Internet Security
Protecting Your Business

Hayden Johnston & Rik Perry
WYSCOM

WYSCOM
wise in communications

Internet Security – Protecting Your Business
Introduction

* Protecting Your Network
* Securing Your Information
* Standards & Best Practices
* Tools & Options
* Into The Future
* Creating A Security Culture

WYSCOM
wise in communications

Internet Security – Protecting Your Business Standards & Best Practice

* Backups
  * Must be reliable – check your back ups
  * Set them up correctly – are you backing up what you need to
  * Store them off site – your back up won't help if it is damaged in the same flood that damages your practice

WYSCOM
wise in communications

Internet Security – Protecting Your Business Standards & Best Practice

* Patching
  * Ensure your software and operating systems (eg., Windows) are updated regularly
  * ‘Patches’ are released to upgrade software with various features – most importantly, new security features
  * An unpatched system means you risk a higher chance of being compromised by system failures or hackers

WYSCOM
wise in communications

Internet Security – Protecting Your Business Standards & Best Practice

* Privileges
  * User accounts with administrative (or ‘admin’) privileges allow that user to make changes over the network and on the server and download/install software, among other things
  * Users should be set up to access only what they need to for their role. This will limit any potential security breaches.

WYSCOM
wise in communications

Internet Security – Protecting Your Business Standards & Best Practice

* Passwords
  * A complex password can mean the difference between an attacker gaining access to your network and keeping your data secure.
  * Enforcing complex passwords from your staff will protect your staff, your business and your clients.
  * Complex passwords should contain a variety of letters and numbers as well as a symbol. Long “phrase” passwords can also work very well.

WYSCOM
wise in communications

Internet Security – Protecting Your Business Standards & Best Practice

* Firewalls and Remote Access Methods
  * Firewalls let you restrict inbound and outbound access to and from your network
  * Remote access methods can be a major security risk
  * Only provide remote access to people/organisations who have a genuine need for it
  * Ensure that your remote access methods a reviewed regularly to block any potential gaps

WYSCOM
wise in communications

Internet Security – Protecting Your Business Standards & Best Practice

* Virus Protection
  * If the previous standards are followed then the risk of virus infection is greatly reduced, however there is still a need for anti-virus software

WYSCOM
wise in communications

Internet Security – Protecting Your Business
Tools & Options

* Anti-Virus
  * Anti-Virus software should update automatically to ensure it is set up to detect the latest viruses and threats
  * Standalone/Free software can be cost effective, however they can be unreliable in staying up to date with definitions

WYSCOM
wise in communications

Internet Security – Protecting Your Business
Tools & Options

* Firewall
  * It is imperative that you limit the connection ports to and from your network
  * A Firewall will allow traffic flow to and from your network to be logged, with the ability to produce reports
  * The information contained in these reports can prove fruitful in preventing attacks and compromise

WYSCOM
wise in communications

Internet Security – Protecting Your Business
Tools & Options

* Remote Monitoring and Management (RMM)
  * It is critical that you work closely with your IT Service Provider to ensure you have adequate remote monitoring in place.
  * An RMM application that sits on all servers and workstations collecting statistics, logs, and errors, and providing alerts back to your IT Service Provider on what it finds.

WYSCOM
wise in communications

Internet Security – Protecting Your Business Tools & Options

* Web Filtering
  * Blocking websites containing malware, spyware, or certain types of products is a must for preventing accidental attacks and providing access into your network.
  * An essential feature is an integration with Google's blacklists and the ability to scan websites for embedded viruses, Trojans or malware and subsequently block them.

WYSCOM
wise in communications

Internet Security – Protecting Your Business Tools & Options

* SPAM & Email Filtering
  * SPAM continues to be received because there are people who click on the links within the emails, or follow the instructions, thus meaning that the SPAM is effective
  * It is important to educate your staff NOT to click on links or open attachments in SPAM emails.
  * Effective SPAM and email filtering should eliminate all types of phishing, spam and general messages that contain virus or tracking attachments

WYSCOM
wise in communications

Internet Security – Protecting Your Business Tools & Options

* Remote Access Methods
  * A recent example of remote access gone wrong occurred in a medical practice in QLD. Russian hackers were able to gain access through ports left open for RDP purposes. What followed was a business that was held to ransom when their database was encrypted and money demanded.
  * If simple IP Blocking or closure on RDP had been in place, along with a complex password and lockout policy in place, this type of attack could have been prevented.
  * Speak to your IT Provider about the best way to secure your Remote Access Methods

WYSCOM
wise in communications

Internet Security – Protecting Your Business Tools & Options

* Backups
  * There are various options available for backup, as a minimum you should have, daily full server image backups.
  * In addition to your image backups you should also ensure you separately backup your business applications eg such as Best practice, Zedmed, Medical Director.
  * All these backups should be taken offsite daily, and as Rik has mentioned, it is important these backups are tested periodically to ensure they are restorable.

WYSCOM
wise in communications

Internet Security – Protecting Your Business
Tools & Options

* Network Security Auditing & Scanning
  * Scanning the network, both internal and external, with an auditing tool is an annual process where a tool is used to check potential problems and vulnerabilities
  * Discuss this with your IT Provider to ensure that your system is as safe and secure as possible

WYSCOM
wise in communications

Internet Security – Protecting Your Business Into The Future

* Passwords
  * Protect Yourself, Your Business, Your Patients
  * Implement a complex password regime
* Backups
  * Insure your information
  * Implement a system that works
  * Implement it….Monitor it….Take it off site.
  * You never know when you'll need it

WYSCOM
wise in communications

Internet Security – Protecting Your Business Into The Future

* The Cloud
  * Make it work for you
  * Consider the risks and how available (and protected) your data is)
* Bring In The Professionals
  * In the same way that you will refer a patient to a Specialist, it is important to refer your IT to a Specialist as well

WYSCOM
wise in communications

Internet Security – Protecting Your Business Into The Future

* Security Culture
  * Implement & Promote It
  * An organisation with a strong security culture is critical in remaining vigilant in the ever changing world of internet security
  * An educated staff member will not only know not to click on the link or open the attachment in an email, but will also promote these values and practices to other employees

WYSCOM
wise in communications

Internet Security – Protecting Your Business
Thankyou

* Questions?

WYSCOM
wise in communications