21].

TREND ANALYSIS CONTINUED...

As for the tools and techniques being used to harvest data however, social engineering is an increasingly popular attack vector for conducting reconnaissance and establishing backdoor footholds into organisational systems [27]. From here, data can be collected by the attacker by accessing services behind an organisation's firewall or even by impersonating trusted employees [29]. Looking at Figure 5, an upward trend of social engineering incidents in the graph would correlate the trend seen in table, malware that is usually primarily delivered via email, seeming to suggest that phishing emails are on the rise should an attacker wish to collect data.



Position	Name of Malware	Date of Discovery
1	Netsky	February 16, 2004
2	Mytob	April 1, 2005
3	Bagle	January 18, 2004
4	Agent	May 19, 2008
5	Bifrose/Pakes	July 21, 2005
6	Small	August 21, 2008
7	Mywife/Nyxem	September 21, 2005
8	Mydoom	January 26, 2004
9	Zafi	September 14, 2004
10	LovGate	March 27, 2003

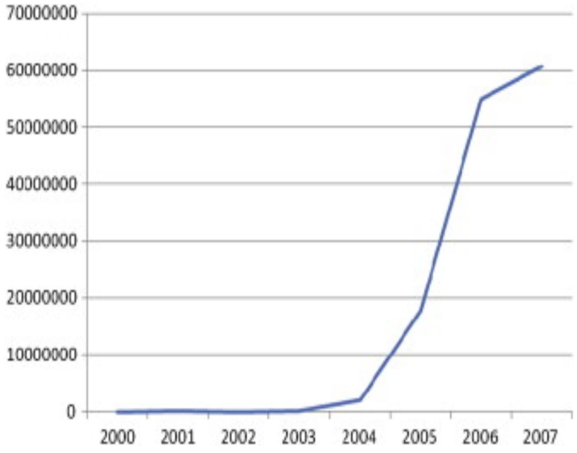


Figure 5: Top malware, commonly delivered by email, alongside number of 2009 security incidents utilising social engineering [27, 28].

However, what Figure 5 does not show is the recent movement towards ransomware as a service since 2016, possibly due to the universal attack surface that is encryption [30]. In concept the recon stage is the same, but the malware package is different, encrypting data to be used as ransom instead of collecting and selling it. Figure 6 does however show the increase in ransomware, with the added quirk of it being used in conjunction with data mining in some cases [32]. With ransomware appearing to be the dominant choice over data miners, SME's and developing countries may struggle more in the future when deploying their cyber presence, as they sometimes cannot afford backup data solutions [36].

Regarding the covid-19 pandemic, the healthcare and education sector is under extra strain from both physical and virtual contagions (Figure 7 [34]) malicious to them [18]. Although HIPAA [23] disagrees with this theory when it comes to attacks on individuals, it does show more complex and scalable attacks occurring more often, interestingly showing a drop in 2017 despite WannaCry [35].

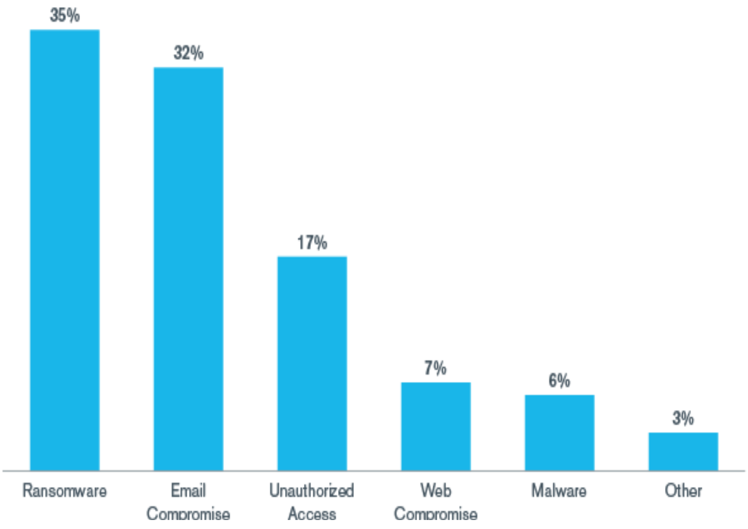
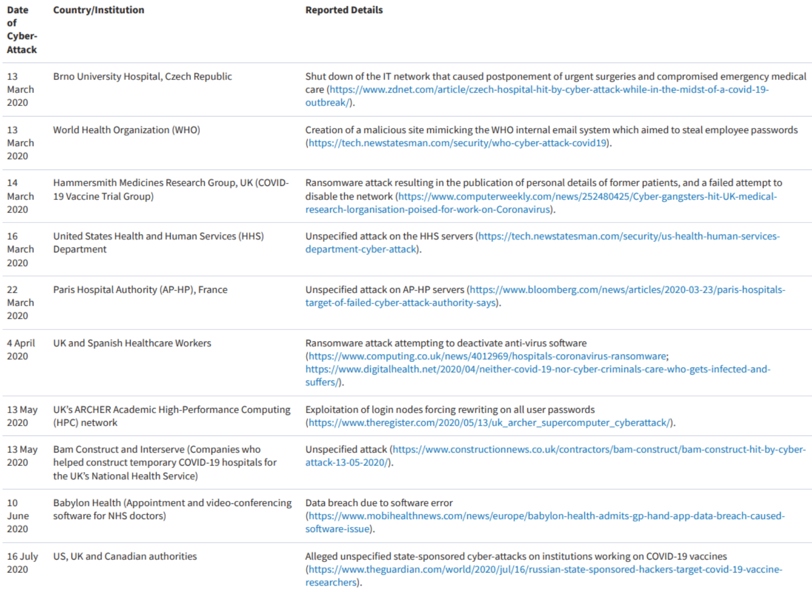


Figure 6: % of reported malware attacks in 2020 by type [32].



Date of Cyber-Attack	Country/Institution	Reported Details
13 March 2020	Brno University Hospital, Czech Republic	Shut down of the IT network that caused postponement of urgent surgeries and compromised emergency medical care (https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/).
13 March 2020	World Health Organization (WHO)	Creation of a malicious site mimicking the WHO internal email system which aimed to steal employee passwords (https://tech.newstatesman.com/security/who-cyber-attack-covid19).
14 March 2020	Hammersmith Medicines Research Group, UK (COVID-19 Vaccine Trial Group)	Ransomware attack resulting in the publication of personal details of former patients, and a failed attempt to disable the network (https://www.computerweekly.com/news/252480425/Cyber-gangsters-hit-UK-medical-research-lorganisation-poised-for-work-on-Coronavirus).
16 March 2020	United States Health and Human Services (HHS) Department	Unspecified attack on the HHS servers (https://tech.newstatesman.com/security/us-health-human-services-department-cyber-attack).
22 March 2020	Paris Hospital Authority (AP-HP), France	Unspecified attack on AP-HP servers (https://www.bloomberg.com/news/articles/2020-03-23/paris-hospitals-target-of-failed-cyber-attack-authority-says).
4 April 2020	UK and Spanish Healthcare Workers	Ransomware attack attempting to deactivate anti-virus software (https://www.computing.co.uk/news/4012969/hospitals-coronavirus-ransomware; https://www.digitalhealth.net/2020/04/neither-covid-19-nor-cyber-criminals-care-who-gets-infected-and-suffers/).
13 May 2020	UK's ARCHER Academic High-Performance Computing (HPC) network	Exploitation of login nodes forcing rewriting on all user passwords (https://www.theregister.com/2020/05/13/uk_archer_supercomputer_cyberattack/).
13 May 2020	Bam Construct and Interserve (Companies who helped construct temporary COVID-19 hospitals for the UK's National Health Service)	Unspecified attack (https://www.constructionnews.co.uk/contractors/bam-construct/bam-construct-hit-by-cyber-attack-13-05-2020/).
10 June 2020	Babylon Health (Appointment and video-conferencing software for NHS doctors)	Data breach due to software error (https://www.mobihealthnews.com/news/europe/babylon-health-admits-gp-hand-app-data-breach-caused-software-issue).
16 July 2020	US, UK and Canadian authorities	Alleged unspecified state-sponsored cyber-attacks on institutions working on COVID-19 vaccines (https://www.theguardian.com/world/2020/jul/16/russian-state-sponsored-hackers-target-covid-19-vaccine-researchers).

Figure 7: Report cyber attacks in 1st half of 2020

INSIGHTS AND EVALUATIONS

Summarising the results, it is clear the quantity of yearly data breaches is consistently increasing but the scale of each is bigger than the last. Expedited by the emergence of ransomware and the need for a coronavirus vaccine [38], Figure 7 seems to suggest APT's and other groups are using increasingly complex techniques to achieve greater success rates with their attacks [39]. Even without ransomware, scams leveraging the public's need for information during the pandemic have been common and highly effective, likely accounting for the high email compromising malware (Figure 6) [40]. When accounting for ransomware, even before the pandemic, attacks utilising it have been common and increasing in profit, clearly depicted in Figure 8.

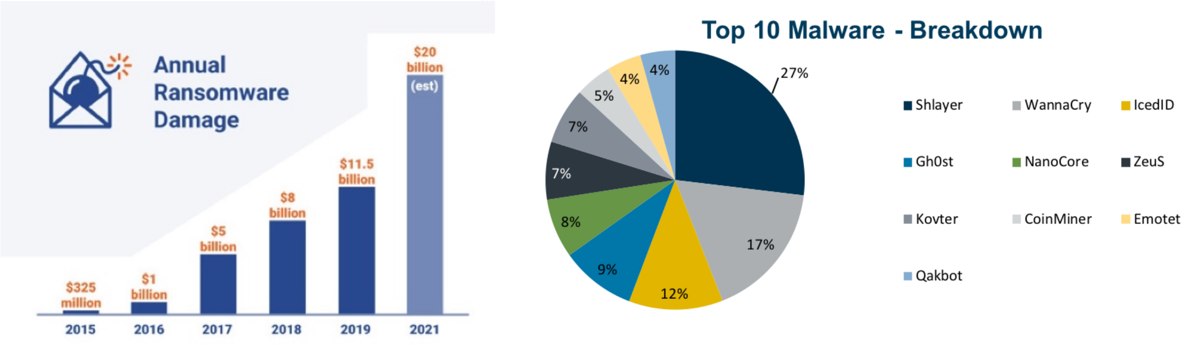


Figure 8: Incremental increase in ransomware damages [41] compared to the 2019 Top 10 malware (the 2nd top being ransomware) [42].

This suggests that businesses continue to not have effective backup solutions available to restore data loss quickly, leading to greater profits from the effort for the cyber criminals.

So where does this leave us for the future? Based on the trends seen above, I imagine we will continue to see coronavirus scams and tampering of vaccine research until the pandemic is over [37]. Not only this, but organisations have been heavily reliant on homeworkers, an ideology that is likely to continue to be driven post covid [43]. Therefore, I imagine we will see a resurgence of data breaches and cyber-attacks targeting solutions that aim to assist home-workers [44], perhaps even adapted to be used in spear phishing attacks of the attackers choosing [46]. In fact, we have already started to see such events like this relating to Zoom (Figure 9) [45]. In conclusion, it is likely that attacks on data will only grow should global laws that aim to mitigate them stall [47] and organisations continue to fail to catch & mitigate vulnerabilities before they are exploited [48].

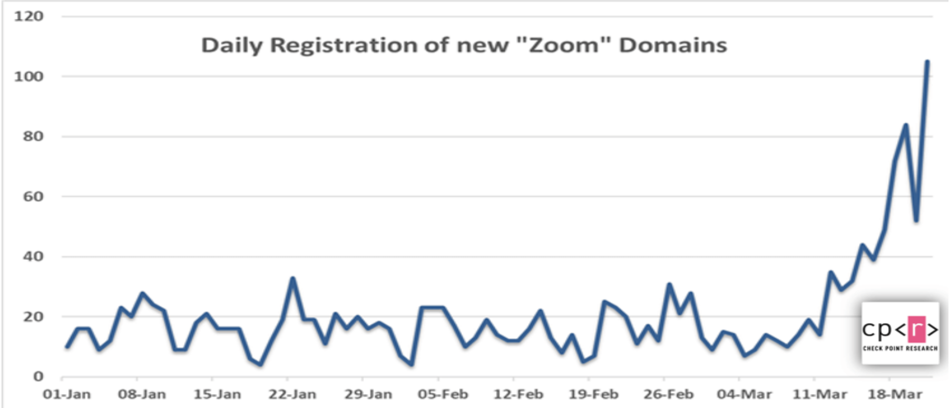


Figure 9: 2020 Domains registered including "zoom" in the name. Although some are benign, 4% were found to contain suspicious charecteristics according to Check point tech [45].

Conclusions

More data has been stored, shared, stolen and held-for-ransom than ever before during the coronavirus pandemic, however this is not a new concept to the world at large. Information can be used and abused for a multitude of reasons and comes in many different forms, each with their own value to the owner and attacker.

The analysis conducted has implied that interest in this data will continue and grow, perhaps even evolving into dynamic targeted attacks on specific institutions.

Regardless of whether interest will increase or not, we can say for sure that attackers (APT or not) will continue to tailor their techniques to the situation at hand, gaining as much of an advantage as they can in an increasingly digital and security conscious world.

Bibliography

[1] Y. McDermott, “Conceptualising the right to data protection in an era of Big Data,” 1 1 2017. [Online]. Available: https://journals.sagepub.com/doi/10.1177/2053951716686994. [Accessed 20 3 2021].

[2] netActivity, “PROTECTING YOUR DATA PRIVACY IS HARDER THAN EVER,” 24 9 2020. [Online]. Available: https://www.netactivity.us/protecting-your-data-privacy-is-harder-than-ever/. [Accessed 20 3 2021].

[3] J. B. Bump, F. Baum, M. Sakornsin, R. Yates and K. Hofman, “Political economy of covid-19: extractive, regressive, competitive,” 22 1 2021. [Online]. Available: https://www.bmj.com/content/372/bmj.n73. [Accessed 20 3 2021].

[4] N. Manworren, J. Letwat and O. Daily, “Why you should care about the Target data breach,” 5 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0007681316000033. [Accessed 21 3 2021].

[5] M. Ricardo and K. Cynthia, “Ransomware - Kidnapping personal data for ransom and the information as hostage,” 13 9 2018. [Online]. Available: https://gredos.usal.es/handle/10366/139223. [Accessed 21 3 2021].

[6] PurpleSec, “2020 Cyber Security Statistics (Data Breach Statistics),” 2021. [Online]. Available: https://purplesec.us/resources/cyber-security-statistics/#:~:text=The%20total%20number%20of%20breaches,95%25%20of%20all%20enterprise%20networks.. [Accessed 21 3 2021].

[7] C. Mondschein, R. Crutzen and G.-J. Ygram Peters, “Why and how we should care about the General Data Protection Regulation,” 21 5 2019. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/08870446.2019.1606222. [Accessed 21 3 2021].

[8] F. C. Braulin and T. Valletti, “Selling customer information to competing firms,” 12 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0165176516303974. [Accessed 21 3 2021].

[9] S. Mello, “Data Breaches in Higher Education Institutions,” 4 2018. [Online]. Available: https://scholars.unh.edu/cgi/viewcontent.cgi?article=1407&context=honors. [Accessed 21 3 2021].

[10] M. Riley, B. Elgin, D. Lawrence and C. Matlack, “Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It,” 17 3 2014. [Online]. Available: https://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data. [Accessed 21 3 2021].

[11] S. Saha, A. Das, A. Kumar, D. Biswas and S. Saha, “Ethical Hacking: Redefining Security in Information System,” 30 11 2019. [Online]. Available: https://link.springer.com/chapter/10.1007/978-981-15-0361-0_16. [Accessed 21 3 2021].

[12] T. Olavsrud, “11 Steps Attackers Took to Crack Target,” 2 9 2014. [Online]. Available: https://www.cio.com/article/2600345/11-steps-attackers-took-to-crack-target.html. [Accessed 21 3 2021].

[13] Tenable, “O'Reilly WebSite uploader.exe Arbitrary File Upload,” 19 1 2021. [Online]. Available: https://www.tenable.com/plugins/nessus/10291. [Accessed 21 3 2021].

[14] N. Marinos, “Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach,” 8 2018. [Online]. Available: https://www.warren.senate.gov/imo/media/doc/2018.09.06%20GAO%20Equifax%20report.pdf. [Accessed 21 3 2021].

[15] NATIONAL VULNERABILITY DATABASE, “CVE-2017-5638,” 24 2 2021. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2017-5638. [Accessed 21 3 2021].

[16] J. Fruhlinger, “Equifax data breach FAQ: What happened, who was affected, what was the impact?,” 12 2 2020. [Online]. Available: https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html. [Accessed 21 3 2021].

[17] K. Chinthapalli, “The hackers holding hospitals to ransom,” 10 5 2017. [Online]. Available: https://doi.org/10.1136/bmj.j2214. [Accessed 21 3 2021].

[18] M. Muthuppalaniappan and K. Stevenson, “Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health,” 27 9 2020. [Online]. Available: https://academic.oup.com/intqhc/article/33/1/mzaa117/5912483?login=true. [Accessed 21 3 2021].

[19] National Cyber Security Center, “UK and allies expose Russian attacks on coronavirus vaccine development,” 16 7 2020. [Online]. Available: https://www.ncsc.gov.uk/news/uk-and-allies-expose-russian-attacks-on-coronavirus-vaccine-development. [Accessed 21 3 2021].

[20] T. Floyd, M. Grieco and E. F. Reid, “Mining hospital data breach records: Cyber threats to U.S. hospitals,” 30 9 2016. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7745441. [Accessed 22 3 2021].

[21] Breach Level Index, “2016 Mining for Database Gold,” 2016. [Online]. Available: https://www.paymentscardsandmobile.com/wp-content/uploads/2017/04/Breach-Level-Index-Report.pdf. [Accessed 22 3 2021].

[22] V. Viala, “DATA BREACHES COMPROMISED 3.3 BILLION RECORDS IN FIRST HALF OF 2018,” 23 10 2018. [Online]. Available: https://www.thalesgroup.com/en/markets/digital-identity-and-security/press-release/data-breaches-compromised-3-3-billion-records-in-first-half-of-2018. [Accessed 22 3 2021].

[23] HIPAA Journal, “Healthcare Data Breach Statistics,” 2020. [Online]. Available: https://www.hipaajournal.com/healthcare-data-breach-statistics/. [Accessed 22 3 2021].

[24] SelfKey, “All Data Breaches in 2019 & 2020 – An Alarming Timeline,” 5 7 2020. [Online]. Available: https://selfkey.org/data-breaches-in-2019/. [Accessed 22 3 2021].

[25] H. S. Lallie, L. A. Shepherd, J. R. C. Nurse, A. Erola, G. Epiphaniou, C. Maple and X. Bellekens, “Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic,” 21 6 2020. [Online]. Available: https://arxiv.org/pdf/2006.11929.pdf. [Accessed 22 3 2021].

[26] C. P. Garrison and M. Ncube, “A longitudinal analysis of data breaches,” 11 10 2011. [Online]. Available: https://www.emerald.com/insight/content/doi/10.1108/09685221111173049/full/html. [Accessed 22 3 2021].

[27] S. Abraham and I. Chengalur-Smith, “An overview of social engineering malware: Trends, tactics, and implications,” 8 2010. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0160791X10000497. [Accessed 23 3 2021].

[28] T. Zink, “The top ten spam, malware and e-security stories of 2009,” 1 1 2010. [Online]. Available: https://www.virusbulletin.com/virusbulletin/2010/01/top-ten-spam-malware-and-e-security-stories-2009. [Accessed 23 3 2021].

[29] My Security Awareness, “What is Impersonation in Social Engineering?,” [Online]. Available: http://mysecurityawareness.com/article.php?article=384&title=what-is-impersonation-in-social-engineering. [Accessed 23 3 2021].

[30] A. Adamov and A. Carlsson, “The state of ransomware. Trends and mitigation techniques,” 29 9 2017. [Online]. Available: https://ieeexplore.ieee.org/document/8110056. [Accessed 23 3 2021].

[31] C. Singleton, C. Kiefer and O. Villadsen, “Ransomware 2020: Attack Trends Affecting Organizations Worldwide,” 28 9 2020. [Online]. Available: https://securityintelligence.com/posts/ransomware-2020-attack-trends-new-techniques-affecting-organizations-worldwide/. [Accessed 23 3 2021].

[32] L. Iacono, K. Wojcieszek and D. Ackerman, “Kroll Ransomware Attack Trends – 2020 YTD,” 6 10 2020. [Online]. Available: https://www.kroll.com/en/insights/publications/cyber/ransomware-attack-trends-2020. [Accessed 23 3 2021].

[33] M. Muthuppalaniappan and K. Stevenson, “Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health,” 27 9 2020. [Online]. Available: https://academic.oup.com/intqhc/article/33/1/mzaa117/5912483?login=true. [Accessed 23 3 2021].

[34] M. Muthuppalaniappan and K. Stevenson, “Summary of reported cyber-attacks/data breaches in healthcare and academic organisations during the COVID-19 outbreak,” 27 9 2020. [Online]. Available: https://academic.oup.com/view-large/228520012. [Accessed 23 3 2021].

[35] Department for Digital, Culture, Media and Sport, “Cyber security breaches survey 2017,” 2 2018. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf. [Accessed 23 3 2021].

[36] Q. Liao, “RANSOMWARE: A GROWING THREAT TO SMES,” 2007. [Online]. Available: http://www.swdsi.org/swdsi08/paper/swdsi%20proceedings%20paper%20s400.pdf. [Accessed 24 3 2021].

[37] A. Zwitter and O. J. Gstrein, “Big data, privacy and COVID-19 – learning from humanitarian expertise in data protection,” 4 5 2020. [Online]. Available: https://link.springer.com/content/pdf/10.1186/s41018-020-00072-6.pdf. [Accessed 24 3 2021].

[38] J. Grierson and H. Devlin, “Hostile states trying to steal coronavirus research, says UK agency,” 3 5 2020. [Online]. Available: https://www.theguardian.com/world/2020/may/03/hostile-states-trying-to-steal-coronavirus-research-says-uk-agency. [Accessed 24 3 2021].

[39] Threat Intelligence Team, Malwarebytes, “APTs and COVID-19: How advanced persistent threats use the coronavirus as a lure,” 9 4 2020. [Online]. Available: https://blog.malwarebytes.com/threat-analysis/2020/04/apts-and-covid-19-how-advanced-persistent-threats-use-the-coronavirus-as-a-lure/. [Accessed 24 3 2021].

[40] D. Ruiz, “Battling online coronavirus scams with facts,” 10 2 2020. [Online]. Available: https://blog.malwarebytes.com/social-engineering/2020/02/battling-online-coronavirus-scams-with-facts/. [Accessed 24 3 2021].

[41] Anna, Spin Technology, “24 Recent Ransomware Attacks in 2019,” 20 12 2019. [Online]. Available: https://spinbackup.com/blog/24-biggest-ransomware-attacks-in-2019/. [Accessed 24 3 2021].

[42] Center for Internet Security, “Top 10 Malware February 2019,” 2019. [Online]. Available: https://www.cisecurity.org/blog/top-10-malware-february-2019/. [Accessed 24 3 2021].

[43] A. Hern, “Covid19 could cause permanent shifttowards home working,” 6 11 2020. [Online]. Available: http://www.miamidadetpo.org/library/2020-03-13-uk-covid19-could-cause-permanent-shift-towards-home-working.pdf. [Accessed 24 3 2021].

[44] J. Holtzclaw and R. Sawyer, “Cybersecurity After COVID-19: 10 Ways to Protect Your Business and Refocus on Resilience,” 2021. [Online]. Available: https://coronavirus.marsh.com/us/en/insights/research-and-briefings/cybersecurity-after-covid-19.html. [Accessed 24 3 2021].

[45] Check Point, “COVID-19 Impact: Cyber Criminals Target Zoom Domains,” 2020. [Online]. Available: https://blog.checkpoint.com/2020/03/30/covid-19-impact-cyber-criminals-target-zoom-domains/. [Accessed 24 3 2021].

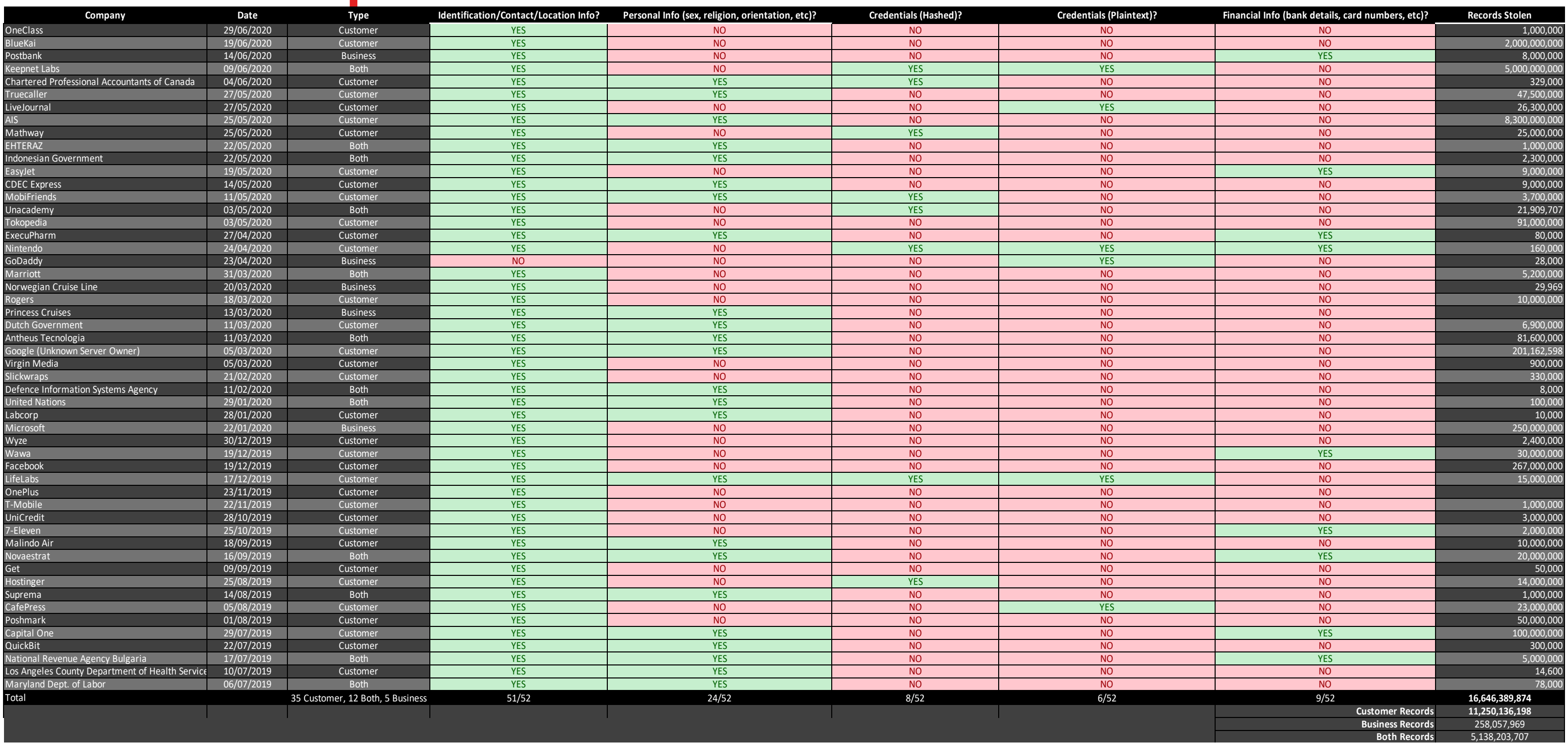
[46] B. Alibe, “Zoom & Doom: How INKY Unraveled A Credential Harvesting Phishing Scam,” 2020. [Online]. Available: https://www.inky.com/blog/zoom-doom-how-inky-unraveled-a-credential-harvesting-phishing-scam. [Accessed 24 3 2021].

[47] B. Edwards, S. Hofmeyr and S. Forrest, “Hype and heavy tails: A closer look at data breaches,” 30 12 2016. [Online]. Available: https://academic.oup.com/cybersecurity/article/2/1/3/2736315. [Accessed 24 3 2021].

[48] M. Ahmed, “Impact of Human Factors in Cloud Data Breach,” 30 11 2019. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-34387-3_70. [Accessed 24 3 2021].

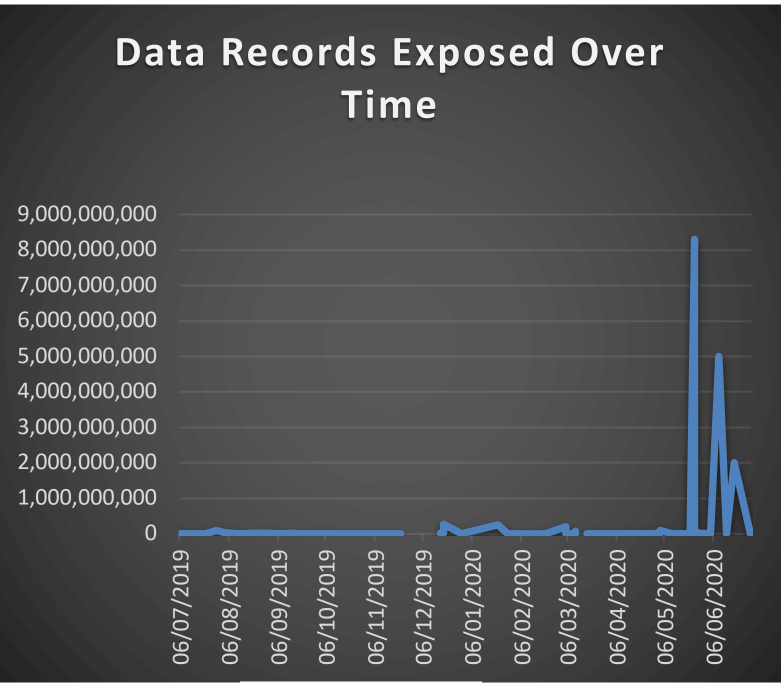
Appendix 1: Business vs Customer Data Exposures Q32019 – Q32020

Table 1



Company	Date	Type	Identification/Contact/Location Info?	Personal Info (sex, religion, orientation, etc)?	Credentials (Hashed)?	Credentials (Plaintext)?	Financial Info (bank details, card numbers, etc)?	Records Stolen
OneClass	29/06/2020	Customer	YES	NO	NO	NO	NO	1,000,000
BlueKai	19/06/2020	Customer	YES	NO	NO	NO	NO	2,000,000,000
Postbank	14/06/2020	Business	YES	NO	NO	NO	YES	8,000,000
Keepnet Labs	09/06/2020	Both	YES	NO	YES	YES	NO	5,000,000,000
Chartered Professional Accountants of Canada	04/06/2020	Customer	YES	YES	YES	NO	NO	329,000
Truecaller	27/05/2020	Customer	YES	YES	NO	NO	NO	47,500,000
LiveJournal	27/05/2020	Customer	YES	NO	NO	YES	NO	26,300,000
AIS	25/05/2020	Customer	YES	YES	NO	NO	NO	8,300,000,000
Mathway	25/05/2020	Customer	YES	NO	YES	NO	NO	25,000,000
EHTERAZ	22/05/2020	Both	YES	YES	NO	NO	NO	1,000,000
Indonesian Government	22/05/2020	Both	YES	YES	NO	NO	NO	2,300,000
EasyJet	19/05/2020	Customer	YES	NO	NO	NO	YES	9,000,000
CDEC Express	14/05/2020	Customer	YES	YES	NO	NO	NO	9,000,000
MobiFriends	11/05/2020	Customer	YES	YES	YES	NO	NO	3,700,000
Unacademy	03/05/2020	Both	YES	NO	YES	NO	NO	21,909,707
Tokopedia	03/05/2020	Customer	YES	NO	NO	NO	NO	91,000,000
ExecuPharm	27/04/2020	Customer	YES	YES	NO	NO	YES	80,000
Nintendo	24/04/2020	Customer	YES	NO	YES	YES	YES	160,000
GoDaddy	23/04/2020	Business	NO	NO	NO	YES	NO	28,000
Marriott	31/03/2020	Both	YES	NO	NO	NO	NO	5,200,000
Norwegian Cruise Line	20/03/2020	Business	YES	NO	NO	NO	NO	29,969
Rogers	18/03/2020	Customer	YES	NO	NO	NO	NO	10,000,000
Princess Cruises	13/03/2020	Business	YES	YES	NO	NO	NO	
Dutch Government	11/03/2020	Customer	YES	YES	NO	NO	NO	6,900,000
Antheus Tecnologia	11/03/2020	Both	YES	YES	NO	NO	NO	81,600,000
Google (Unknown Server Owner)	05/03/2020	Customer	YES	YES	NO	NO	NO	201,162,598
Virgin Media	05/03/2020	Customer	YES	NO	NO	NO	NO	900,000
Slickwraps	21/02/2020	Customer	YES	NO	NO	NO	NO	330,000
Defence Information Systems Agency	11/02/2020	Both	YES	YES	NO	NO	NO	8,000
United Nations	29/01/2020	Both	YES	YES	NO	NO	NO	100,000
Labcorp	28/01/2020	Customer	YES	YES	NO	NO	NO	10,000
Microsoft	22/01/2020	Business	YES	NO	NO	NO	NO	250,000,000
Wyze	30/12/2019	Customer	YES	NO	NO	NO	NO	2,400,000
Wawa	19/12/2019	Customer	YES	NO	NO	NO	YES	30,000,000
Facebook	19/12/2019	Customer	YES	NO	NO	NO	NO	267,000,000
LifeLabs	17/12/2019	Customer	YES	YES	YES	YES	NO	15,000,000
OnePlus	23/11/2019	Customer	YES	NO	NO	NO	NO	
T-Mobile	22/11/2019	Customer	YES	NO	NO	NO	NO	1,000,000
UniCredit	28/10/2019	Customer	YES	NO	NO	NO	NO	3,000,000
7-Eleven	25/10/2019	Customer	YES	NO	NO	NO	YES	2,000,000
Malindo Air	18/09/2019	Customer	YES	YES	NO	NO	NO	10,000,000
Novaestrat	16/09/2019	Both	YES	YES	NO	NO	YES	20,000,000
Get	09/09/2019	Customer	YES	NO	NO	NO	NO	50,000
Hostinger	25/08/2019	Customer	YES	NO	YES	NO	NO	14,000,000
Suprema	14/08/2019	Both	YES	YES	NO	NO	NO	1,000,000
CafePress	05/08/2019	Customer	YES	NO	NO	YES	NO	23,000,000
Poshmark	01/08/2019	Customer	YES	NO	NO	NO	NO	50,000,000
Capital One	29/07/2019	Customer	YES	YES	NO	NO	YES	100,000,000
QuickBit	22/07/2019	Customer	YES	YES	NO	NO	NO	300,000
National Revenue Agency Bulgaria	17/07/2019	Both	YES	YES	NO	NO	YES	5,000,000
Los Angeles County Department of Health Service	10/07/2019	Customer	YES	YES	NO	NO	NO	14,600
Maryland Dept. of Labor	06/07/2019	Both	YES	YES	NO	NO	NO	78,000
Total		35 Customer, 12 Both, 5 Business	51/52	24/52	8/52	6/52	9/52	**16,646,389,874**
							Customer Records	**11,250,136,198**
							Business Records	258,057,969
							Both Records	5,138,203,707

A zoomable version of the table and graphs below is viewable here: *https://liveplymouthac-my.sharepoint.com/:x:/g/personal/morgan_davies_students_plymouth_ac_uk/Ebj7i9gJ6epGrmkXTlRrpFwBBd6yHSmwMmOw67aWMtGgMw?e=XAtyVi*
Table 1 was created by parsing SelfKey's publically available breach data [24] and various sources regarding each individual breach. Graphs 1 & 2 were generated from Table 1's data. With regards to the no. of records, values are either exact values or my approximate estimates from compiling available information on the relevent breaches. Ommited values imply that even approximate values are unable to be calculated (e.g. not enough info on the breach).

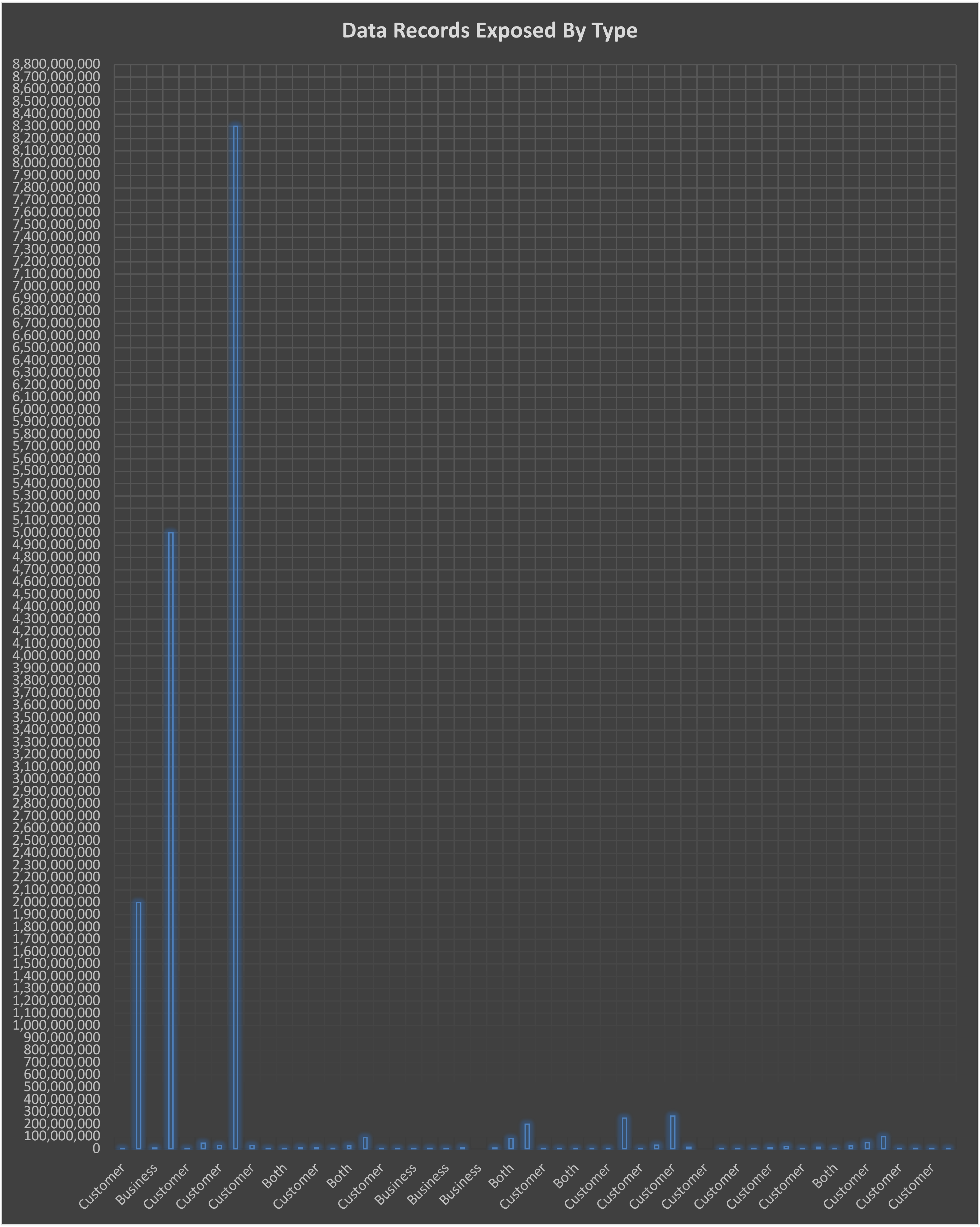


Graph 1

Graph 1 depicts how data has been exposed over time. Towards mid 2020 there is a clear spike in records exposed, chronally speaking. This reflects modern claims that data breaches are more common in the era of covid [25]. Futhermore, Graph 2 gathers breaches by type in reverse chronological order, we see a trend that supports this theory. Proportionally speaking, the situations with a high number of records exposed is clusters in Q1/Q2 2020.

However, look at Table 1 again. The total number of customer records exposed is over double the number of mixed and business records. This contradicts a long running theory that attacks on businesses produce a greater number of stolen records than customer ones [26].

Graph 2


Data Records Exposed By Type
8,800,000,000
8,700,000,000
8,600,000,000
8,500,000,000
8,400,000,000
8,300,000,000
8,200,000,000
8,100,000,000
8,000,000,000
7,900,000,000
7,800,000,000
7,700,000,000
7,600,000,000
7,500,000,000
7,400,000,000
7,300,000,000
7,200,000,000
7,100,000,000
7,000,000,000
6,900,000,000
6,800,000,000
6,700,000,000
6,600,000,000
6,500,000,000
6,400,000,000
6,300,000,000
6,200,000,000
6,100,000,000
6,000,000,000
5,900,000,000
5,800,000,000
5,700,000,000
5,600,000,000
5,500,000,000
5,400,000,000
5,300,000,000
5,200,000,000
5,100,000,000
5,000,000,000
4,900,000,000
4,800,000,000
4,700,000,000
4,600,000,000
4,500,000,000
4,400,000,000
4,300,000,000
4,200,000,000
4,100,000,000
4,000,000,000
3,900,000,000
3,800,000,000
3,700,000,000
3,600,000,000
3,500,000,000
3,400,000,000
3,300,000,000
3,200,000,000
3,100,000,000
3,000,000,000
2,900,000,000
2,800,000,000
2,700,000,000
2,600,000,000
2,500,000,000
2,400,000,000
2,300,000,000
2,200,000,000
2,100,000,000
2,000,000,000
1,900,000,000
1,800,000,000
1,700,000,000
1,600,000,000
1,500,000,000
1,400,000,000
1,300,000,000
1,200,000,000
1,100,000,000
1,000,000,000
900,000,000
800,000,000
700,000,000
600,000,000
500,000,000
400,000,000
300,000,000
200,000,000
100,000,000
0
Customer
Business
Customer
Customer
Customer
Both
Customer
Both
Customer
Business
Business
Business
Both
Customer
Both
Customer
Customer
Customer
Customer
Customer
Customer
Customer
Both
Customer
Customer
Customer