Data Breaches

COS30015 IT Security- Week 11

Troy Cao

CONTENT

01 Introduction of Data Breach

02 How Data Breach Happen?

03 Data Breach Cases

04 Medibank & Optus Data Breach Comparison

05 Urgent Need for Privacy Law Changes

SWINBURNE UNIVERSITY OF TECHNOLOGY

What is Data Breach?

- **A data breach** occurs when unauthorized parties infiltrate computer systems, networks or databases to gain access to confidential information.

- Breached data can include **personal information**, **financial records**, **intellectual property** or any other **protected information** that falls into the wrong hands. .

- Potential consequences of a data breach:
  - ❖ financial losses, reputational damage, legal implications;
  - ❖ potential harm to victims, e.g., privacy leakage.

Source: https://www.forbes.com/advisor/business/what-is-data-breach/

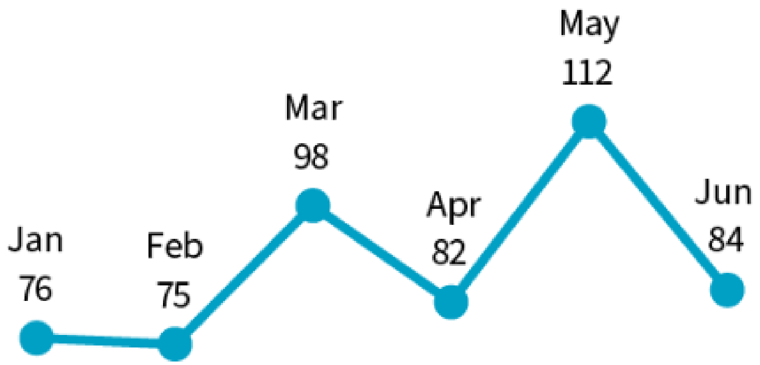
Snapshot of Data Breach in Australia

↑ 527

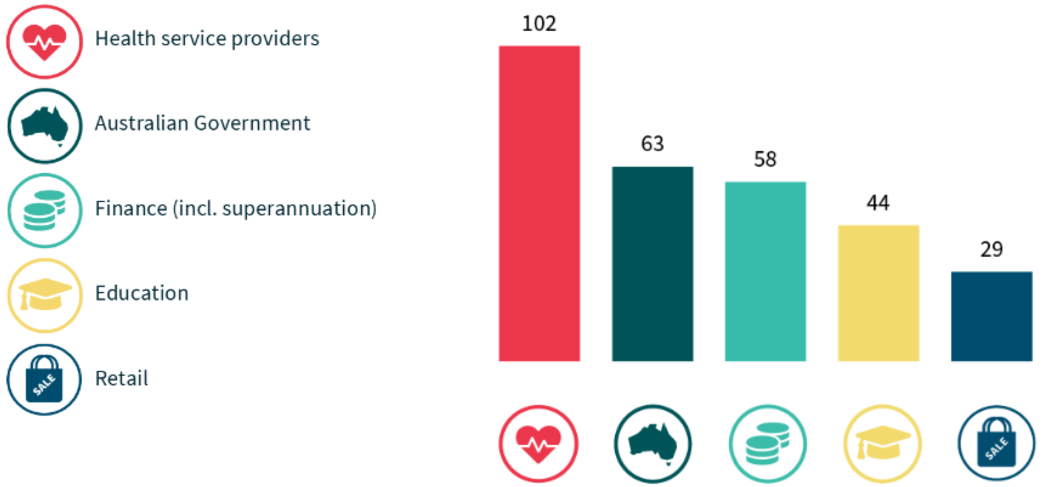
notifications

Up 9% compared to July to December 2023

Some data breaches affect more than one entity. The OAIC received an additional 17 secondary data breach notifications.



Top 5 sectors to notify data breaches



Source: https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-january-to-june-2024

CONTENT

01 Introduction of Data Breach

02 How Data Breach Happen?

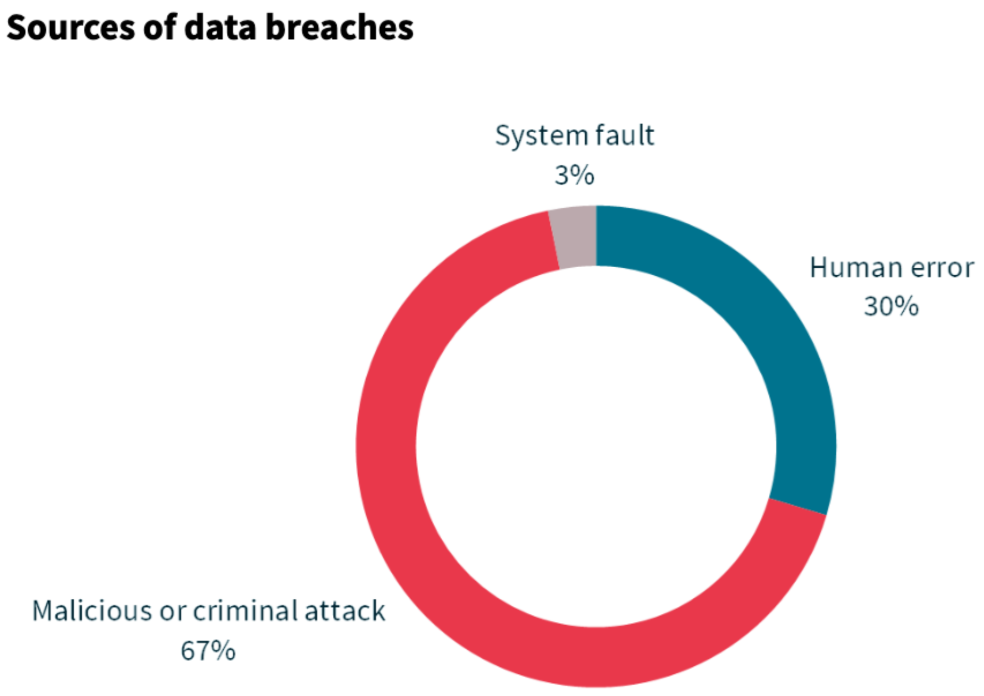
03 Data Breach Cases

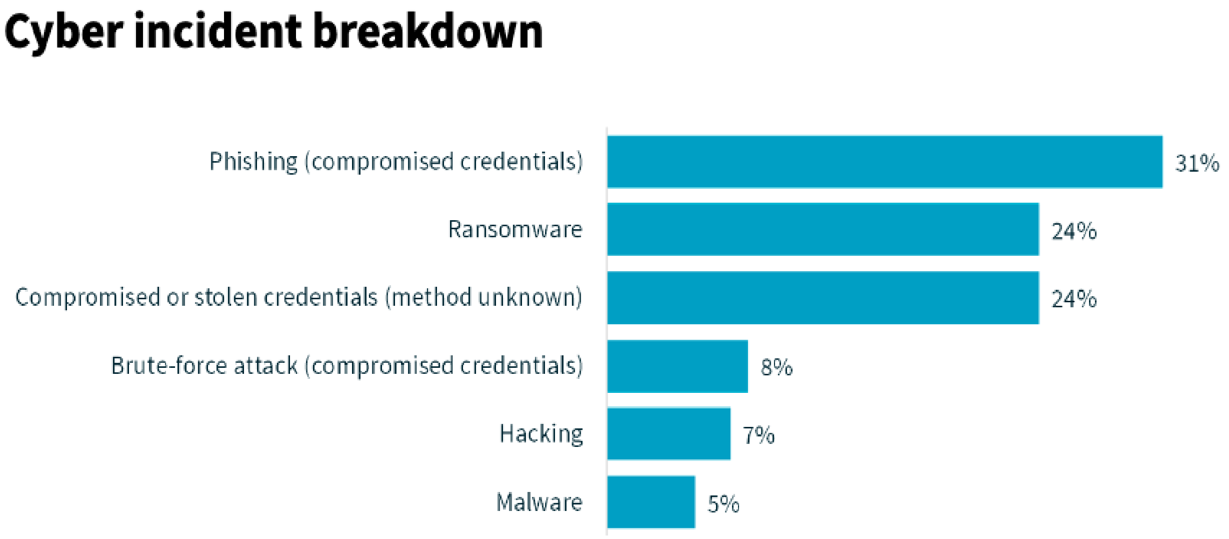
04 Medibank & Optus Data Breach Comparison

05 Urgent Need for Privacy Law Changes

SWINBURNE UNIVERSITY OF TECHNOLOGY

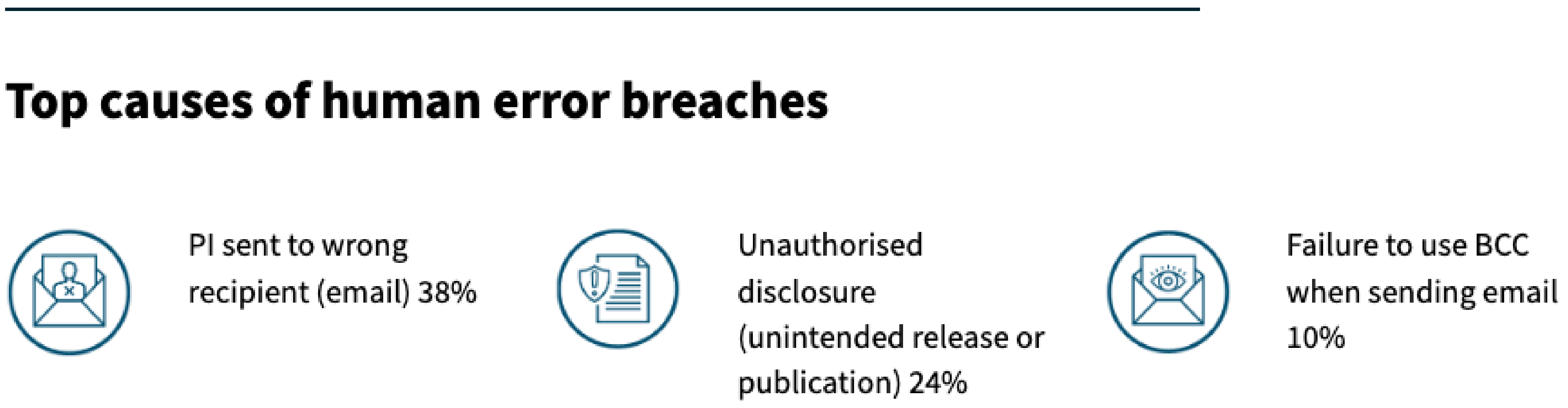
How Data Breaches Happen?





Source: https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-january-to-june-2024

How Data Breaches Happen?



Top causes of human error breaches

PI sent to wrong recipient (email) 38%

Unauthorised disclosure (unintended release or publication) 24%

Failure to use BCC when sending email 10%

Source: https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-january-to-june-2024

CONTENT

01 Introduction of Data Breach

02 How Data Breach Happen?

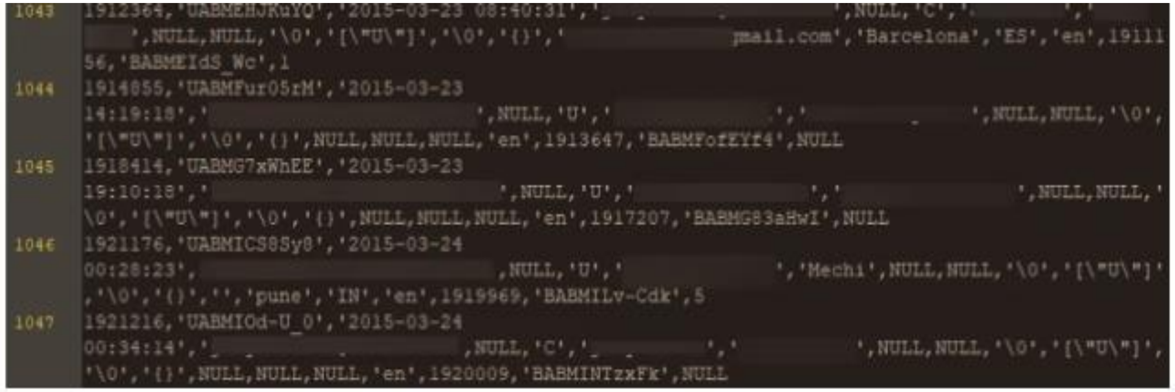
03 Data Breach Cases

04 Medibank & Optus Data Breach Comparison

05 Urgent Need for Privacy Law Changes

SWINBURNE UNIVERSITY OF TECHNOLOGY

Canva Data Breach



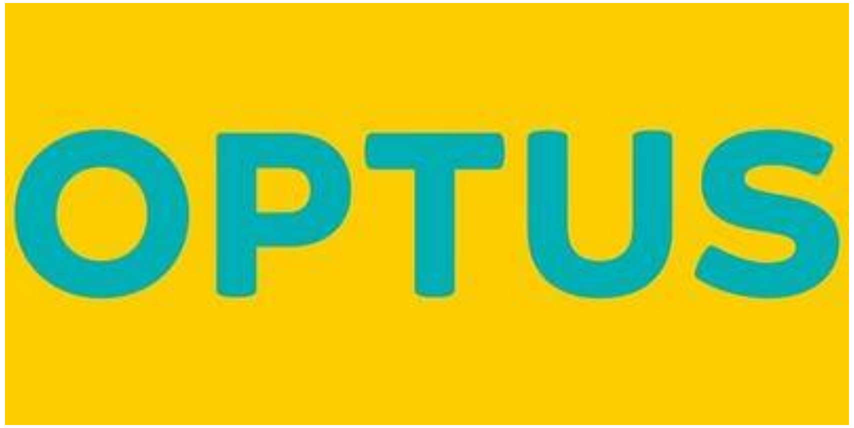
```
1912364,'UABMEHJKuYQ','2015-03-23 08:40:31','[redacted]',NULL,'C','[redacted]','
[redacted]',NULL,NULL,'\0','[\"U\"]','\0','{}','[redacted]gmail.com','Barcelona','ES','en',19111
56,'BABMEIdS_Wc',1
1914855,'UABMFur05rM','2015-03-23
14:19:18','[redacted]',NULL,'U','[redacted]','[redacted]',NULL,NULL,'\0',
'[\"U\"]','\0','{}',NULL,NULL,NULL,'en',1913647,'BABMFofEYf4',NULL
1918414,'UABMG7xWhEE','2015-03-23
19:10:18','[redacted]',NULL,'U','[redacted]','[redacted]',NULL,NULL,'
\0','[\"U\"]','\0','{}',NULL,NULL,NULL,'en',1917207,'BABMG83aHwI',NULL
1921176,'UABMICS8Sy8','2015-03-24
00:28:23',[redacted],NULL,'U','[redacted]','Mechi',NULL,NULL,'\0','[\"U\"]'
,'\0','{}','','pune','IN','en',1919969,'BABMILv-Cdk',5
1921216,'UABMIOd-U_0','2015-03-24
00:34:14','[redacted],NULL,'C','[redacted]','[redacted]',NULL,NULL,'\0','[\"U\"]',
'\0','{}',NULL,NULL,NULL,'en',1920009,'BABMINTzxFk',NULL
```

- ❖ "I download everything up to May 17," the hacker said. "They detected my breach and closed their database server." --- ZDNet

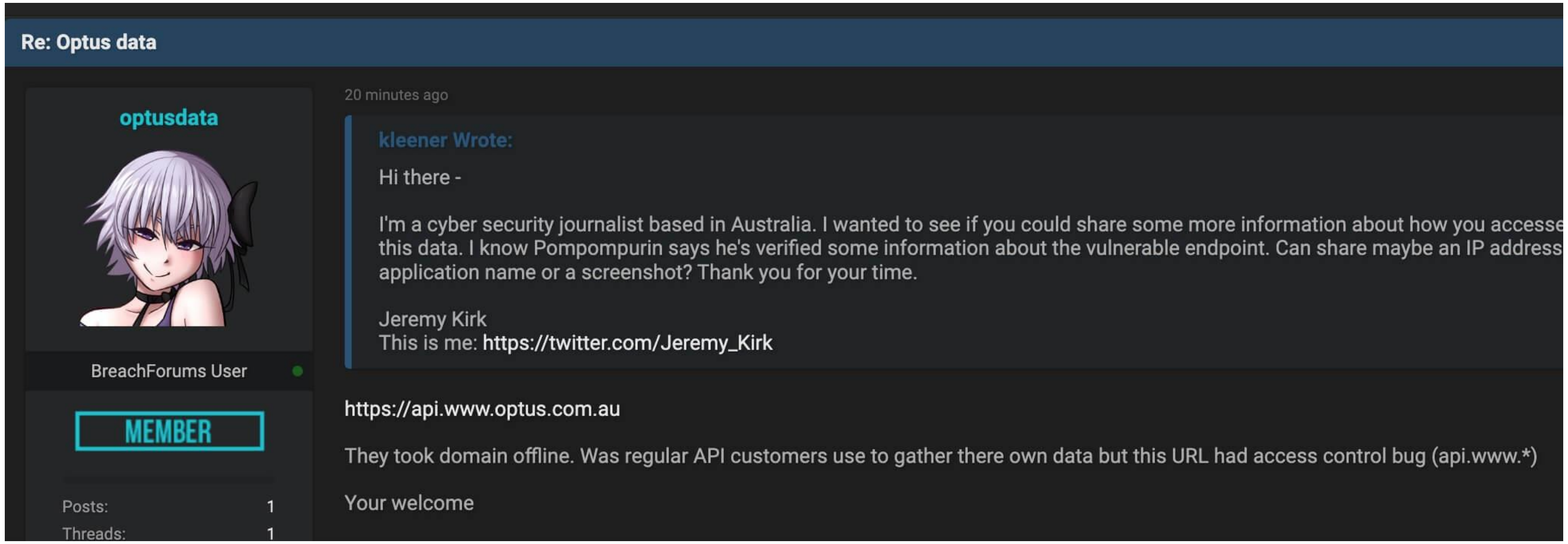
- ❖ Australian unicorn ***Canva*** suffered a monumental data breach impacting ***137 millions*** of its users.

Source: https://www.upguard.com/blog/biggest-data-breaches-australia

Optus



- The Optus data breach was one of the biggest security breaches ever in Australian history.
- Impacting up to **9.8 million** customers, almost 40% of the population



Re: Optus data

optusdata

BreachForums User

MEMBER

Posts: 1

Threads: 1

20 minutes ago

kleener Wrote:

Hi there -

I'm a cyber security journalist based in Australia. I wanted to see if you could share some more information about how you accesse this data. I know Pompompurin says he's verified some information about the vulnerable endpoint. Can share maybe an IP address application name or a screenshot? Thank you for your time.

Jeremy Kirk
This is me: https://twitter.com/Jeremy_Kirk

https://api.www.optus.com.au

They took domain offline. Was regular API customers use to gather there own data but this URL had access control bug (api.www.*)

Your welcome

The alleged details of the Optus data breach as revealed by a cybercriminal claiming responsibility - Source: Twitter - Jeremy Kirk.

Source: https://www.upguard.com/blog/biggest-data-breaches-australia

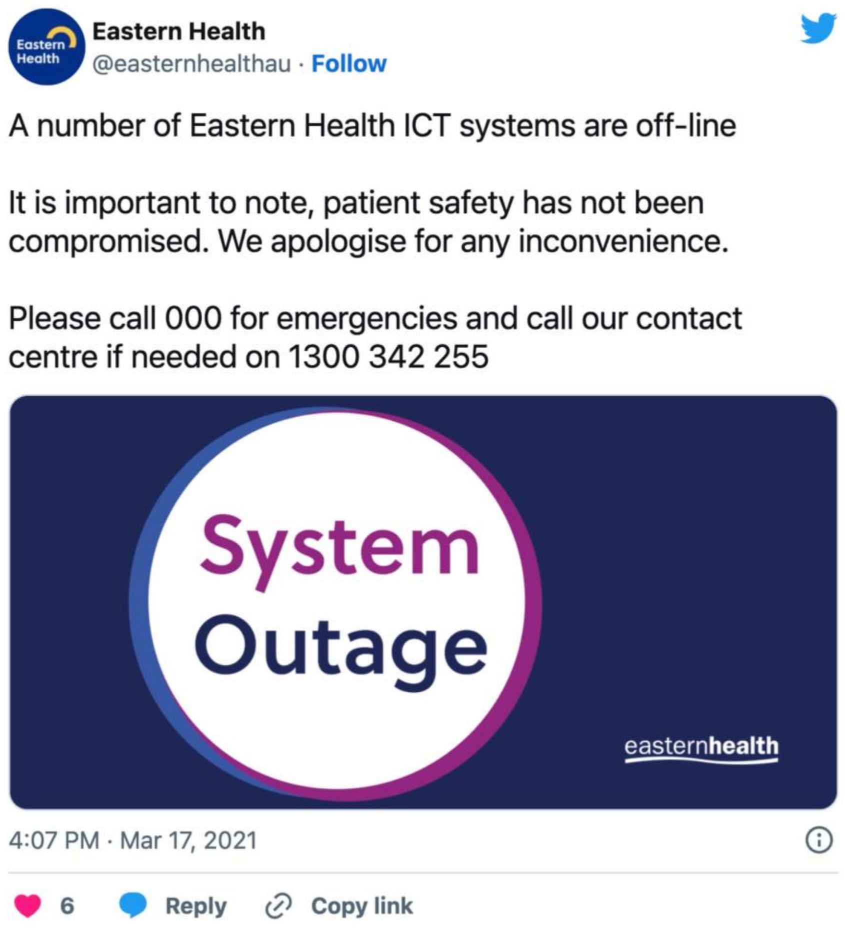
Medibank

- ❖ In December 2022, Medibank data breach incident, affected the personal details of 9.7 million customers.

- ❖ Medibank is currently under investigation by the Office of the Australian Information Commissioner (OAIC) for its information handling practices and could be subject to a $50 million fine if it is determined that it did not have sufficient security practices in place.

Source: https://www.upguard.com/blog/biggest-data-breaches-Australia; https://www.oaic.gov.au/__data/assets/pdf_file/0029/228980/Medibank-civil-penalty-action-overview-infographic.pdf; https://7news.com.au/news/melbourne

Eastern Health



Eastern Health
@easternhealthau · Follow

A number of Eastern Health ICT systems are off-line

It is important to note, patient safety has not been compromised. We apologise for any inconvenience.

Please call 000 for emergencies and call our contact centre if needed on 1300 342 255

4:07 PM · Mar 17, 2021

- "Absolutely, we've learned a lot during this process. But we've also positioned ourselves really well to strengthen and harden our network against any further attempts"

  --- *Lachland Bakewell, Eastern Health CIO*

- Ransomware attacks targeting the Australian health sector are increasing.

- Ransomware attacks see the target entirely locked out of their internal systems, which literally mean life or death for the patients relying on information found within networked systems in this case.

Source: https://www.upguard.com/blog/biggest-data-breaches-Australia; https://www.linkedin.com/pulse/four-worst-healthcare-cyber-attacks-australian-history/

Western Australian Parliament

- The attack left Parliament without the use of its email platform for 19 hours as it worked on a fix.

- WA's Executive Manager of Parliamentary Services Rob Hunter said that a forensic audit found no evidence of a data breach. But it's uncertain whether this consolation is true.

Source: https://www.upguard.com/blog/biggest-data-breaches-australia

CONTENT

01 Introduction of Data Breach

02 How Data Breach Happen?

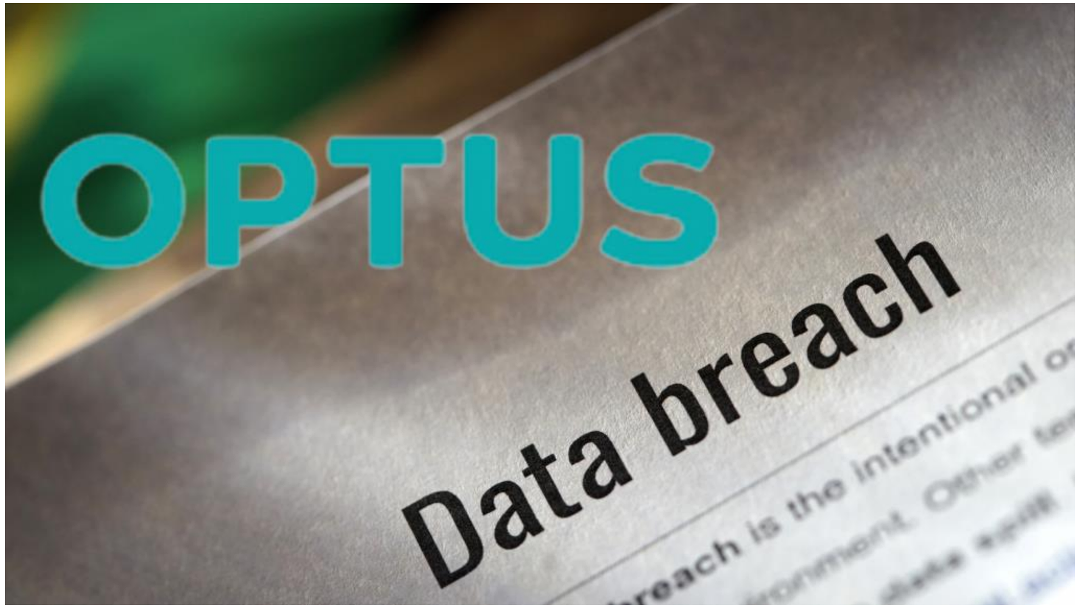
03 Data Breach Cases

04 Medibank & Optus Data Breach Comparison

05 Urgent Need for Privacy Law Changes

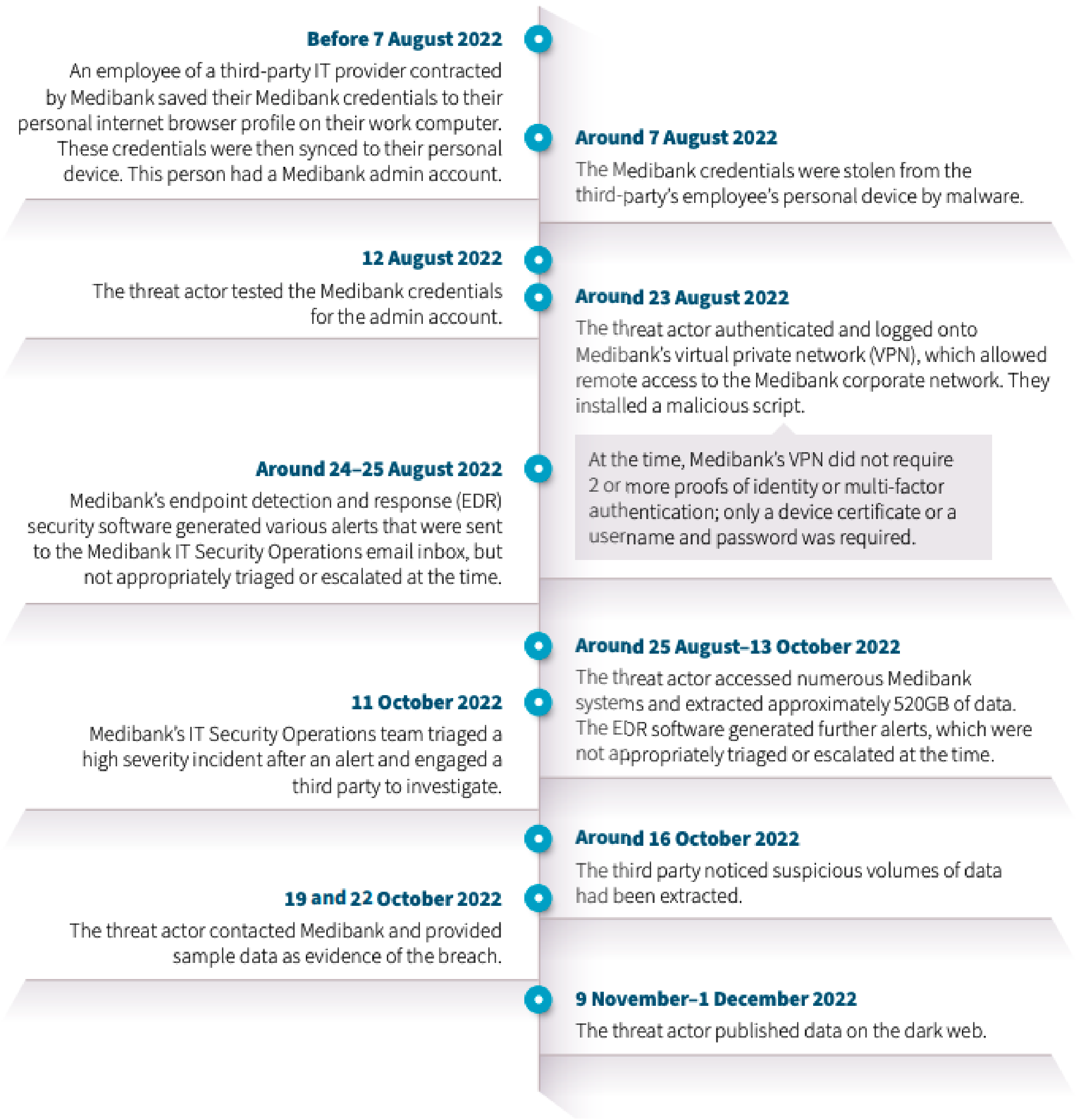
Optus Data Breach - Timeline

- **20 September 2022**: Optus's technical team detected suspicious activity on its network and began investigating.
- **21 September 2022**: Optus confirmed a data breach and notified regulators.
- **22 September 2022**: Optus publicly announced the breach and warned customers of potential fraudulent activity. The company did not specify the number of affected customers or confirm harm. The stolen data included personal information such as names, dates of birth, addresses, phone numbers, emails, and identification numbers (passport, driving license).
- **23 September 2022**: Optus denied insider claims that an API mistake exposed the data and stated that the breach was complex. The company believed the hacker had accessed and scraped a portion of its consumer database.
- **24 September 2022**: The Australian Federal Police (AFP) launched a criminal investigation. Data from the breach was reportedly being sold online. A ransom note was posted on BreachForums, demanding $1.5 million in Monero, threatening to release the data of 10,000 customers daily unless paid. After a few hours, the ransom post was deleted, and the user apologized, stating they did not intend for the data to be published and did not receive payment.



Source: https://en.wikipedia.org/wiki/2022_Optus_data_breach#Legal_action

Medibank Data Breach - Timeline



Before 7 August 2022

An employee of a third-party IT provider contracted by Medibank saved their Medibank credentials to their personal internet browser profile on their work computer. These credentials were then synced to their personal device. This person had a Medibank admin account.

Around 7 August 2022

The Medibank credentials were stolen from the third-party's employee's personal device by malware.

12 August 2022

The threat actor tested the Medibank credentials for the admin account.

Around 23 August 2022

The threat actor authenticated and logged onto Medibank's virtual private network (VPN), which allowed remote access to the Medibank corporate network. They installed a malicious script.

At the time, Medibank's VPN did not require 2 or more proofs of identity or multi-factor authentication; only a device certificate or a username and password was required.

Around 24–25 August 2022

Medibank's endpoint detection and response (EDR) security software generated various alerts that were sent to the Medibank IT Security Operations email inbox, but not appropriately triaged or escalated at the time.

Around 25 August–13 October 2022

The threat actor accessed numerous Medibank systems and extracted approximately 520GB of data. The EDR software generated further alerts, which were not appropriately triaged or escalated at the time.

11 October 2022

Medibank's IT Security Operations team triaged a high severity incident after an alert and engaged a third party to investigate.

Around 16 October 2022

The third party noticed suspicious volumes of data had been extracted.

19 and 22 October 2022

The threat actor contacted Medibank and provided sample data as evidence of the breach.

9 November–1 December 2022

The threat actor published data on the dark web.

Source: https://www.oaic.gov.au/__data/assets/pdf_file/0037/228979/Medibank-data-breach-alleged-timeline-infographic.pdf

Comparison

- The Optus data breach was caused by public-facing API, which further allows access to sensitive data.

- While the Medibank data breach happened due to theft of internal credentials of privileged system access.

Commonalities:

- The organisations failed to comply with regulations regarding data handling and cybersecurity; and

- Those failures amounted to breaches of contractual promises and privacy policies, misleading representations and/or breaches of continuous disclosure obligations.

Source: https://otx.alienvault.com/ ; https://encyclopedia.kaspersky.com/

CONTENT

01 Introduction of Data Breach

02 How Data Breach Happen?

03 Data Breach Cases

04 Medibank & Optus Data Breach Comparison

05 Urgent Need for Privacy Law Changes

SWINBURNE UNIVERSITY OF TECHNOLOGY

Ethical Implication behind Medibank Hack

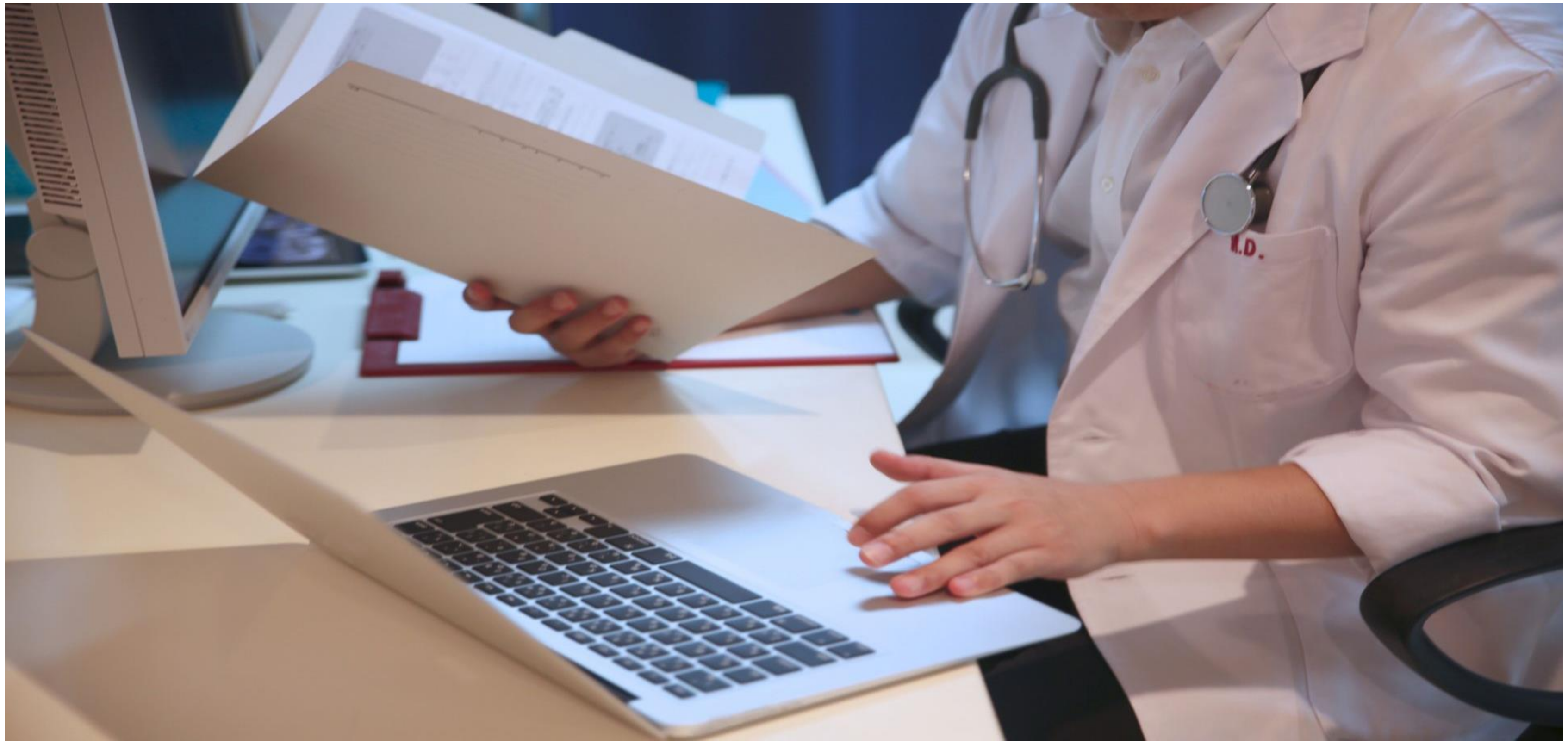
- Following ransom threats, the purported Medibank hackers published the personal medical information of 100 people – separated between “***naughty***” and “***nice***” categories.

- The overtones of moral judgement in the attackers’ actions are unmistakable – creating fear and anxiety over details in those health records.

- More importantly, this tactic highlights how it’s those in society who are already the most marginalised and vulnerable that have the most to lose when their private information is made public without their consent.

Source: https://pursuit.unimelb.edu.au/articles/medibank-s-hack-tells-us-privacy-laws-need-to-change

Ethical Implication behind Medibank Hack



- ❖ For the sake of society’s most vulnerable, we need to recognise that privacy is non-negotiable because breaches of privacy cause real harm.

- ❖ In an age in which we can expect to see more data breaches, privacy laws must keep up.

Source: https://pursuit.unimelb.edu.au/articles/medibank-s-hack-tells-us-privacy-laws-need-to-change

Thanks for Watching

Troy Cao