the private practice

REPORT

There is no silver bullet for cybersecurity

Protecting sensitive health information, patient privacy and your business reputation.

20 November 2017

Jason Borody discusses how medical practices can minimise their risk of cyber-attacks.

Good patient care begins from the moment you capture a patient's details – this includes secure online privacy and record-keeping practices.

In March 2016, Google reported that over 50 million website users were greeted with divergent forms of warning that websites were either trying to steal information or install malicious software. Only a year earlier the reported number was 17 million.

THE THREAT OF CYBER ATTACKS

Most people have seen the various news reports of cyber-attacks on healthcare organisations. For example, earlier this year there was a nationwide breach of personal Medicare details being sold on the dark web.

Healthcare providers may believe that if they are small and low profile, they will escape the attention of the 'invaders' who are running these attacks. In fact, according to the Website Security Statistics Report 2015, over 50% of healthcare/social assistance websites were rated as "always vulnerable". This includes healthcare organisations such as medical practices, pharmacies and hospitals.

Jason Borody is the Director of Vividus Medical Marketing.

Criminals have been highly successful at penetrating smaller organisations, carrying out their activities while their unfortunate victims are unaware until it is too late. Even if you feel your practice is too small to be targeted, or that you have no valuable information online, you are still at risk, as hackers use automated tools to indiscriminately find and attack vulnerable sites.

It is vital that providers take greater responsibility to protect sensitive health information such as Electronic Health Records (EHR), online payment details, online contact forms, account details and web portal information. The consequences of a successful cyber-attack could be very serious, with legal, financial and reputational risks. Depending on the size of the business and nature of the breach, there may be fines, penalties, or risks to licence or registration conditions. The downtime to repair and secure systems can cause a significant interruption to your business, and then there is the reputational damage and loss of patient trust. Mandatory notification, media attention, removal from blacklists and browser warnings when people visit your site can take a lot of effort and can be costly to recover from.

Examples large and small abound. Barely a month goes by that the press does not have reports of the latest cyber-attacks. Last month Victoria's Minister for Health, Jill Hennessy, announced a new cyber security pilot for hospitals. The ABC reported on the growing problem of healthcare cyber-attacks similar to recent USA hospital ransomware attacks and a Gold Coast practice that was required to pay thousands of dollars to hackers after electronic files were compromised.

With increasing adoption of EHRs and web-based portals, payments and communications, many more practices will soon have cloud systems in place which could increase the risk of cyber-attacks. Even though cyber-attacks from hackers and other criminals often make news headlines, research indicates that most times, well-meaning computer users can be their own worst enemies. This is because businesses fail to implement and train employees in basic, security policies.

The implementations recommended in this Special Report are ways to overcome the 'human blind spot' with respect to protecting EHRs and other private information. By following a set of prescribed practices and actively applying them, at least some of the risks can be avoided.

SSL CERTIFICATES

This October , Google updated their Chrome browser to display a "NOT SECURE" warning when users submit data to an unsecured (HTTP) website.

Google is urging businesses to update their websites to use HTTPS, which requires the purchase and installation of an SSL Certificate. When users browse a website that doesn't have an SSL certificate, the browser displays a message warning the viewers against the unsafe or unverified identity of the web server. When patients, colleagues or industry bodies view this type of warning on a healthcare website, it raises serious questions and perceptions which can harm a practice and damage reputation.

An SSL Certificate enables messages between a sender and a receiver to be encrypted, to avoid "third-party snooping". As a website security layer, an SSL certificate makes the encrypted message useless to hackers even if they can intercept a data stream.

While there are different types of SSL certificates, most medical practices need only a basic product. Installing a certificate is not always straight forward, especially for larger sites that use third party resources, or integrate with other services. Your site may still be vulnerable if it is not properly configured. Consideration should be given to other services such as mail and AdWords campaigns that may need to be adjusted or reconfigured to avoid downtime. Your SSL certificate will involve initial setup fees as well as ongoing costs to ensure proper domain verifications, site resource management, and proper integration with your website and online services.

SSL is just one of the many security measures you can choose when it comes to protecting your practice's website.

UPDATES & BACKUPS

Our experience is that most medical practices do not update their website software, update security patches as they become available, or perform regular website backups. At Vividus we recommend several steps as a minimum for our clients including; CMS anti-intrusion measures, monthly backups, CMS and plugin updates monthly or as required, ongoing site speed and uptime reporting, and regular site security scans.

CHANGE PASSWORDS REGULARLY

A medical practitioner is familiar with the importance of regular healthy habits to maintain good health and reduce the risk of infection and disease. The same applies to updating security passwords regularly in order to lessen the chances of private information being accessed.

Creating complex passwords is the first line of defence in preventing unauthorised access to any computer or website. Regardless of the type of operating system, a password should be required to log in and do any work.

Strong passwords are ones that are not easily guessed. Since hackers may use automated methods to attempt guessing a password, it is important to choose a password that does not have characteristics that could make it vulnerable. Strong passwords should not include:

- Words found in the dictionary, even if they are slightly altered, for example replacing a letter with a number
- Personal information such as birth date, names of self, or family

Instead, strong passwords should include:

- At least 8 characters in length
- Include a combination of upper case and lower case letters, at least one number and at least one special character (such as a punctuation mark).

Pass phrases are a good way to make strong passwords. Passwords like "DoRabbitsLike5RedCarrots?" incorporates all of the rules for strong paswords yet is easy to remember.

Finally, your practice should implement regular password changes. While this may be inconvenient for employees; it reduces the risks of a system being easily broken into with a stolen password.

It was found that over 21% of businesses do not evaluate their cyber security policies, even after a breach in their systems.

ESTABLISH A SECURITY CULTURE

Within this report, it has been clearly demonstrated how compulsory it is for any healthcare practice to support proper information protection, through establishing a culture of security. Every person in the organisation must contribute to a shared vision of information protection so that habits and practices are automatic. Security practices must be built in, not bolted on.

A practice may be able to implement these steps in order to help decrease the likelihood of patients' personal health information being exposed to an unauthorised view.

However, none of these measures can be effective unless a healthcare practice is willing and able to implement them. It was found that over 21% of businesses do not evaluate their cyber security policies, even after a breach in their systems.

It can be very difficult to raise peoples' awareness about cyber threats and website vulnerabilities, especially when it isn't taken seriously. Therefore, being able to enforce security policies requires effective and proactive actions in training all users so that they are sensitised to the importance of data security.

Each medical practice must support a security-minded organisational culture. Accountability and taking responsibility for information safety must be amongst an organisation's core values. Protecting patients through good data protection policies should be as second nature to a healthcare practice as disinfection.

WHAT YOU NEED TO CONSIDER

With the ever-increasing adoption of web-based systems in healthcare, it is vital that providers take greater responsibility to protect sensitive health information, patient privacy, and their own business reputation. ⓟ

Vividus specialises in business development and marketing solutions for medical practices and the healthcare sector. If you would like to decrease your risk of a cyber-attack, give us a call on 1300 84 84 38 to see how Vividus can work with your team to strengthen your online security. Further details about Vividus and the services we offer are also available at **vividus.com.au**