Protect Your Business

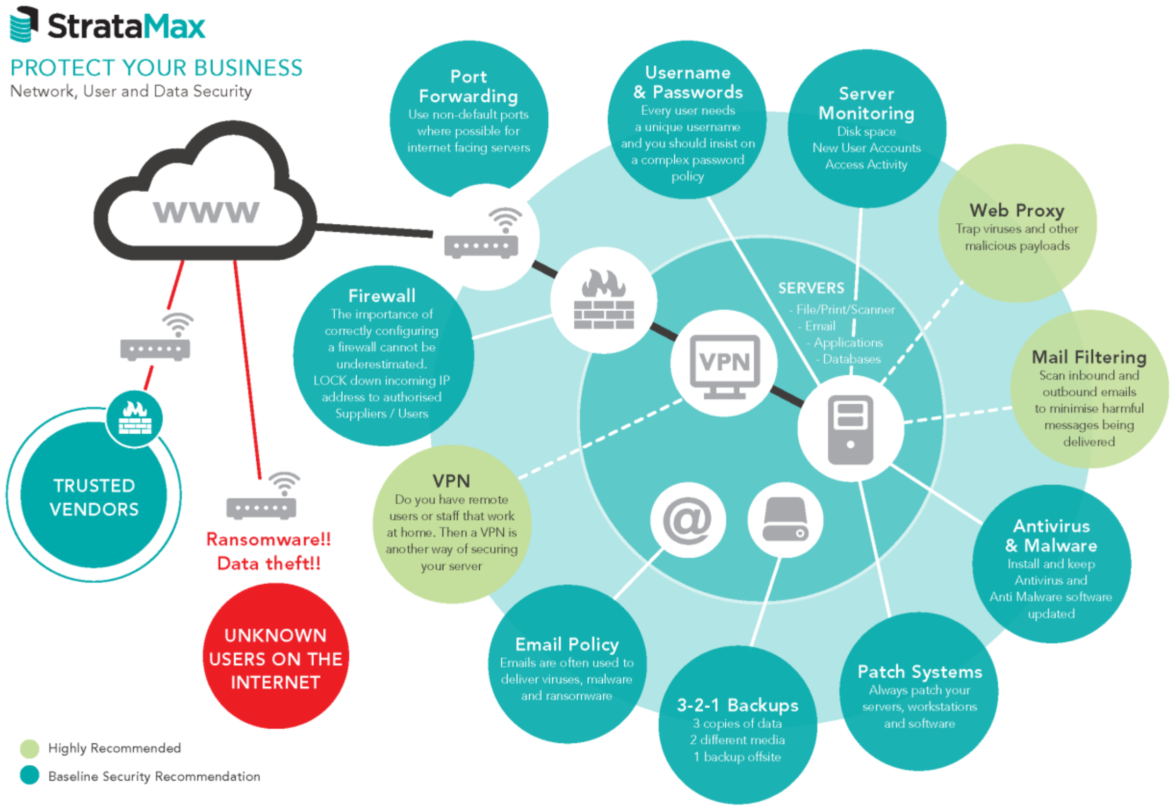
Network, User and Data Security

As a technology specialist to the Strata Industry for over 30 years, StrataMax has a wealth of experience in helping strata management companies maximise their use of technology to gain efficiencies and better service their clients.

It is evident that some strata management businesses have been struggling to keep up with the demands of emerging technologies and cyber threats. While each company may use varying technologies and solutions, the core security requirements are generally the same.

In your office, both staff and contractors will utilise various applications to get their job done. Many of these applications are required to connect to the internet in order to serve their function. It is via this internet connection that the majority of cyber threats originate.

How can you protect your business?



StrataMax

PROTECT YOUR BUSINESS

Network, User and Data Security

- File/Print/Scanner
- Email
- Applications
- Databases

Port Forwarding Use non-default ports where possible for internet facing servers

Username & Passwords Every user needs a unique username and you should insist on a complex password policy

Server Monitoring Disk space New User Accounts Access Activity

Web Proxy Trap viruses and other malicious payloads

Mail Filtering Scan inbound and outbound emails to minimise harmful messages being delivered

Antivirus & Malware Install and keep Antivirus and Anti Malware software updated

Patch Systems Always patch your servers, workstations and software

3-2-1 Backups 3 copies of data 2 different media 1 backup offsite

Email Policy Emails are often used to deliver viruses, malware and ransomware

VPN Do you have remote users or staff that work at home. Then a VPN is another way of securing your server

Firewall The importance of correctly configuring a firewall cannot be underestimated. LOCK down incoming IP address to authorised Suppliers / Users

● Highly Recommended

● Baseline Security Recommendation

Port Forwarding

Use non-default ports where possible for internet facing servers.

The Internet is full of standards which make everything work but these very standards also make it easy for a would-be hacker to scan your servers and attempt to hack them. In many cases they can simply guess the generic usernames and passwords which are often configured.

Firewall

The importance of correctly configuring a firewall cannot be underestimated. LOCK down incoming IP address to trusted Vendors and Users

Locking down an Internet facing network is a must. Port scanning occurs every second of every day and it literally takes minutes for a new computer connected on the internet to be found. By configuring your Firewall to allow only Trusted Vendors and Users IP addresses it will significantly reduce the risk of an outside hack.

Username and Passwords

Every user needs a unique username and you should implement a complex password policy.

Many business still have generic usernames and poorly created passwords and as a result are very vulnerable to outside hacking.

Email Use Policy

Emails are often used to deliver viruses, malware and ransomware.

Having a staff training program in place to make sure all users of email know what to look for with regards to SPAM, Malware and Malicious attachments is important. Fake bills and invoices often contain some form of Malware or even Ransomware such as CryptoLocker which can infect all your files.

Backups (3-2-1)

3 Copies of Data, 2 different Media and 1 Backup offsite

Backing up can be really inconvenient. Having multiple copies of data and keeping it secure takes time but how would your business survive if you suddenly lost all of your client data. By introducing a simple 3-2-1 policy this could save your business. Keeping 3 copies of your data, on 2 different forms of media and making sure 1 is securely kept offsite will allow your business to survive a disaster. Last but not least, you have to regularly test your backups in order to rely them.

System Patching

Always patch your servers, workstations and software.

A good system is a patched system. Microsoft releases security fixes for Windows and office applications every month. Router suppliers and printer manufacturers also often update built-

in firmware. Without these patches being installed you are simply exposing your business to hundreds of known vulnerabilities and exploits used by hackers.

Antivirus and Antimalware

Install and keep Antivirus and Antimalware software updated.

Computer viruses have been around for over 30 years but today's viruses, in particular Malware is nastier than ever. You have Key loggers capturing every key stroke typed which may include your bank account details. Others could deliver crypto payloads which hold you to ransom. Some malware is able to take complete control over your server. Installing and maintain your Virus and Malware protection is your best defence.

Server Monitoring

Monitoring Disk space, New User Accounts and Access Activity.

The only way you'll know whether someone has accessed your computer or created a new Administrative user account is via server monitoring software. The same software can also provide alerts on low disk space and prevent your servers from crashing and suffering data corruptions as a result.

VPN

If you have remote users connecting to your office, the use of a VPN is best practice for security.

A virtual private network enables users to send and receive data across shared or public networks as if their computing devices were directly connected to your private office network. VPNs should encrypt the data making it extremely difficult for other's to intercept what is being transmitted.

Web proxy

Trap viruses and other malicious payloads.

A web proxy can limit access to inappropriate websites that may contain viruses, malware or non-work related content. As a security measure this will reduce the risk of cyber threats through the web browser. As an additional benefit by reducing non-work related internet content, precious bandwidth is conserved for work purposes.

Mail Filtering

Scan inbound and outbound emails to minimise harmful messages being delivered.

Scanning all inbound emails can certainly help keep viruses and malware from getting to your staff and significantly limit your company's exposure to malware and damaging ransomware. Another thing to remember is that scanning outbound emails also limits your exposure in the event that your system is compromised and becomes the source of sending out SPAM and other damaging emails to your own clients.

We strongly recommend that you discuss these options with your trusted IT partners and providers.

So what happens if your computers, servers and data are not secure? Besides the impact to your business and clients, did you know that the Australian Government passed the Privacy Amendment (Notifiable Data Breaches) Bill 2016 in February with bipartisan support meaning that organisations will have to reveal if their system are compromised by cyber-attack or technical failing.

Besides having to notify the Privacy Regulator you may be required to notify your clients that their personal information may in the hands of an unknown third party. This disclosure could be quite damaging to your business and reputation.

Basically, systems don’t look after themselves. They require regular maintenance and ongoing updates and upgrades in order to keep them safe and functioning.

Taking the time to correctly configure your computing environment and making sure that regular maintenance is carried out will be one of the wisest investments you’ll ever make.

To help you get started with the necessary conversation you should be having with your technical support team, please refer to the following checklist.

Discussion checklist

	Baseline Security Recommendation	
1.	Firewall (lock down incoming IP addresses)	□
2.	Port Forwarding (user non-standard ports)	□
3.	Usernames & Passwords (use complex password policy)	□
4.	Backups (have you got a reliable backup strategy in place)	□
5.	Antivirus & Malware protection	□
6.	Patching (when, how and by who)	□
7.	Email Policy (education and training policy for staff)	□
8.	Server Monitoring (disk space, new users and access activity)	□
	Highly Recommended	
9.	VPN access for remote users	□
10.	Web Proxy	□
11.	Email Filtering	□