# WHY IS HEALTH CARE A LUCRATIVE TARGET FOR ONLINE CRIMINALS?

CYBERCRIME INDUSTRY SNAPSHOT

## Health care

CYBER READY

mailguard

# The health sector is the most vulnerable to cyberattacks

The adoption of online patient medical records, booking and billing systems in the health care sector is rapidly increasing, making the industry a prime target for cybercrime and malware attacks. Standard business operations come to a crippling halt when access to online health care systems are compromised and highly sensitive data is leaked.

**Patient data, including Medicare and social security details, is highly valued by cyber-criminals as the data remains marketable over time**. The rate of sophisticated data encryption within hospitals is quite low due to highly complex IT systems and a tendency to maintain current and outdated legacy systems. On top of this, only one third of hospitals use extensive data encryption according to a 2016 encryption survey report.

**Health service providers are the top sector for reporting data breaches to the Office of the Australian Information Commissioner (OAIC)**, according to the OAIC's first quarterly report on data breach notifications received under the Notifiable Data Breaches (NDB) scheme. The NDBs officially came into force on 22 February 2018.

**In 2016, the Red Cross Blood Service fell prey to Australia's largest ever data breach**. 1.28 million donor records were published to a public-facing website and discovered by an anonymous source. The database contained personal details (name, gender, physical and email address, phone number, date of birth, blood type and country of birth) and other highly-sensitive health information.

# At a glance—impacts on the health sector


**is the estimated cost per patient record**

including lost business due to reputational damage. Cost to prevent a breach: $8 per patient record


**of ransomware attacks target hospitals**

according to a report that healthcare is hit harder by ransomware than any other industry


**health care record breaches**

were recorded in 2015, and ⅓ of health care customers are susceptible to having their data compromised


**more valuable than other forms of data**

as healthcare data on the black market is in great demand than other illegally-obtained records

# Some high profile incidents

In one of the largest cyber incidents of 2017, the **WannaCry ransomware attack debilitated Britain's National Health Service**—affecting computers across one-third of the country's health trusts and around 600 GP surgeries. 19,500 medical appointments were lost in the attack.

**1.5 million patients of health clinics in Singapore** had their personal details illegally accessed and copied— including Singapore's Prime Minister Lee Hsien Loong. The targeted cyberattack in 2018 affected the database of the country's biggest public healthcare group.

In January 2015, US health insurance company **Anthem Blue Cross was the victim of an email phishing attack** which resulted in the loss of personally identifiable information (PII) of 78.8 million customers.


**is the cost of cyberattacks**

against U.S. hospitals, clinics and doctors in the US alone


**of cyber breach victims in the US**

were from the health care sector over the past five years

The cyber-attackers gained access to Anthem's core network via compromising the network credentials of employees with high-level IT access. Post-mortem investigations insinuate this was a nation state attack.

In January 2016, **Australia's Melbourne Health was hit by a new variant of the Qbot malware which infected Windows XP computers** at Royal Melbourne Hospital's pathology department. Later that year, the Red Cross revealed that due to 'human error' the personal details of 550,000 blood donors had been leaked.

**A ransomware attack forced a Californian medical centre to depend on fax machines and paper records for a week.** Rather than lose all its patient medical records, the hospital decided to bite the bullet and paid the ransomware crooks 40 bitcoins, or about $17,000, to restore the hijacked files.

Thousands of operations were cancelled after a **cyberattack forced NHS management to shut down computer systems at three UK hospitals** in late 2016.

# MailGuard reporting on recent phishing scams

Cybercriminals impersonate brands that are household names and have large customer bases. The brand recognition, coupled with curiosity or fear, impel unwary recipients to click through to phishing sites, or inadvertently download executable malware. MailGuard has reported email scams purporting to be from government agencies (ATO, the High Court), popular online subscription or free services (Apple, Netflix, Dropbox, Office 365), delivery services (Australia Post, UPS, DHL) and telco / utilities (Telstra, Origin Energy).

Scams bank on human psychology to respond (e.g. tax evasion, traffic infringements, court order, unauthorised account login attempts, overdue bill), reinforced by sophisticated, well-crafted emails and phishing sites (often indiscernible from the mimicked sites). Unfortunately, these campaigns are effective, with 7.3% of targeted recipients successfully phished. The market value of PII on the dark web ranges from USD2,000 for a passport to USD1,065 for a medical record and up to USD400 for a diploma, so a successful phishing campaign can be a boon for cybercriminals.

## Health care testimonal

WPH Western Private Hospital

"We started using MailGuard in 2012 and it immediately solved our problems with spam and malicious email. In the health care industry, we can't afford any IT-related incidents or downtime, so MailGuard gives us peace of mind. The service is reliable and the Australia-based tech support is fantastic.

There's nothing like being able to pick up the phone, talk to a local, and resolve any queries in a single phone call."

— IT Infrastructure Manager, Western Private Hospital

**GET CYBERREADY WITH MAILGUARD**

We identify and stop fast-breaking attacks in real-time, 2-48 hours ahead of the market

Contact your IT service provider now for an obligation-free, 14-day trial

PHONE 1300 30 44 30
EMAIL expert@mailguard.com.au
WEB mailguard.com.au

CYBER READY

mailguard