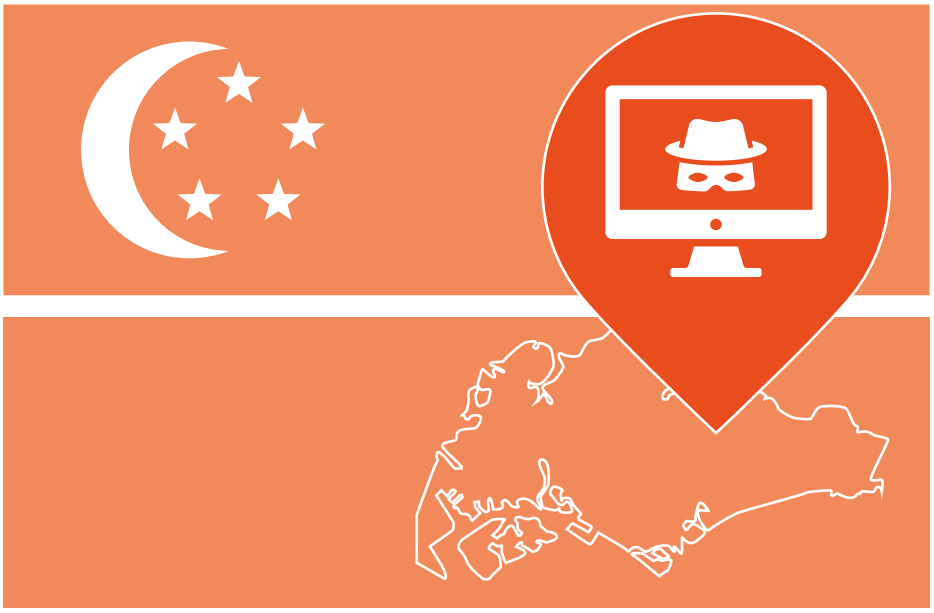
SINGAPORE HEALTH SERVICE CYBER ATTACK

LESSONS LEARNED

Crawford®

STOP ASKING "ARE WE SAFE?" AND START ASKING "WHAT RISKS ARE WE EXPOSED TO BASED ON OUR CURRENT SECURITY PROGRAM?"



1.5 million patients hacked

In the most recent cyber wake up call, the personal data of 1.5 million patients in Singapore has been hacked in the country's largest cyber attack, the Singaporean government announced recently. 160,000 of these patients, including Prime Minister Lee Hsien Loong, had their outpatient prescription medicine data stolen as well.

According to investigations, the data was stolen between 27 June and 4 July 2018.

The timing of the Singapore Health Cyber Service cyber attack is perhaps, inadvertently unfortunate for the Australian Government, in light of the "Opt-Out" program currently underway for the Australian "My Health Record" system.

About 20,000 people opted out on the first day of the Opt-Out period, fearing the risk of privacy breaches - perhaps, as it seems, with good cause.

Healthcare systems, such as Singapore's "SingHealth" and Australia's "My Health Record", are increasingly becoming targets of cyber-criminals because of the information those systems contain, which ranges from Social Security numbers to health insurance identification numbers.

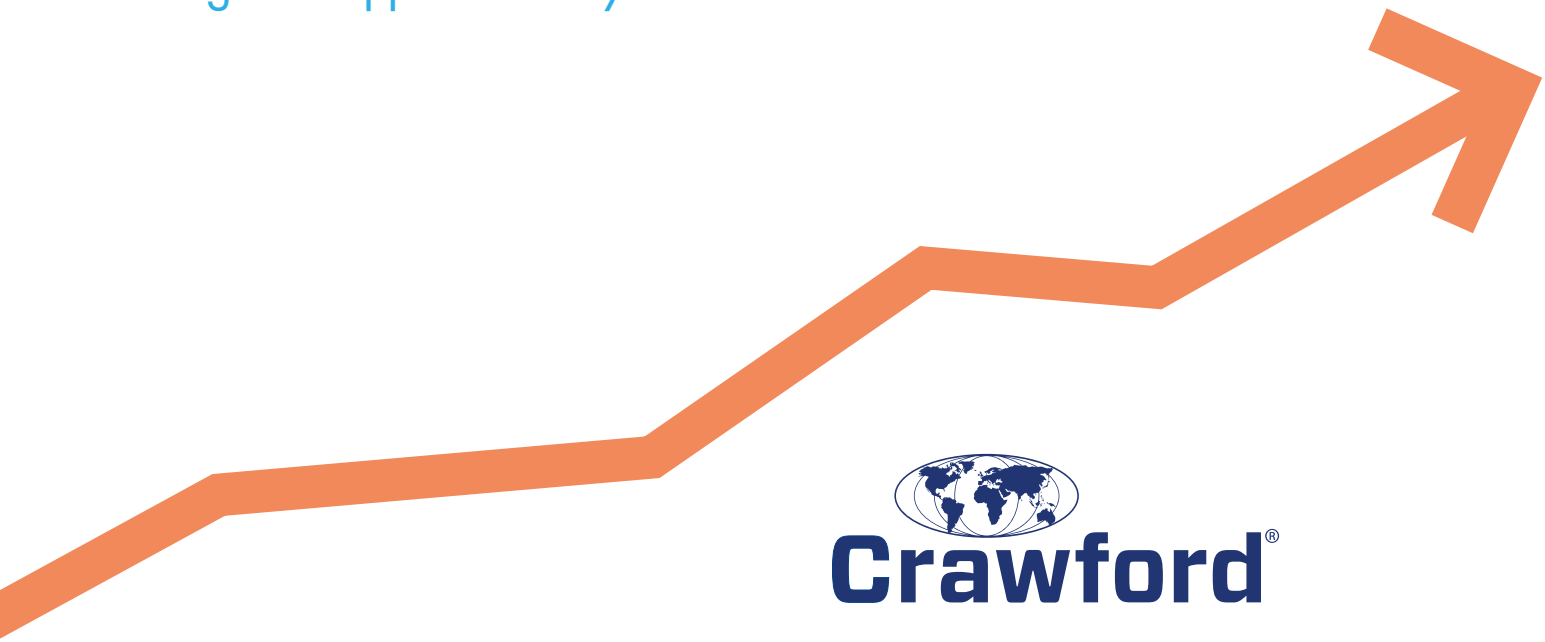
While a Social Security number might sell for less than a dollar in the underground market and a credit card number may fetch a dollar or more, a comprehensive medical record is an order of magnitude above that, sometimes fetching in excess of $1,000.

So, what is it that makes Protected Health Information (PHI – a subset of Personally Identifiable Information), so valuable?

PHI contains more personal data points and cannot just be reissued in the event of a problem. Bank account details, credit card number and passwords can be changed after a breach; but information about allergies, disabilities, mental health or hereditary conditions, cannot.

Access to PHI data can allow cyber criminals to create fraudulent identities allowing them to obtain health services, purchase medical equipment and supplies, drugs or even file fictional claims with insurers. Or alternatively, data can be deleted or modified or updated unbeknownst to the organisation.

What is clear is that incidents like the SingHealth cyber attack are looking to become more common and even unrelated industries may find themselves in the sights of opportunistic cyber-criminals.



Having cyber risk management in place should be of critical importance to every company.

Crawford®

Crawford & Company®, in association with our specialist panel vendors, is able to assist clients prepare for a cyber attack before it occurs. Without data collection, an organisation cannot successfully detect or react to anything. Alarms, audit and investigation all require underlying information to detect bad actors and determine the effectiveness of controls thereby facilitating the preparation of a multilayered approach to defence.

Of course, as with other risks that present-day enterprises face, cyber risk can also be managed and mitigated through adequate cyber insurance and should be considered a key aspect of any company strategy.

According to the Ponemon Institute's 2017 Cost of Data Breach Study, sponsored by IBM, the number one way to reduce the cost of a data breach is with an incident response (IR) team. The phrase 'time is money' is never more applicable when a breach occurs and not having an effective Cyber Security Incident Response Plan (CSIRP) in place could result in a lot of wasted time and money.

Crawford's loss adjuster led cyber solution is at the forefront of the current cyber ecosystem, providing a complete end to end crisis management and claims solution. While prevention is preferable to detection and reaction, in these rapidly changing times, this is a challenging proposition.

Upon detection of a cyber attack, the first 48 hours are pivotal in taking steps towards containment, investigation, mitigation and remediation.

STEP ONE

NOTIFICATION OF THE INCIDENT TO THE CRAWFORD INCIDENT RESPONSE MANAGER (IRM)

A rapid response ensures the situation is assessed and brought under control as soon as possible after discovery of a cyber attack which is often an emotionally charged time. In the first few hours after notification, the IRM assembles the IR team, with appropriate specialists appointed depending on the extent, severity and risk of what has been impacted. It is important to note that not all cyber attacks result in breaches, and at the early stages of an investigation, when a company is still trying to establish what has happened, legal privilege is unlikely to apply.[1]

---

https://www.ashurst.com/en/news-and-insights/legal-updates/privilege-quickguide/
General understanding: Privilege only attaches if
1) Litigation is in the reasonable contemplation of the parties (i.e. Likely to occur, not merely a prospect), AND;
2) The main purpose of the communication (report, etc.) is for use in litigation / arbitration.

STEP TWO

CONTAINMENT, INVESTIGATION AND MITIGATION

Crawford Incident Response Managers, through countless experiences in handling major or complex loss, are key to ensuring the best possible outcomes are achieved. Significant complexities can be involved with even relatively minor cyber attacks. IRMs are crucial in monitoring costs, maintaining awareness of cover as well as limitations of Policies (if any) and act to keep stakeholders updated throughout.

There is often a trade-off between damage assessment (i.e. investigation) and loss mitigation. Both activities are often time sensitive, and the extent of the damage may be increasing without loss mitigation being undertaken. However loss mitigation may interfere with incident investigation activities.

The various priorities will often overlap, with the IRM managing all aspects of the claim.

If the cyber incident is still ongoing, containment is the first priority. This may only be further discovered as investigations unfold. It is also important to establish, what, if any, data may have been exfiltrated. While many cyber attacks, such as the SingHealth attack, aim to access or acquire data, comprising a data breach, other means of attack have the goal of directly extorting funds from a company, such as ransomware encrypting files and demanding payment in order for the decryption key to be provided.

With containment established and investigations underway, mitigation measures will be enacted to minimise the impact to the organisation as much as possible. Early engagement of Crawford Forensic Accounting Services and appointed specialist experts working together provides the specific skillset and expertise to capture forensic evidence to efficiently and effectively manage, often simultaneously, the containment, investigation and mitigation of the incident.

STEP THREE
REMEDIATION

The ultimate aim of the process is to put the organisation back into the position they would have been in, but for the incident. The Crawford IRM skillset and experience, derived from their core focus of loss adjusting, provides the capabilities of crisis management as well as dealing with the operational needs of the affected organisation in order to achieve this goal.

If a data breach has occurred, significant work can be involved in identifying the jurisdictions and breach notification requirements of those jurisdictions as soon as possible. The long term implications of a breach may also require credit and identity monitoring to be established, as well public relations firms to be engaged to protect the brand and reputation of the affected organisation.

The costs of these long tail monitoring arrangements and other costs can run on for a significant duration and adds further argument for the need for comprehensive cyber Insurance cover. Such comprehensive cyber policies typically include incident response cover, which unlike most other policies, can afford the protection of the rapid response, particularly the first 48 hours, from the moment a potential cyber attack has been identified, before an actual cyber claim has been validated.

A data breach could bring your entire business to a standstill, and a ransomware threat could lock down your data, making daily operations impossible.

Get ahead of the threat!

"The worst thing a company can do when it has been attacked is to try and think on their feet!"

– Crawford Cyber Solution by Crawford Global Technical Services®

Restoring and enhancing lives, businesses and communities

https://crawfordgts.com/services/cyber-risk

For further information on Crawford's cyber risk solution, please contact:

Gareth Cottam
MBA CA ACLA ANZIIF (Snr Assoc) CIP
Senior Forensic Accountant

T: +65 6632 8694
M: +65 9727 6017
E: gareth.cottam@crawford.asia

Paul Handy
BSc (Hons) MBA ACII FCILA FUEDI-ELAE FIFAA ACMI
Head of Cyber & Technology Risks

T: +44 207 265 4320
M: +44 7827 879 187
E: paul.handy@crawco.co.uk

Ian McDonald
ANZIIF (Snr Assoc)
Regional Cyber Lead Asia

T: +852 2101 0915
M: +852 9211 1762
E: ian.mcdonald@crawford.asia

Crawford®

www.crawco.com