BROOKY
CYBERSECURITY

HEALTHCARE IN THE CROSSHAIRS

- HOW RANSOMWARE IS TARGETING THE INDUSTRY

A Case Study On The Genea Cyberattack

OVERVIEW OF THE ATTACK

In early 2025, the Australian fertility clinic Genea fell victim to a devastating cyberattack orchestrated by the Termite ransomware group. Over a two-week period, cybercriminals infiltrated Genea's systems, stealing an estimated 700GB–940.7GB of sensitive medical and personal data. The breach exposed patient contact details, Medicare card numbers, medical histories, test results, and medication records.

Shortly after the attack, the stolen data was published on the dark web, putting thousands of patients at risk.

TIMELINE OF EVENTS

January 31, 2025 – February 14, 2025

Attackers gained unauthorized access and remained undetected in Genea's systems.

February 14, 2025

Genea discovered the breach and initiated an investigation.

Following the Discovery

Hackers published the stolen data on the dark web, prompting a rapid response from the clinic.

RESPONSE AND MITIGATION EFFORTS

Investigation

Genea launched an internal and external forensic investigation to determine the extent of the breach.

Patient & Staff Notifications

Affected individuals were notified, with Genea offering support services such as counseling through IDCARE.

Legal Action

A court-ordered injunction was obtained to prevent further dissemination of stolen data.

Government Collaboration

Genea worked closely with the Australian Federal Police, the Office of the Australian Information Commissioner, and other authorities to address the incident.

The repercussions of this breach were significant, affecting both patients and the wider healthcare industry:

Emotional Distress

Patients expressed concerns about how the breach could impact their treatments and privacy.

Financial & Reputational Damage

While no financial data was reported stolen, the goodwill and trust built by Genea over the years suffered a severe blow.

Exploitation Risks

Cybercriminals highly value medical records as they contain comprehensive personal and medical information, making them prime targets for identity theft, scams, and extortion.

IMPACT OF THE ATTACK

THE GROWING THREAT: RANSOMWARE-AS-A-SERVICE (RAAS)

One of the most alarming aspects of modern cybercrime is the accessibility of ransomware.

Ransomware-as-a-Service (RaaS) allows even those with little technical expertise to purchase or rent ransomware on the dark web, effectively outsourcing cybercrime. This means that any disgruntled individual or competitor with malicious intent can easily hire attackers to target a business, putting the healthcare industry at constant risk.

Despite increasing cyber threats, Australian data protection laws remain inadequate in addressing the severity of ransomware attacks. Unlike regions such as the EU with GDPR, Australian businesses often escape with minimal financial penalties following breaches.

THE WEAKNESS OF AUSTRALIAN DATA PROTECTION LAWS LEAVES ROOM TO BE HACKED

However, the real cost is not in fines, it's in lost trust, damaged reputations, and the significant operational disruption that follows a cyberattack.

The regulatory framework fails to serve as a strong enough deterrent against lax security measures, leaving businesses and patients exposed.

How much would it cost you per hour to shut down your medical practice?

ARE YOU AS PROTECTED AS YOU THINK?

Cyber threats are changing every day, and healthcare providers are prime targets due to the sensitive nature of their data. Don't wait until it's too late to assess your cybersecurity resilience.

Click the link below to book a free 15-minute chat with one of our experts today to quickly assess whether your business is as protected as you think.

https://brookycyber.com.au/chat-to-an-expert