Article

May 2024

Preventing the Next Big Breach: Key Takeaways from MediSecure's Cyber Attack

It seems that hardly a day goes by here in Australia that we don't hear of another massive breach. The unfortunate truth is this is going to get worse before it starts getting better. The MediSecure breach serves as a stark reminder of the importance of robust cybersecurity measures, doubly so in the healthcare industry.

It seems that hardly a day goes by here in Australia that we don't hear of another massive breach. The unfortunate truth is this is going to get worse before it starts getting better. The MediSecure breach serves as a stark reminder of the importance of robust cybersecurity measures, doubly so in the healthcare industry.

Details of the breach, which was announced on Thursday, appear to be a little thin at this stage but has prompted a whole-of-government response, with the Australian Signals Directorate's Australian Cyber Security Centre and the Australian Federal Police investigating the incident. If this attack sticks to the current trends MediSecure will be facing what is known as a double extortion attack, where the attacker not only encrypts the victims data but also threatens to leak confidential information exfiltrated during the attack. This, as the name suggests doubles the pressure on victims to pay the ransom but doesn't guarantee the data will not be leaked anyway.

What we do know for certain is what I believe Medisecure have done well so far:

1. Rapid Response: MediSecure acted swiftly to contain the breach and minimize the potential damage.
2. Transparency: The company was open and honest about the incident, providing timely updates to the public.
3. Regulatory Compliance: MediSecure followed all necessary legal and regulatory requirements in reporting the breach, resisting the temptation to just pay the ransom and sweep it under the rug.

The exact details of how MediSecure was compromised have yet to be released but they have hinted that the breach likely originated from a third-party vendor. This being the case what could MediSecure done to avoid this situation:

1. Before onboarding a third-party vendor, conduct a thorough background check and risk assessment. This includes reviewing their security practices, compliance with relevant regulations, and their track record with other clients. A comprehensive vendor risk management program can help identify potential risks and mitigate them early on.
2. Once a vendor is onboarded, maintain a regular monitoring process to ensure they continue to meet your security standards. This includes keeping an eye on their financial health, security posture, and any changes in their operations that could introduce new risks.
3. Have a clear plan in place for how to respond to a security incident involving a third-party vendor. This includes communication protocols, roles and responsibilities, and steps to mitigate the impact. Regularly test and update this plan to ensure it remains effective.

On this third point it seems that it is exactly what MediSecure had in place. Though this is only speculation from the outside looking in. Whatever the case may be, sensitive data is now in the hands of cyber criminals and third-party vendor or not, that data was entrusted to Medisecure. It's a wake-up call to companies that handle sensitive data to step up their game and ensure that their security measures are up to par. After all, the last thing anyone wants is their personal and health information being used for nefarious purposes.

There are no silver bullets but companies can avoid being the next headline by:

1. Prioritising the implementation of robust security measures, including encryption, firewalls, intrusion detection systems, and regular security audits.
2. Regular training and awareness programs can help employees recognize and respond to potential threats, reducing the risk of human error leading to a breach.
3. Carefully vet third-party vendors and ensure they adhere to strict security protocols. Regular audits and monitoring of third-party systems can help prevent breaches originating from external sources.
4. Collect and store only the data necessary for providing services. This reduces the potential impact of a breach and simplifies data management.
5. Develop and maintain a comprehensive incident response plan to ensure a rapid and effective response in the event of a breach. This should include clear communication protocols and predefined roles and responsibilities for all team members.

The MediSecure breach serves as a valuable lesson for companies in the healthcare industry and beyond. By learning from MediSecure's experience, companies can better prepare themselves to face the ever-evolving landscape of cybersecurity threats. Prioritising advanced security measures, employee training, third-party risk management, data minimization, and having a robust incident response plan in place can significantly reduce the risk of a data breach and its potential impact.

This article and other fantastic insights are shared in our monthly cyber threat report. You can join the mailing list to receive it here.

Waterstons has 25+ years' experience across the UK and Australia preparing and protection organisations from cyber threats. We are committed to assisting all organisations to stay agile and prepared in today's cyber conscious economy.

Empower your organisation today, get in touch with one of our team members.

info@waterstons.com.au | 02 9160 8430