It is no secret that Cybercrime is rife, and big enterprise is not the target. There has been no reduction in the number of attacks in recent years and attackers are now concentrating on Small and Medium Enterprises, particularly in the Health sector.

According to the Australian Small Business and Family Enterprise Ombudsman (ASBFEO), small businesses account for 35% of Australia’s gross domestic profit and employ 44% of Australia’s workforce. Of the 877,744 total employing businesses, 823,551 are small businesses (93.8%) and of those, 627,932 employ only 1 – 4 people, known as micro businesses (76.2%).

When putting the above into context and reviewing SME’s by turnover, the ASBFEO provide the following data:

<table>
<thead>
<tr>
<th>Turnover Range</th>
<th>No of Businesses</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>$0 to less than $50k</td>
<td>572,826</td>
<td>24.76</td>
</tr>
<tr>
<td>$50k to less than $200k</td>
<td>792,373</td>
<td>34.25</td>
</tr>
<tr>
<td>$200k to less than $2 mil</td>
<td>787,685</td>
<td>34.05</td>
</tr>
<tr>
<td>$2 mil to less than $5 mil</td>
<td>92,126</td>
<td>3.98</td>
</tr>
<tr>
<td>$5 mil to less than $10 mi</td>
<td>32,483</td>
<td>1.40</td>
</tr>
<tr>
<td>$10 mil or more</td>
<td>35,798</td>
<td>1.56</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>2,313,291</strong></td>
<td><strong>100.00</strong></td>
</tr>
</tbody>
</table>

Table 1: SME sorted by Turnover - ASBFEO
Industry figures provided by the Australian Bureau of Statistics (ABS Catalogue No. 8155.0 Australian Industry Table 5 2017-18, May 2019 and ASBFEO calculations) revealed that the Healthcare and Social Assistance Sector (private), contributes $89.5 billion, 55.8% of which is contributed by small and medium businesses. Therefore, it is no surprise that Healthcare providers, arguably holding some of the most sensitive of personal client information, can fall foul to cyber-attack.

In this article, Chris Zietsman, Senior Cyber Adjuster, CTA Brisbane, outlines his experience with cybercrime within the Health sector, including trends, ramifications and responses within the Insurance industry.

Data Breach

The Notifiable Data Breach (NDB) scheme outlined in the Commonwealth Privacy Act of 1988 specifies requirements applicable to organisations with a turnover greater than AUD 3,000,000 per annum and for those organisations which do not meet the turnover but which includes organisations that provide health services or hold health information. Although the NDB scheme has been effective for only 2 years, the data published reveals an average of 242 eligible data breaches being referred to the Office of the Australia Information Commissioner (OAIC) per quarter. This means just under a thousand cases are referred annually to the OAIC. Of this, Health Services providers were the top reporting sector to the OAIC having notified 253 eligible breaches during the period of February 2018 to June 2019, accounting for nearly 20% of all eligible breaches in Australia. In second place was finance with 14% and in third, legal, accounting and management services with 9.7%.

In terms of what triggered such notifications, we note that the Health Services sector had 138 cases where the breach was related to Human Error, and 112 cases relating to Malicious or Criminal Attack. In our experience, human error would typically be the inadvertent release or loss of medical data, such as sending information by email to non-authorised recipients.

What is a Cyber Risk?

- Financial Loss
- Data Breach
- Client Disruption
- Business Interruption
- 3rd Party Liability
- Physical Damage
- Reputation Damage
- Regulatory Violations
- Regulatory Fines
Technology Lag

Technological development is critical in any sector and healthcare is no exception. Technology is relied upon to improve the quality of healthcare delivery, increasing patient safety, reducing medical errors, and promoting interaction between patients and healthcare providers, as well as in the supply chain of medical organisations.

The Internet of Medical Things (IoMT) has also seen rapid developments across the healthcare industry with connected medical devices, giving providers the ability to improve patient care, provide better clinical data, increase efficiency and reduce healthcare costs. However, not all connected devices are secure.

A report compiled by Forescout revealed that more than 70% of medical devices in their study still run on Windows 7, Windows 2008 and Windows Mobile.

It would therefore appear that hospitals and healthcare organisations are not ready to say goodbye to Windows 7, although Windows 7 Microsoft support end date was January 14, 2020. Since January 2020, there has therefore been no technical assistance and software updates from Windows Update that help protect the devices and monitoring systems. This will leave the devices and monitoring systems exposed to potential threats as we have seen in 2017’s Wannacry outbreak, which had devastating effects globally across all sectors.

An interesting observation, however, is that the Wannacry outbreak spared computers operating on Windows 10 but in order to assist with customers still on older systems, Microsoft provided patches for Windows XP, for which support had ended in 2014. Microsoft similarly issued patches for out of support Operating Systems when the Bluekeep vulnerability was identified in 2019.

The Wannacry attack exploited a vulnerability designed to work against un-patched Windows 7 and Windows 2008 systems. Of the 400,000 devices worldwide infected by Wannacry, 98% were running some version of Windows 7.

The UK’s National Healthcare Service (NHS) became the case study for Windows upgrades following the Wannacry outbreak that devastated a large portion of the organisation’s IT systems. They reportedly spent tens of millions in securing their systems against the next Wannacry.
Software Upgrades

A report by Duo revealed that Healthcare is the most Windows-dominated industry, with nearly half a million endpoints (or 52% of Windows endpoints) still running the outdated operating system.

The situation does not seem to have improved, and whilst it may be easy to criticise organisations for failing to migrate when Microsoft cut off dates are announced, some industries would still be unable to meet the pace required to upgrade, leaving the end-user in a predicament. Others still rely on obsolete systems or proprietary systems for which a replacement or integration of new systems is not always possible.

Nearly 3 years after the Wannacry event, it is reported that the NHS still has over 1 million computers running Windows 7, which reflects over 75% of the total NHS IT estate.

At the time of ending support for Windows 7 on 14 January 2020, figures suggested that approximately 440,000,000 computers worldwide were still running the specific operating system, with some transition being evident to Windows 10.

Utilising an Operating System which is no longer supported makes it more vulnerable. We would anticipate this to be the theme in cases being investigated over the next few years.

To understand why unsupported software poses such a risk, a basic understanding of the Operating System security needs to be provided. In essence, Operating System security is a game of “whack-a-mole”. There are thousands of undiscovered vulnerabilities in any large piece of software which are discovered over time. A good software company will deliver software with fewer unknown vulnerabilities, and a bad one will deliver with more, but they all have vulnerabilities. Each vulnerability follows a very similar lifecycle:

1. The vulnerability is discovered;
2. The vulnerability gets published (often at https://cve.mitre.org/);
3. The software company researches and publishes a fix; and
4. Each customer implements the fix according to their own timescale. Testing will be required before this can be implemented, and the company will have to consider false positives and a staggered implementation so as not to impact its Operating Systems.

Some software customers will fix that one vulnerability quickly, some will fix it slowly; but if you look at the entire population of customers, there will always be some customers that haven’t yet fixed it.

Putting the above together, you have a game of “whack-a-mole”, with new vulnerabilities constantly popping up and being resolved. The faster the vulnerabilities pop up, the more vulnerable that entity; the faster they resolve them, the less vulnerable they are.

---

The Windows 7 Predicament

For those still using Windows 7 after 14 January 2020, these “moles” which pop up will not be “whacked” so easily. Over time, they will become increasingly vulnerable, and the solutions are difficult, expensive, unreliable, and generally more complex than simply moving to Windows 10.

Hackers do not target all old systems, as there are legacy systems from 20 years ago that are still in use with unfixed vulnerabilities, but so few people use them that it is not worth attackers undertaking a mass market attack. They will try to find the path of least resistance and exploiting a vulnerability on Windows 7 may still give them access to valuable data, so we anticipate seeing some new claims relating to these vulnerabilities for some time.

Attackers seek financial gain. Typically, if a system is breached, personal data may be stolen to be used straight away or as a leverage to pay a ransom or threaten to delete/corrupt the data. In most recent claims, we have seen a direct link between ransomware and data breach. This type of attack is often passed towards the cyber Insurers which have provided a policy of cover to their Insured.

Ransomware Trends

Q4 of 2019 saw a rise in RYUK and Sodinokibi ransomware attacks, which are virulent strains of malware, causing a great deal of damage. But these attacks have recently been evolving.

Firstly, the ransom demands are increasing, and attackers are being much more assertive about the amounts they are demanding. The days of ransomware demands of a few thousand dollars have passed; these were designed to be cheaper to pay than to do anything else - with Sodinokibi, we are seeing ransom demands in the millions of dollars.

Secondly, the attackers have spent time to improve the “user experience” and a new type of criminal activity has emerged in the form of “ransomware as a service”. Attackers have identified that, like any legitimate software company, the better they explain the process and the more support they give their “customer” (victim), the fewer “sales” (payments for the decryption key) they will lose. Payment processes have therefore been simplified and appear to be professionally designed. Attackers refer to guarantees about the quality of their product, offer chat support, and give the impression of a technology company trying to manage many customers. The consequences of this are frightening, especially as the individual ransom demands start hitting the millions.

Finally, we have seen the emergence of data breach as leverage to incite customers to pay the ransom in the recent MAZE attacks. These attacks were targeting the health market right before Covid-19 and whilst the criminals responsible for the Maze ransomware attacks indicated that they would not target health services during this time, it did not stop them from striking the UK’s Hammersmith Medicine Centre on 23 March 2020, stealing data and then threatening to publish it online unless the centre paid ransom.

Therefore, outdated software, posing as a mass market vulnerability position with more virulent ransomware, creates a potential economic disaster in waiting.
In December 2019, the New South Wales Supreme Court accepted the settlement of a pioneering class action in Australia against the New South Wales Ambulance Service, following a data breach. The breach occurred when a NSW Ambulance contractor sold the worker’s compensation files of 130 former and current employees to personal injury lawyers in 2016, which included personal and medical information.

The settlement sets a precedent for future cases, specifically focussing on the accountability of companies following a data breach. The consensus in the legal fraternity is that this settlement is likely to trigger a more aggressive pursuit by Plaintiff firms to pursue claims through the courts following data breaches, posing an additional risk and exposure to companies.

The Australian Government also tightened the noose by announcing a privacy reform agenda in March 2019, which included the following:

1. **Additional Funding to the OAIC;**
   An additional AUD 8 million per year for the next three years has been indicated to strengthen its enforcement powers.

2. **Additional powers for the regulator;**
   The OAIC will have the ability to issue infringement notices under several laws including the Spam Act and ASIC Act.

3. **Increased Penalties;**
   The current maximum penalty of AUD 2.1 million (for a corporation) is one of the highest under any Asia Pacific data protection law, however the proposed changes would increase that maximum penalty to the greater of:
   - AUD 10 million
   - Three times the value of the benefit obtained from the breach; or
   - 10% of the corporation’s annual domestic turnover from the last 12 months.

While there is no confirmation whether the reform will be passed, it does provide some insight into the direction of the Australian Government.

At this time, we are not aware of any penalties having been issued in Australia. We have noted the OAIC is more active on breaches notified and have progressively increased the depth of their enquiries into the actions taken during a data breach.

The message from the Australian Government, however, is clear: companies have been placed on notice and the Government will not hesitate to act.
Conclusion

The Healthcare Sector contributes a great deal to the Australian economy and remains extremely vulnerable, as is evident from the breach data released by the OAIC and from our involvement as Cyber Incident Managers and Adjusters.

Vulnerabilities appear to be rife, with unsupported Operating Systems being only one of them, which is likely to be around for several years. The question remains to what extent the Healthcare sector will be required to take steps to avoid liability to data subjects for failure to secure networks and vulnerabilities, when dealing with sensitive patient and other data which may result in harm.

The Healthcare sector globally appears to rely on taking out insurance instead of investing in the upgrades. Insurance does not provide betterment and unfortunately, in some cases, migration to the Cloud or setup of new systems is necessary.

The recent COVID-19 pandemic has resulted in the advancement of technology, and pioneering innovations to allow workaround solutions to challenges posed by the pandemic. The confinement imposed in Australia required companies to move swiftly to a new way of operating. Online consultations or renewal of prescriptions and working from home have been implemented, but we are already seeing issues with security in place to enable these functions including the vulnerabilities associated with Zoom meeting software and RDP network vulnerabilities, which have been exploited. It is anticipated that claims relating to these issues may rise significantly in the coming months.

As technology advances, attackers are also continually refining their attacks, which appear to be more sophisticated and difficult to avoid or remediate. More than ever, it is more a question of when than if a company will be under threat. Work to remediate these sophisticated attacks is also more time and cost intensive. These demands normally exceed the limits on Cyber Policies held by SME’s, leaving them even more vulnerable. It is also evident that attackers can adapt their attacks at frightening speeds and may strike more than once.

From a regulatory point of view, the Government have made their intentions clear with proposed increases in penalties, additional funding to the OAIC for enforcement and the progressively more intense review of breach notifications. The situation appears to be primed for the OAIC to send a message to SME’s who fail to comply with their Privacy obligations in the NDB scheme. It is likely that such a message would have to be relatable to other SME’s in order to resonate and create the necessary shock to drive them to comply with Privacy obligations. Policy limits in respect of Regulatory Fines cover may also have to adapt.

With the recent class action settlement in New South Wales, the focus is on the accountability of corporations in the event of a data breach. It would be interesting to monitor the weaknesses Plaintiff firms look at to expose organisations in future cases involving data breaches, and how the courts receive them. It is therefore more likely that companies will seek advice and financial support when confronted with third party claims from insurers, under the Privacy Liability cover for notification and defence costs.

It will therefore be interesting to see whether Insurers provide additional products to the market or move towards increasing coverage for the increased potential penalties. The market is still soft and declarations or pro-forma questionnaires are still short but we are likely to see a move on the market in years to come to enable either pre-loss screening or longer declarations which may result in healthcare companies having to invest more in their security and systems.

Increasing policy limits to cover ransoms claimed through Sodinokibi might place the costs of these policies out of reach of SME’s, so the attacks ultimately result in the business going under.

The Healthcare sector, and SME’s in general, are likely to feel the pressure from all sides requiring even greater resilience to weather the challenges ahead.
Our Expertise:

It is clear cybercrime is here to stay and constantly changing, and Charles Taylor Adjusting is ready to respond on behalf of its clients to deal with the subsequent insurance claims that will inevitably flow. If you want to hear more about CTA’s specialist team of cyber adjusters and particularly about our 24/7 global incident response and co-ordination of experts (IT consultants, lawyers, forensic accountants, etc), please reach out. We operate in Australia through our offices in Brisbane, whilst our experts are based all over the country.

About Charles Taylor Adjusting

CTA is one of the leading loss adjusting businesses in the market. We provide loss adjusting services across energy, marine, aviation, property, casualty and special risks along with average adjusting services for ship owners. The business primarily focuses on larger and more complex commercial losses arising from major insured incidents and claims. CTA is a business of Charles Taylor.

Charles Taylor is a global provider of professional services and technology solutions dedicated to enabling the global insurance market to do its business fundamentally better. Dating back to 1884, Charles Taylor now employs approximately 3,100 staff in more than 120 locations spread across 30 countries in Europe, the Americas, Asia Pacific, the Middle East and Africa.