In October 2022, Medibank, one of Australia's largest health insurers, discovered an attempt to exploit a vulnerability in its Windows Server through unauthorised file modification. The investigation, outsourced to a cybersecurity firm, revealed that a significant amount of data had been exfiltrated from Medibank's network, including sensitive information. Shortly thereafter, cybercriminals contacted Medibank, demanding a ransom to prevent the release of the stolen data. The compromised information included personal details such as names, addresses, dates of birth, Medicare and policy numbers, phone numbers, and specific claims data, including where customers received medical services and codes related to their diagnoses and procedures. After executives of Medibank refused to pay the ransom, the stolen data was leaked on the dark web, escalating the impact of the breach. (Information Commissioner & Kangeson, 2024b)

The Medibank cyber incident had profound repercussions. 9.7 million customers had their personal and medical information exposed, raising serious privacy concerns and leaving them vulnerable to identity theft and misuse of their health data ("Medibank Taken to Court by Australia's Privacy Watchdog," n.d.).

Moreover, the breach resulted in substantial costs for Medibank, including those associated with breach response, legal actions, potential regulatory fines (Australian Information Commissioner, 2022), and compensation for affected individuals (MauriceBlackburn.com.au, n.d.). The company also had to make significant investments in strengthening its cybersecurity infrastructure.

Lastly, the breach also inflicted considerable damage to Medibank's reputation, eroding customer trust and confidence in the company's ability to safeguard sensitive information.

But, How could an organisation of Medibank's scale and financial resources fall victim to such a significant data breach? A detailed analysis of the incident reveals that several factors and deficiencies in protective mechanisms contributed to the breach. This report will examine each factor chronologically:

Human Target: Stolen Credentials from a Third-Party IT Service Provider

The threat actor gained administrative access through compromised credentials obtained from a third-party IT service provider (Tonkin, n.d.). The breach occurred due to improper handling of credentials by the provider's personnel. Specifically, the administrator credentials were saved in a personal browser profile, which was linked to the employee's personal laptop. This laptop was subsequently compromised by malware, allowing the attacker to extract the credentials ("Medibank Allegedly Missed EDR Alerts Before Data Breach," n.d.-b).

Misconfigured Firewall

Initially, the hacker attempted to access a Microsoft Exchange Server using stolen

credentials but was unsuccessful. Upon discovering that the credentials were from Medibank's network, the hacker used them to access the enterprise VPN successfully. This was possible due to the lack of additional control mechanisms, such as registered device verification or IP source checks, which would have prevented unauthorised access.

Lack of Multi-Factor Authentication (MFA) for Login Access
In addition to the missing control mechanisms, Medibank's network did not require an additional authentication step, such as multi-factor authentication (Tonkin, n.d.). This oversight allowed the hacker to easily access the system using only the stolen admin credentials.

Improper Handling of Endpoint Detection and Response (EDR) Alerts
Once inside the network, the hacker quickly escalated privileges by obtaining further usernames and passwords, gaining access to multiple Medibank systems without restrictions (Medibank, 2023). While the Endpoint Detection and Response (EDR) system issued alerts, these were ignored by Medibank's IT team ("Medibank Allegedly Missed EDR Alerts Before Data Breach," n.d.). Two months later, the hacker attempted to exploit a vulnerability in Medibank's Microsoft Exchange Server by modifying a file system. This time, Medibank's team responded to the alert and initiated a thorough investigation with assistance from a third-party cybersecurity specialist, ultimately uncovering the incident and its full extent. Notably, external auditors had previously reported weaknesses in Medibank's access control and protection mechanisms in 2020 and 2021(Taylor, 2024).

This sequence of events illustrates how a lack of robust control mechanisms, compounded by human negligence or omission, led to one of the major data breaches. However, these lessons highlight how similar incidents can be prevented in the future, including but not limited to:

1. **Adopting a Zero Trust Security Policy**
   Implementing a Zero Trust Security Policy, which operates under the principle of "never trust, always verify," can provide a comprehensive approach to securing networks, systems, personnel, and organisational assets. This framework emphasises least privilege access and strictly enforced access controls (Chapman & Garbis, 2021).
2. **Utilising advanced technology for Enhanced Security**
   Incorporating AI tools can further bolster security by classifying legitimate and illegitimate privacy policies. Advanced machine learning models can analyse large volumes of privacy policies, identifying discrepancies and potential red flags that indicate unauthorised or unethical data practices (Kayes et al., 2024).
3. **Enforcing Security Standards for Third-Party Contractors**
   Organisations must ensure that third-party contractors adhere to the same or higher security standards as the primary organisation, minimising

vulnerabilities introduced by external partners (“Cyber Resilience Good Practices,” n.d.)

4. **Fostering a Security Culture**
   Since human factors often represent the weakest link in security, cultivating an information security culture is crucial. This involves promoting good security practices through shared knowledge, values, and beliefs, making security an integral part of employees’ daily routines. A strong security culture ensures that employees understand and internalise security measures, reducing the likelihood of incidents due to inadequate separation of personal and professional profiles (AlHogail, 2015).

Consequences of the Incident

As previously discussed, this incident led to several significant consequences. The most severe impact stemmed from the exposure of personal and sensitive health information of millions of Medibank customers, resulting in increased risks of impersonation, identity theft, extortion, discrimination, and stigmatisation due to the disclosure of medical records (Kayes et al., 2024). This breach caused considerable distress among affected customers, with psychological effects such as anxiety, fear, and a loss of trust. In response, Medibank took measures to mitigate the impact, providing customer support, mental health professionals, and guidance on steps to take through multiple communication platforms (Ritchie, 2022).

Medibank suffered significant reputational damage, as customers lost confidence in the company's ability to protect their data. The financial repercussions included costs associated with response and remediation efforts, legal fees, and fines totaling $2,220,000 for each contravention within the relevant period (Information Commissioner & Kangeson, 2024), along with potential compensation claims from civil actions initiated by affected customers. In response, Medibank implemented enhanced security measures, including improved firewall configuration, strengthened authentication protocols, expanded monitoring and detection capabilities, and Operation Safeguard policy (Medibank, 2023b).

Furthermore. The Medibank breach served as a wake-up call for the healthcare sector and broader industry, highlighting the urgent need to reassess and bolster cybersecurity defences. It underscored the critical importance of robust data protection measures and comprehensive incident response plans to safeguard sensitive information against increasingly sophisticated cyber threats.

Finally, in a significant regulatory development, Australia imposed its first cyber sanction under the Autonomous Sanctions Act 2011 on Russian national Aleksandr Ermakov for his involvement in the data breach. This action followed extensive efforts by the Australian Signals Directorate, the Australian Federal Police under Operation Aquila, Commonwealth agencies, and international partners(Cyber Sanction Imposed on Russian Cybercriminal for 2022 Medibank Private Compromise

| Cyber.gov.au, 2022). This sanction not only addresses the individual's actions but also serves as a broader deterrent against future cyber threats.

Insights and Key Takeaways

Based on the analysis of this incident and its widespread impact on the industry, society, and government, it is clear that the current framework serves as both a precedent and a wake-up call. Information-related threats are unlikely to diminish; in fact, they are expected to grow as they have become increasingly lucrative and organised in recent years. With the advent of new technologies such as AI, IoT, and greater interconnectivity of devices, the co-dependency between technology and data will continue to expand. Therefore, it is imperative that "good actors" strive to stay one step ahead of these threats by investing more resources into research and the application of emerging technologies to mitigate or prevent such risks. Moreover, it is essential that these initiatives are driven by a collaborative effort that goes beyond industry and technical experts alone. Strategies should be developed by a multidisciplinary group comprising industry leaders, government, civil society, technical experts, sociologists, and policymakers, ensuring a comprehensive approach to addressing the importance of information security from all perspectives.

REFERENCES

MauriceBlackburn.com.au. (n.d.). Medibank Data Breach 2022 investigation. Retrieved from https://www.mauriceblackburn.com.au/class-actions/join-a-class-action/medibank-data-breach/

Medibank. (2023). *2023 half year results*. Retrieved from https://www.medibank.com.au/content/dam/retail/about-assets/pdfs/investor-centre/results/HY23_Results_Media_Release.pdf

Medibank allegedly missed EDR alerts before data breach. (n.d.). Retrieved from https://www.itnews.com.au/news/medibank-allegedly-missed-edr-alerts-before-data-breach-608922

Cyber sanction imposed on Russian cybercriminal for 2022 Medibank Private compromise | Cyber.gov.au. (2022). Cyber.gov.au. https://www.cyber.gov.au/about-us/view-all-content/news-and-media/cyber-sanction-imposed-russian-cybercriminal-2022-medibank-private-compromise

Information Commissioner, A., & Kangeson, G. (2024). Concise statement. (Medibank Private Limited ACN 080 890 259 & DLA Piper Australia), Federal Court of Australia. Retrieved from

https://www.oaic.gov.au/__data/assets/pdf_file/0025/221974/Australian-Information-Commissioner-v-Medibank-Private-Limited-concise-statement.pdf

Kayes, A. S. M., Rahayu, W., Dillon, T., S., A. S., & Alavizadeh, H. (2024). Safeguarding Individuals and Organisations from Privacy Breaches: A Comprehensive Review of Problem Domains, Solution Strategies, and Prospective Research Directions. TechRxiv. https://doi.org/10.36227/techrxiv.171328715.51528864/v1

Ritchie, E. (2022, October 20). Medibank cyber incident response. Medibank Newsroom. https://www.medibank.com.au/livebetter/newsroom/post/medibank-cyber-incident-response

Cyber resilience good practices. (n.d.). Retrieved from https://asic.gov.au/regulatory-resources/corporate-governance/cyber-resilience/cyber-resilience-good-practices/

Cybercrime update – Deloitte incident review. (n.d.). Retrieved from https://www.medibank.com.au/livebetter/newsroom/post/cybercrime-update-deloitte-incident-review

Medibank taken to court by Australia's privacy watchdog. (n.d.). Retrieved from https://www.itnews.com.au/news/medibank-taken-to-court-by-australias-privacy-watchdog-608559

Australian Information Commissioner. (2022). Medibank civil penalty action. Retrieved from https://www.oaic.gov.au/__data/assets/pdf_file/0029/228980/Medibank-civil-penalty-action-overview-infographic.pdf

Tonkin, C. (n.d.). Medibank finally reveals 'rookie mistake' in breach. Retrieved from https://ia.acs.org.au/article/2023/medibank-finally-reveals--rookie-mistake--in-breach.html

Taylor, J. (2024, June 17). Medibank's lack of multi-factor authentication allowed hackers to infiltrate systems, regulator alleges. The Guardian. Retrieved from https://www.theguardian.com