CYBERSECURITY:

Can you defend your data?

www.masmanagementsystems.com.au

Cybersecurity is big business and big news.

Many more of us are in hybrid arrangements, working from home and in the office.

Businesses have had to re-think not just how they work but also the security of their systems.

As if it wasn't under enough pressure during 2020, the healthcare sector was particularly hard hit with malware, ransomware and hacking.

This exposed loopholes across Government and private healthcare sectors but also demonstrated the importance of regular data backups.

Many ISO standards including ISO/IEC 17025, ISO 15189 and ISO 9001 contain requirements for ensuring the security of your computerised systems.

And as you'd expect from ISO, there's also a standard on information security management- ISO 27001.

These requirements don't just cover control of data and information management. They also address where you store it, how you store it and who can access it.

Controlling access to your lab network

You may already have a firewall set up for your organisation including multifactor authentication. That would probably work well within the lab and organisational intranet but what about when people are working from home?

Generally speaking, we tend to be less concerned with cybersecurity on our personal devices. However, each time an external device connects to a network, it's like putting a tiny hole in that network.

If you can access your emails through your smartphone, laptop, or tablet, that's an opportunity for you to inadvertently pass on malware.

Are smarter devices really a smart idea?

The increase of automation and smart devices in labs means more hacking opportunities.

Consider your lab balance for example. It's connected to your network, but does it have the same level of protection as your laptop? Does the manufacturer provide patches to ensure the device can't be accessed?

Hackers are particularly interested in personal information and labs have plenty of this.

Data isn't available on whether access through a lab balance has occurred, but this is a vulnerability that needs to be considered. Devices can be purchased that are more resistant to cyberattack.

The US Government's National Institute of Standards and Technology (NIST) recommends that any new smart devices – whether it's a balance, liquid handler, or coffee pot – should have the following features or capabilities:

* **Identification:** A unique address on computing networks
* **Configurability:** A lab manager should be able to change or update its security software and firmware configuration
* **Data protection**: Encryption or other data protection methods embedded into the device to protect it from unauthorised modification
* **Limited network interfaces:** Devices should require user authentication to access them thereby limiting their access to the local and wide area networks
* **Software and firmware updates:** A secure, configurable way to update software and firmware should be available, whether automatic or manual
* **Event logging:** Cybersecurity events should be logged by the device to alert lab managers to vulnerabilities and to enable forensic analysis if hacked.

In addition, a virtual private network (VPN) should be established for any devices that personnel can access remotely.

It's becoming easier to find devices that have these security features. However, hackers are sneaky and will keep trying to find vulnerabilities.

That's why installing patches for your equipment as they're released is critical. Although nothing is 100 percent secure, these patches may mean that hackers may decide it's not worth the effort and move on.

Zero trust environment

While we certainly don't recommend zero trust in your colleagues, in the cyber world this could save you a lot of time, anxiety and money.

A 'zero trust' cyber environment means segmenting your equipment from the wider company network. This means that if a hacker penetrates that part of the firewall, they're still locked out from other network segments.

Data back up

Businesses recognise that data is their most valuable asset (along with their staff, of course!).

And yet around 60 percent of small to medium size enterprises (SMEs) still prefer to back up their data using direct attached storage. And almost half of those have experienced data loss, some of which was unrecoverable!

Holding data in cloud storage makes perfect sense. The public cloud has proven to be safer than private data centre environments based on-premises.

However, that doesn't mean you shouldn't be mindful of your provider's security infrastructure. For example, what security measures do they have in place during data migration?

www.masmanagementsystems.com.au

Ensure that you have a process in place to carry out regular backups of your data. Write this into your quality system.

In case of disaster

Despite best efforts, if the worst happens and a breach occurs a crisis management plan should be in place.

In some cases, your business may be required to notify authorities of data breaches. Keep this in mind when preparing your crisis management plan.

Include the crisis management plan in your manual. This will demonstrate to any external accreditation or certification body that privacy and possible breaches have been seriously considered.

A word of warning about your disaster recovery plan. Do NOT wait until a disaster occurs before you test it!

Test and trial this regularly and ensure you have regular and open communication with your storage provider. They'll understand you need to be sure the recovery process is swift and seamless. And that you need to be certain with regular testing.

If not? Find another provider.

Support and advice

There are so many variables and decisions to make about data security, it can be overwhelming.

We discuss some of this during our Risk management in your lab training course but IT Consultants such as our friends at AUP IT and Crypses can take all the guesswork out of data security for you.

In a future article, we'll examine some of the options for protecting your data.

You don't have to do this alone!