EasyChair Preprint

№ 10793

Australia's Notifiable Data Breach Scheme: an Analysis of Risk Management Findings for Healthcare

Martin Dart and Mohiuddin Ahmed

August 28, 2023

Australia's Notifiable Data Breach scheme: An analysis of risk management findings for healthcare

Martin Dart [0000-0002-2035-8232] and Mohiuddin Ahmed [0000-0002-4559-4768]

School of Science, Edith Cowan University, Joondalup WA 6027, Australia.
m.dart@ecu.edu.au

Abstract. This paper provides an overview of the first five years of data published via the Australian Governments' Notifiable Data Breach (NDB) scheme, operated by the Office of the Australian Information Commissioner (OAIC). Applying investigative techniques including descriptive and inferential statistics, Pareto analysis, distribution analysis, and bivariate correlations it is discovered that 80% of data breach incidents are substantively caused by fives forms of human error, particularly failures in email management. A deeper investigation across each of the periods studied reveals significant correlations often involve insider-based threats, suggesting these can be an indicative predictor for other events such as phishing and ransomware attacks. The included summary of increasing privacy concerns from the public and government-led legislative amendments in Australia, further illustrates the urgency and importance of applying this knowledge to the critical infrastructure of healthcare.

Keywords: Healthcare, Data breach, Cyber security.

1. Introduction

There have been many media and industry reports claiming healthcare is the most breached, attacked, or vulnerable industry in Australia [1-3], but seeking confirmatory data beyond the headlines is challenging given the stigma attached to such events. However, learning from data breach mistakes of the past is an important risk management technique [4], and very relevant in the complex field of assuring the digital transformations currently underway in many large Australian healthcare providers (LAHPs).

Khan [5] defines a data breach as, "*a security incident in which sensitive, protected, or confidential data are copied, transmitted, viewed, stolen, or used by an unauthorised individual*", and a similar definition was arrived at by Hendee [6], "*…a confirmed incident in which sensitive, confidential or otherwise protected data has been accessed and/or disclosed in an unauthorised fashion*". Previous analyses of healthcare data breaches [7-9] have tended to rely on figures from the United States due to their 1996 adoption of the *Health Insurance Accountability and Portability Act* (HIPAA), which introduced a mandatory data breach reporting scheme. Since implementation began via the Department of Health and Human Services (DHHS) that scheme has recorded 5,501 healthcare incidents over fourteen years, leading to breaches of 435 million patient records [10]. Reviewers of this data include Collins [11] who concluded that the Federal Government legislated approach was essential in ensuring compliance and

transparency, and Raghupathi [12] who used a variety of charting and mapping techniques that showed these breach events occurring in every US state.
The United Kingdom also enacted a similar scheme via the *Data Protection Act 2018 (UK)*, with breaches recorded and published by the Information Commissioners Office (ICO). Between 2019-2022 there were 15,629 healthcare breaches recorded in the UK, making it the second most impacted sector in the UK after education [13].

In Australia the *Privacy Act 1988 (Cth)* defines data breaches as, "an act or practice… contrary or inconsistent with any of the Australian Privacy Principles" [14]. Since being amended in 2018 the Act has required many organisations to report such breaches via a mandatory Notifiable Data Breach (NDB) scheme, administered by the Office of the Australian Information Commissioner (OAIC), and this has recorded 929 such incidents occurring in healthcare [15]. Yet while this requirement applies to all private LAHPs in Australia it is not enforceable against all state government agencies delivering public services. This is an important issue to note as it means there is still no single mandatory national scheme, and those exclusions include some of the largest healthcare systems treating millions of patients. This was noted by Hile [16], who concluded that while the Privacy Act and NDB scheme creates in theory an effective liability attribution framework to identify data breaches, it does little to empower impacted individuals with subsequent access to court action or compensation. However, this is a rapidly changing situation and other laws have been tightened (and penalties increased) in response to millions of Australians having their privacy breached via incidents at Optus (telecommunications) and Medibank (health insurance) in 2022 [17]. The most recent major change occurred in 2022 when the Australian Government amended the *Security of Critical Infrastructure Act 2018 (Cth)* to apply to healthcare for the first time, demanding greater risk governance and reporting from LAHP executives including all state entities previously excluded from the Privacy Act [18, 19]. The small sample of media-reported incidents shown at Table 1 illustrates a range of impacts and causes, but to fully understand and manage the risk from data breach events LAHPs need a deeper understanding. This paper uses detailed techniques to analyse the first five years of data from the NDB, to seek conclusions that can practically assist with this.

Table 1. Select Australian healthcare data breaches 2018-2022.

Provider	Incident	Cause	Year
Health Engine	59,600 items of 'patient feedback' accessed [20]	Website misconfiguration	2018
Cabrini Hospital Melbourne Heart Group	15,000 patient records encrypted by malware. Attempts to pay the ransom failed to recover the data [21]	Unpatched systems and malware	2019
Victoria Health	Multiple sites attacked, and numerous systems impacted over several weeks. Multiple surgeries cancelled [22]	Emotet malware	2019
Tasmanian Ambulances	Unencrypted radio transmissions intercepted and posted online [23]	Legacy communications	2021
Eastern Health	Elective surgeries cancelled across 4 Melbourne hospitals [24]	Ransomware	2021
Medibank	A 200Gb database containing approx. 9.7 million customer records stolen [25]	Phishing attack (stolen privileged credentials)	2022

2. Methods

To date the OAIC has recorded NDB scheme data for all industries across 12 periods. This commenced from April 2018 with 5 quarterly reports, and from July 2019 a further 7 reports have been issued covering 6-month intervals [15]. Healthcare data was extracted from this full set to identify the following measures:

1. Descriptive and inferential statistics:
   a. Total occurrences of 4 high-level breach cause categories
   b. Total occurrences of 22 detailed breach cause categories
2. Temporal trends (for 5 x annually aggregated and 12 individual periods):
   a. 2018 – 2022 trend of 4 high-level breach cause categories
   b. 2018 – 2022 trend of 22 detailed breach cause categories
3. Analysis:
   a. A Pareto distribution evaluation to establish the most impactful causes
   b. A Pearsons correlation of the top-10 causes to establish *r* & *P* values

2.1 Descriptive statistics for high level data breach causes

Between 2018-2022 there were *N*=929 data breaches reported by eligible Australian healthcare entities, using the four high-level classifications shown in Figure 1.

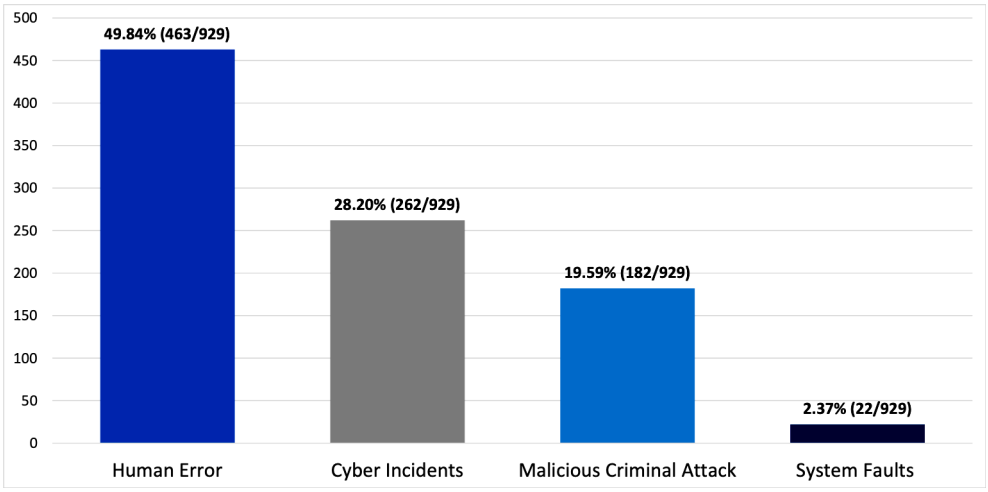

Figure 1. Australian healthcare data breaches by high level cause, 2018-2022 (*N*=929).

2.2 Descriptive statistics for detailed data breach causes

Within the four high-level classifications (represented by the first 2 letters of each code) further detail is captured to provide 22 specific data breach causes, detailed at Table 2. While the high-level descriptions capture overall risk categories, these detailed causes show exactly how those risks are materialising and this is where LAHPs can begin to extract specific lessons from the data.

Table 2. Data breach causes - detailed categories with definitions.

Category	Detailed Cause	Definition (as per OAIC)
1. (CI) Cyber incidents	CI1: Brute force	Automated software used to generate a large number of consecutive guesses as to the value of the desired data, for example, passwords.
	CI2: Hacking (other means)	Unauthorised access to a system or network (other than by phishing, brute-force, or malware), to exploit system data or manipulate its behaviour.
	CI3: Ransomware	A type of malicious software designed to block access to data or a computer system until a sum of money is paid or other conditions are met.
	CI4: Compromised/stolen credentials (method unknown)	Credentials are compromised or stolen by methods unknown.
	CI5: Phishing (credentials compromised)	Untargeted mass messages asking users for information, to open a malicious attachment, or visit a fake website.
	CI6: Malware (malicious software)	Software used to gain unauthorised access to computers, steal information and disrupt or disable networks (i.e., trojans, viruses and worms).
	CI7: Other	-
2. (HE) Human error	HE1: Failed to use BCC	Sending a group email with all recipient email addresses in the 'To' field, thereby disclosing all email addresses to all recipients.
	HE2: Loss or insecure disposal of paperwork or devices	Disposing of information in a manner that could lead to its unauthorised disclosure (i.e., using a public rubbish bin to dispose of customer records).
	HE3_Email incorrectly sent	Personal information sent to the wrong recipient via email (i.e., as a result of a misaddressed email or having a wrong address on file).
	HE4: PI incorrectly faxed	Personal information sent to the wrong recipient via fax (i.e., a result of an incorrectly entered fax number or having a wrong fax number on file).
	HE5: PI incorrectly mailed	Personal information sent to the wrong recipient via postal mail (i.e., as a result of a transcribing error or having a wrong address on file).
	HE6: PI incorrectly sent (other)	Personal information sent to the wrong recipient via channels other than email, fax or mail (i.e., delivery by hand or uploading to a web portal).
	HE7: Failure to redact	Failure to effectively de-identify a record before disclosing it.
	HE8: Unauthorised release or publication	Unauthorised disclosure of personal information in a written format, including paper documents or online.
	HE9: Unauthorised verbal disclosure	Disclosing personal information verbally without authorisation (i.e., calling it out in a waiting room).
	HE10: Other	-
3. (MC) Malicious or criminal attack	MC1: Rogue employee	Employee or insider/contractor acting against the interests of their employer.
	MC2: Social engineering or impersonation	An attack that exploits human interaction to manipulate people into breaking normal security procedures to gain access to systems, networks or locations.
	MC3: Paperwork/device theft	Theft of paperwork or data storage device.
4. (SF) System faults	SF1: Unintended access	Business or technology process errors not caused by direct human error.
	SF2: Unintended release or publication	

Figure 2 presents the data from all 12 periods and shows the 22 detailed breach reasons arranged in order, from the most regularly reported at the furthest peak. This illustrates the differing scale of occurrences stemming from prevalent causes such as email being incorrectly addressed or phishing, as opposed to much rarer threats from unintended access or brute force attacks. The same data is also presented in descending order of frequency at Table 3 and includes the mean occurrence for each incident reason per year (μ), and its representative percentage across all five years of incidents.

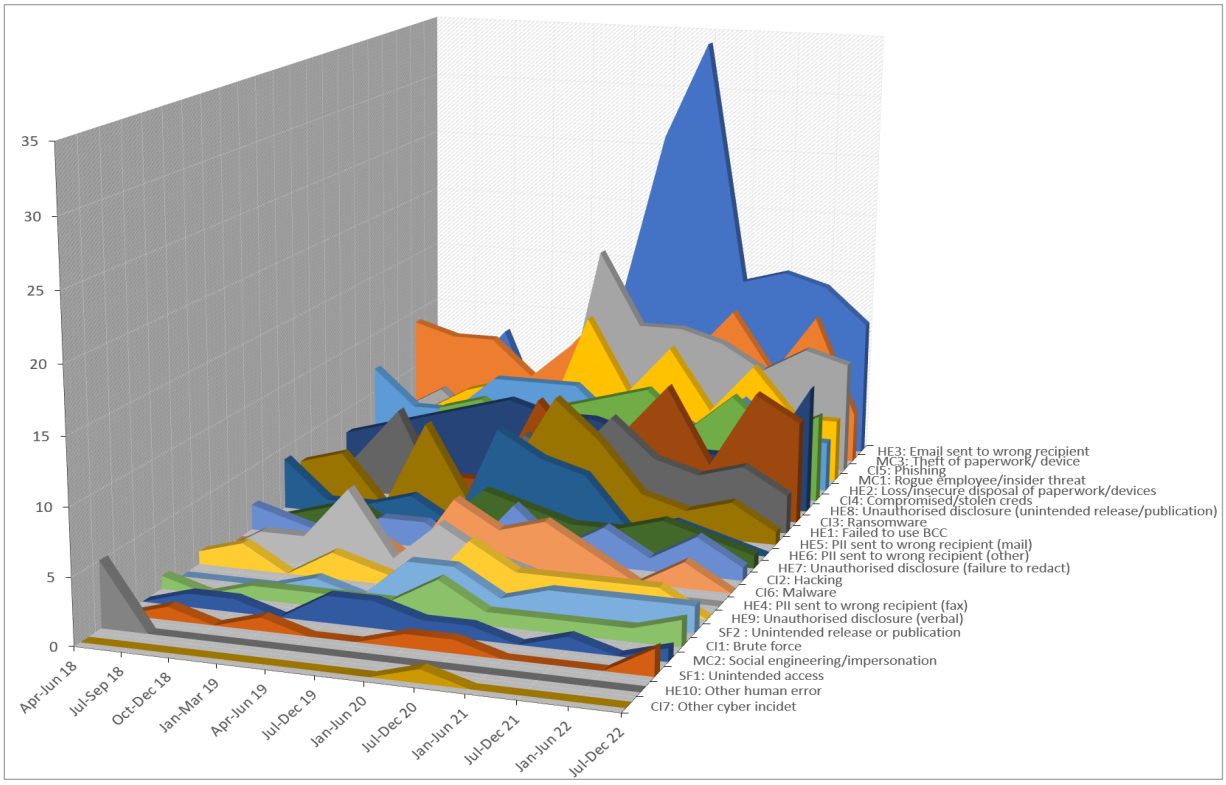

Figure 2. Detailed data breach causes for 12 periods 2018-2022.

The inclusion of cumulative totals at columns B and E of Table 3 reveals the majority of incidents (751/929, 80.84%) were attributed to a minority of detailed cause categories (10/22, 45%). The most frequently occurring specific cause is shown as 'HE3_Email sent to wrong recipient', responsible for 151/929 (16.25%, μ=30.20) of all incidents over 5 years.

Table 3. Detailed data breach causes by total 2018-2022.

No.	CAUSE	A: Total (/929)	B: Cumulative total	C: μ (Per year)	D: % of all breaches	E: Cumulative %
1	HE3_Email sent to wrong recipient	151	151	30.20	16.25%	16.25%
2	MC3_Theft of paperwork/ device	100	251	20.00	10.76%	27.02%
3	CI5_Phishing	087	338	17.40	09.36%	36.38%
4	MC1_Rogue Employee/ Insider threat	072	410	14.40	07.75%	44.13%
5	HE2_Loss/insecure disposal	065	475	13.00	07.00%	51.13% (k_0)
6	CI4_Compromised/stolen creds	064	539	12.80	06.89%	58.02%
7	HE8_Unauthorised disclosure	064	603	12.80	06.89%	64.91%
8	CI3_Ransomware	058	661	11.60	06.24%	71.15%
9	HE1_Failed to use BCC	045	706	09.00	04.84%	76.00%
10	HE5_PI sent to wrong recipient (mail)	045	751	09.00	04.84%	80.84% (k_1)

11	HE6_PI sent to wrong recipient (other)	031	782	06.20	03.34%	84.18%
12	HE7_Unauthorised disclosure (unredacted)	021	803	04.20	02.26%	86.44%
13	CI2_Hacking	020	823	04.00	02.15%	88.59%
14	CI6_Malware	018	841	03.60	01.94%	90.53%
15	HE4_PI sent to wrong recipient (fax)	018	859	03.60	01.94%	92.47%
16	HE9_Unauthorised disclosure (verbal)	018	877	03.60	01.94%	94.40%
17	SF2_Unintended Release or publication	016	893	03.20	01.72%	96.12%
18	CI1_Brute force	014	907	02.80	01.51%	97.63%
19	MC2_Social engineering/impersonation	010	917	02.00	01.08%	98.71%
20	SF1_Unintended Access	006	923	01.20	00.65%	99.35%
21	HE10_Other	005	928	01.00	00.54%	99.89%
22	CI7_Other	001	929	00.20	00.11%	100.0%

2.3 Pareto analysis

The data from Table 3 is further investigated using a Pareto analysis, shown at Figure 3, which seeks to verify if there is any pattern of "predictable imbalance [26]" present in the data set. Using a standard Pareto approach the dataset shown at Figure 3 is arranged in descending order of frequency, using annual μ, with an overlay line (in blue) showing the cumulative % of N as each new breach cause is introduced. Also depicted are two boundary zones: k_0, where $n \leq 50\%$ of N, and k_1 where $n \leq 80\%$ of N. The mapping of the k_1 zone achieves the goal of this Pareto analysis, being the identification of those "vital few [27]" items which represent 80% of the data breach risk. To calculate the threshold values for these zones, formulae (1) and (2) were applied to Column C of Table 3:

$$k_0 = \sum_{i=1}^{5} x_i \quad (1)$$

$$k_1 = \sum_{i=1}^{10} x_i \quad (2)$$

This analysis shows that k_0 = 51.13% (475/929), and is comprised of just five specific causes, being in descending order: 1) incorrect emailing, 2) physical theft, 3) phishing attacks, 4) rogue employees or insider threats, and 5) insecure disposal. Where k_1 = 80.84% (751/929), an additional five causes contribute to the effect, bringing the total number of causes to ten: 6) compromised credentials, 7) unauthorised publication or release of data, 8) ransomware attacks, 9) failure to use BCC fields in email, and 10) PI data being posted incorrectly.

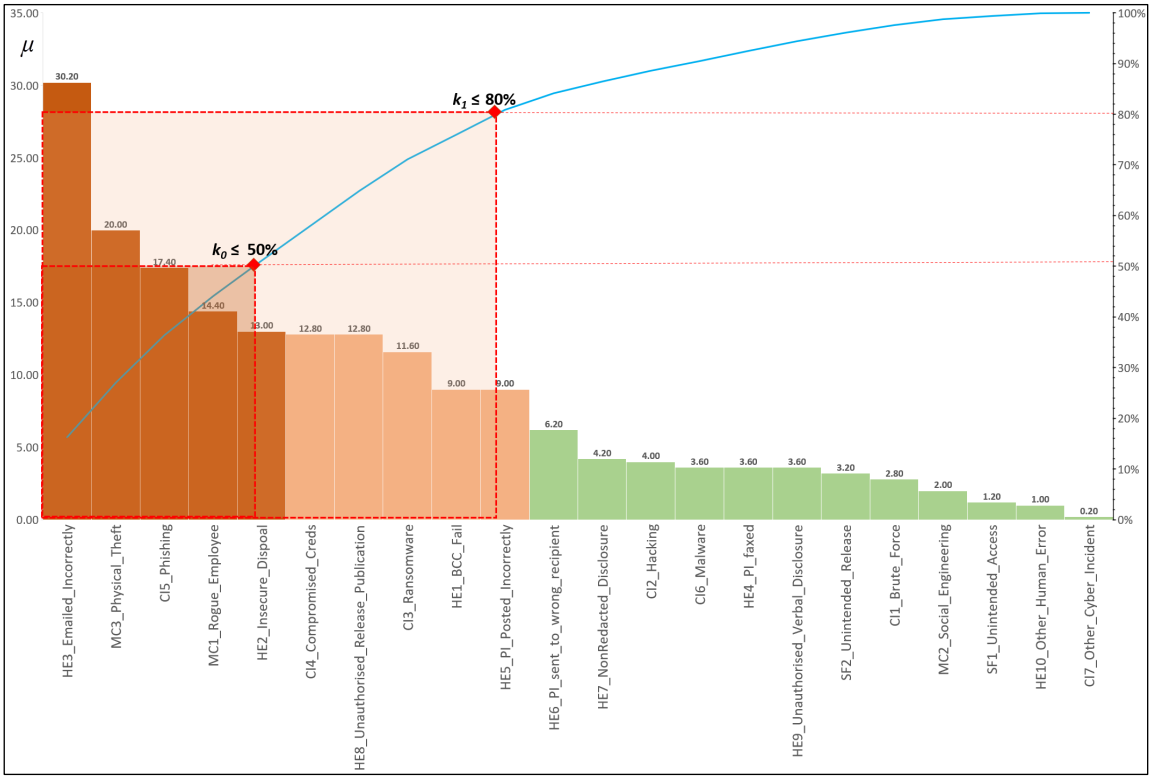

Figure 3. Pareto analysis of μ 2018-2022 (highlighting k_0 & k_1 boundaries).

The Pareto analysis provides the detail confirming the ten specific data breach causes (the "vital few", or the k_1 breach threshold) which accounts for 751/929 (80.84%) of all incidents. Within k_1 370/751 (49.26%) of incidents are attributable to elements of 'human error', 209/751 (27.82%) were identified as 'cyber incidents', and 172/751 (22.92%) 'malicious criminal acts'.

2.4 Correlation of data breach causes

To establish if there are any temporal linear relationships occurring within the k_1 data, each of the contributing causes from that region was assessed using a bivariate correlation analysis within SPSS[1]. This analysis was intended to measure the strength of relationship between each pair within the k_1 threshold (using the Pearsons correlation, or r value), and the significance of that relationship (the P value).

The default, or null hypothesis (H_0) for this evaluation was that one type of data breach would not be significantly correlated to any other another (P=0). In this case, for example, increases in phishing data breaches would not lead to regular increases in physical

[1] Software used for analysing results and creating charts was Microsoft Excel V2301 Build 16.0.16026.20196, and IBM SPSS Statistics V29.0.0.0 (241).

theft incidents within the same reporting period. If such relationships could however be demonstrated via an alternative hypothesis (H_a or $P \neq 0$), they could further increase the power of the Pareto analysis findings by offering a refinement in defining the most problematic data breach cause reasons from within k_1.

While the Pareto analysis was evaluated using total annual figures (x5) to obtain μ, the bivariate correlation analysis has been executed against the measures from all 12 periods as originally reported by the OAIC, in order to increase the temporal count and establish a more reliable P value. This output is presented at Table 4, where strong significance is shown in bold italics and moderate significance is in italics only.

Table 4. Pearsons correlation of k_1 data breach reasons (evaluated over 12 periods).

			CI3	CI4	CI5	HE1	HE2	HE3	HE5	HE8	MC1	MC3
CI3	Ransomware	Pearson Correlation	--									
		Sig. (2-tailed)										
CI4	Compromised_Creds	Pearson Correlation	.422	--								
		Sig. (2-tailed)	.172									
CI5	Phishing	Pearson Correlation	***.741****	.539	--							
		Sig. (2-tailed)	***.006***	.071								
HE1	BCC_Fail	Pearson Correlation	*.628**	.446	.576	--						
		Sig. (2-tailed)	*.029*	.146	.050							
HE2	Insecure_Dispoal	Pearson Correlation	-.433	.092	-.099	-.397	--					
		Sig. (2-tailed)	.160	.776	.758	.201						
HE3	Emailed_Incorrectly	Pearson Correlation	.415	*624**	*.599**	*652**	-.166	--				
		Sig. (2-tailed)	.180	*.030*	*.040*	*.022*	.606					
HE5	PII_Posted_Incorrectly	Pearson Correlation	-.111	.270	.358	.049	.026	.480	--			
		Sig. (2-tailed)	.732	.397	.253	.880	.937	.114				
HE8	Unauthorised_Release_Publication	Pearson Correlation	.120	.391	.126	-.126	-.086	-.012	-.083	--		
		Sig. (2-tailed)	.711	.208	.697	.697	.791	.970	.798			
MC1	Rogue_Employee	Pearson Correlation	.385	*704**	***746****	*594**	.355	.516	.290	.050	--	
		Sig. (2-tailed)	.217	*.011*	***.005***	*.042*	.257	.086	.361	.877		
MC3	Physical_Theft	Pearson Correlation	.503	-.260	.397	.375	-.062	.113	-.107	-.565	.169	--
		Sig. (2-tailed)	.095	.414	.201	.230	.849	.726	.740	.056	.600	

* Correlation is significant at the 0.05 level (2-tailed).

** Correlation is significant at the 0.01 level (2-tailed).

The relationships considered relevant by this analysis include the finding of both strong and moderately positive associations, and these are detailed further in Table 5.

Table 5. Evaluation of significant linear correlations.

1st Measure		2nd Measure	*r* value	*P* value
Strong positive associations (H_a is proven)				
MC1_Rogue_Employee	→	**CI5_Phishing**	**.746**	**.005**
The strongest correlation uncovered in this analysis shows the danger in rogue employees, who are more likely to engage in reckless online behaviour and are more likely to be targeted in phishing attacks.				
CI5_Phishing	→	**CI3_Ransomware**	**.741**	**.006**
This strong correlation is strongly supported by real world experience, where users interacting with phishing emails are likely to execute malicious code that initiates a ransomware attack.				
Moderate positive associations (H_a is accepted)				
HE1_BCC_Fail	→	**CI3_Ransomware**	**.628**	**.029**
A strong association with average significance, but the implications of poor BCC use as shown here as a means by which compromised emails expose large BCC lists to subsequent ransomware attackers.				
HE3_Emailed_Incorrectly	→	**CI4_Compromised_Credentials**	**.624**	**.030**
Another strong association and average significance, but yet another means by which bad email practice can be exploited to initiate scam conversations that lead to compromised credentials.				
HE3_Emailed_Incorrectly	→	**CI5_Phishing**	**.599**	**.040**
A strong association and average significance, this suggests bad email practices can lead to 'replay' attacks when incorrect recipients leak valid email addresses to malicious attackers who can then target organisations.				
HE3_Emailed_Incorrectly	→	**HE1_BCC_Fail**	**.652**	**.022**
On the border of a very strong association, this further demonstrates the need to be mindful of good email usage behaviours, as seen in other associations above this is an association that can lead to ransomware attacks.				
MC1_Rogue_Employee	→	**CI4_Compromised_Credentials**	**.704**	**.011**
A near very strong correlation, suggesting that rogue employees can have a devastating impact on an organisation, particularly if they are the holder of privileged credentials that are breached.				
MC1_Rogue_Employee	→	**HE1_BCC_Fail**	**.594**	**.042**
While moderate in its association, this relationship is indicative of how a de-motivated or malicious insider can make mistakes (or deliberately misuse) process in order to cause an incident to 'get back' at their employer.				

3. Principal Results

The analysis undertaken by this paper has shown that in Australia the most significant data breach risk for LAHPs stems from 'human error' based incidents with a mean annual occurrence of $\mu = 92.60$, which over 5 years has resulted in 463/929 (49.84%) of all reported data breaches to the NDB scheme. The most persistent threat within this category that has caused the largest number of data breaches across all periods (151/929, 16.25%, $\mu = 30.20$) is sensitive data being emailed to the wrong recipient.

The Pareto analysis has shown that the classic 80:20 rule holds true for this data set, with 751/929 (80.84%) of all data breaches triggered by a "vital few" of 10 repeated data breach causes. Within this priority set (k_1) the strongest contributor was again confirmed as coming from five different forms of 'human error' which between them caused 370/751 (49.26%) of those incidents.

Finally, the linear correlation analysis has shown that for this sample, there are strong indicators that increases in rogue employee associated data breaches can lead to increases in phishing attack breaches ($r = .746$, $P = .005$), and that successful phishing attacks are associated with ransomware data breaches ($r = .741$, $P = .006$).

4. Discussion

The phased approach undertaken for the analysis of this data set supports the hypothesis that human factors are contributing a significant degree to data breaches in LAHP environments. Not only are human factors the single largest contributor, but they are also embedded and persistent in their re-occurrence so cannot be dismissed as only "a few bad apples" doing the wrong thing.

In looking beyond the statistics focussed only the volume of data breaches, the Pareto and linear correlation analyses confirm that LAHPs should consider a holistic approach to learning the lessons from this data. This includes developing a greater awareness of those relationships which can make one type of data breach an enabler, or amplifier, of others. For example, the Pareto chart (Figure 3) shows that while 5 of the top 10 data breach reasons are human error generated, relative positions 2-4 on the *X* axis also generate significant events due to malicious targeted attacks and other cyber incidents. The correlation analysis further confirms the power of these linkages with repeated insider threats and email-related failures in particular leading to incidents of phishing, compromised credentials, and ransomware which have all been shown to have had repeated and devastating effects on healthcare providers across Australia (as shown at Table 1).

Worthy of note at the opposite end of the scale is the dearth of data breaches resulting from system faults. This puts some doubt on users who may claim "I never touched anything" when things go wrong in the event of a data breach. Very rarely (only in 22/929, or 2.37% of cases over 5 years) has faulty software or hardware resulted in data breaches, which again supports the fact that systems are unlikely to do bad things unless directed to do so by a human operator.

4.1 Limitations and future work

The data breach statistics produced by the OAIC contain inherent limitations, due to restraints in the *Privacy Act 2018 (Cth)* which still do not require all large government-run LAHPs to report all data breach events. It should be noted that legislative review is currently underway by the Australian Government, with amendments already enacted to the *Security of Critical Infrastructure Act 2018 (Cth)* which will require greater board-level risk management and reporting of cyber security incidents by LAHPs from 2023 onwards. A new *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022 (Cth)* has also been enacted, which greatly increases the financial penalties for privacy data breaches [28]. A Privacy Act Review Report, published in 2023 by the Attorney-General's Department [29], is also seeking public feedback on further proposals to strengthen the Commonwealth's Privacy Act, including enhanced data breach reporting requirements. As these amendments come into effect and provide extended data sets to the research community, this work can be re-visited and expanded to examine if the trends identified in this paper continue or diverge.

It should also be noted that the correlations undertaken at Table 3 are only representative of the currently sampled population within the scope of this paper, and further analysis of related data sets (such as those provided by the UK or USA) could explore the correlations identified there to great benefit.

5. Conclusions

This paper has shown there is significant and urgently needed value to be gained from analysing the NDB scheme data for Australia's healthcare industry. Not only does this allow them to learn from the mistakes and bad fortune of others, but it can also contribute significantly to avoiding future public distrust and legal implications as the national governance environment matures. For LAHPs this has highlighted the need to accept that the highly diverse nature of their very large workforces, which can number in the tens of thousands of employees per organisation, represents a significant risk vector as healthcare adopts ever more digital ways of working. By focussing on improving risk governance, staff awareness and training, incident reporting, and daily monitoring of systems there is great potential to halt the rising tide of healthcare privacy breaches which the first five years of NDB data have evidenced.

References

1. Australian Broadcasting Corporation (ABC). Healthcare industry continues to be main target of data breaches, with 79 reported in six months. 2022 [07/01/2023]; Available from: https://www.abc.net.au/news/science/2022-11-10/data-breach-medibank-healthcare-system/101612056.
2. Australian Cyber Security Magazine. Cyberattacks on Australian Healthcare Doubles. Australian Cyber Security Magazine. 2022.
3. Landi H. Relentless cyberattacks are putting financial pressure on hospitals: Fitch Ratings. Fierce Healthcare [10/12/2022]; Available from: https://www.fiercehealthcare.com/tech/relentless-cyber-attacks-are-putting-pressure-hospital-finances-fitch-ratings.
4. Fleury-Charles A, Chowdhury MM, Rifat N, editors. Data Breaches: Vulnerable Privacy. 2022 IEEE International Conference on Electro Information Technology (eIT); 2022; Minnesota State University, USA: IEEE.
5. Khan F, Kim JH, Mathiassen L, Moore R. Data breach management: An integrated risk model. Information & Management. 2021;58(1):103392.
6. Hendee LA. The Data Breach Epidemic: A Modern Legal Analysis. Journal of Technology Law & Policy. 2021;24(1):3.
7. Seh AH, Zarour M, Alenezi M, Sarkar AK, Agrawal A, Kumar R, et al., editors. Healthcare data breaches: insights and implications. Healthcare; 2020: MDPI.
8. Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care. 2017;25:1-10. doi: 10.3233/THC-161263.
9. Chernyshev M, Zeadally S, Baig Z. Healthcare Data Breaches: Implications for Digital Forensic Readiness. Journal of Medical Systems. 2018 2018/11/28;43(1):7. doi: 10.1007/s10916-018-1123-2.
10. U.S. Department of Health and Human Services. Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. 2023 [5/8/2023]; Available from: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.
11. Collins JD, Sainato VA, Khey DN. Organizational Data Breaches 2005-2010: Applying SCP to the Healthcare and Education Sectors. International Journal of Cyber Criminology. 2011;5(1):794-810.

12. Raghupathi W, Raghupathi V, Saharia A. Analyzing Health Data Breaches: A Visual Analytics Approach. AppliedMath. 2023;3(1):175-99.
13. UK Information Commissioner's Office (ICO). Data security incident trends. 2023 [02/08/2023]; Available from: https://ico.org.uk/action-weve-taken/data-security-incident-trends/.
14. Australian Government. Privacy Act 1988 (Cth). 1988 [14/01/2023]; Available from: https://www.legislation.gov.au/Details/C2022C00361.
15. Office of the Australian Information Commissioner (OAIC). Notifiable data breaches publications. 2023 [14/08/2023]; Available from: https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications.
16. Hile J. Dude, where's my data?: The effectiveness of laws governing data breaches in Australia. Journal of Telecommunications and the Digital Economy. 2021;9(2):47-68.
17. Petkauskas V. Hackers were interested in Australia long before Medibank and Optus breaches. 2022; Available from: https://cybernews.com/security/hackers-australia-medibank-optus/.
18. Australian Government. Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (No. 33, 2022).
19. Australian Government. Security Legislation Amendment (Critical Infrastructure) Act 2021.
20. IT News. HealthEngine reveals data breach. 2018 [cited 2019 14/05/2019]; Available from: https://www.itnews.com.au/news/healthengine-reveals-data-breach-496175.
21. Healthcare IT News. Medical records at Victorian hospital get hacked. 2019; Available from: https://www.healthcareitnews.com/news/anz/medical-records-victorian-hospital-get-hacked.
22. The West Australian. Limited delays after Vic hospital hacks. 2019.
23. Clarke P. Significant data breach from Ambulance Tasmania. 2021; Available from: http://www.peteraclarke.com.au/2021/01/08/significant-data-breach-from-ambulance-tasmania-through-interception-of-its-paging-service-with-data-of-patients-who-contact-ambulances-published-on-line/.
24. Cunningham M. Staff unable to access patient files after Eastern Health cyber attack. The Age. 2021.
25. Kost E. What Caused the Medibank Data Breach? 2022; Available from: https://www.upguard.com/blog/what-caused-the-medibank-data-breach.
26. Powell T, Sammut-Bonnici T. Pareto analysis. 2014.
27. Karuppusami G, Gandhinathan R. Pareto analysis of critical success factors of total quality management: A literature review and analysis. The TQM magazine. 2006.
28. Paltiel M. Recent Amendments to the Australian Privacy Act. Journal of Bioethical Inquiry. 2023:1-7.
29. Attorney-General's Department (Australia). Privacy Act Review Report. 2023.