eBook

Your Ultimate Cyber Security Handbook

The essential information you need to effectively protect your business from current cyber threats

Modern cyber security risks

As we near the end of 2021, one thing is clear: the digital landscape has changed forever. Following the effects of Covid-19, businesses were forced to adapt to remote work almost overnight. Luckily, most organisations found that intelligently using technology allowed their businesses to not only survive, but thrive in the pandemic. The ability to effectively innovate, collaborate and communicate using IT has meant that hybrid working is here to stay for many companies, even as Covid eases.

Although the pandemic offered the chance to implement creative and inventive IT solutions, it also created huge cyber security risks. Cyber criminals were able to exploit businesses' increased reliance on technology for their own gain. As we move forward, we are facing a far more sophisticated threat landscape, with increasingly diverse and varied methods of attack. In order to protect your business, you need to know what your company is up against.

Phishing and spear phishing

Phishing is a dangerous type of cyber-attack that relies on social engineering. Criminals send fake correspondence, most commonly emails, masquerading as official messaging, to try and get you to divulge sensitive information or download malware to your device. Although general awareness of phishing is growing, you cannot drop your guard. Phishing emails are becoming more advanced.

In particular, the rise of spear phishing is a concern. In contrast to phishing, which targets the masses with a generalised rhetoric, spear phishing emails target specific individuals or organisations. You are far more likely to open an email that appears to contain sensitive information that is directly linked to you. You need to prepare your business for the increase in spear phishing and invest in further training to ensure that your staff do not fall victim to this type of scam.

Ransomware

Ransomware has been on the rise in 2021. Ransomware is a type of malware that encrypts data until a ransom is paid. This type of cyber-attack exploits the fact that businesses' data is exceedingly valuable. Recently, double-extortion ransomware has become more common. Cyber criminals know that your data is confidential and sensitive. With a double-extortion attack, they not only encrypt the data so that you can no longer access it, but they steal it too.

The threat of publishing your data is meant to encourage you to pay the ransom. As double-extortion ransomware has become more popular in recent years, it is important to prepare your business for both types of ransomware attack.

Modern cyber security risks

Exploitation of remote access solutions

As it became common place to work from home, workplaces needed solutions that would allow employees to access the information they needed remotely. Virtual private networks (VPNs) allow team members to access their corporate network with a hidden IP address and location. Remote desktop protocol (RDP) allows employees to access their work desktop and connected applications virtually, via the internet.

While these solutions enhanced remote productivity, they also created easy targets for exploitation. Cyber criminals monitor for unprotected, unpatched VPNs or poor password security, and capitalise on vulnerabilities, gaining access to corporate networks. This allows them to steal data and information or plant ransomware, which would be extremely damaging for your business.

Compromised endpoints

The rise of remote work has resulted in more people using personal devices for their job. However, BYOD creates a number of security issues. Personal devices often do not benefit from the same level of cyber protection as corporate devices. Often personal devices are not updated as frequently, meaning that they do not benefit from the protection of regular patches. Your employees' devices might not even be compliant with your corporate policies.

Have you checked? Cyber criminals are more than aware of these weaknesses. It is vital that you employ effective endpoint protection and encryption across all devices that access your corporate network, to ensure that cyber criminals cannot prey upon exposed information.

Cloud computing vulnerabilities

Cloud computing and cloud-based solutions offer businesses increased flexibility, agility and scalability. Fittingly, many businesses are starting to migrate to the cloud. However, this move comes with a host of security challenges. If your business is using a public cloud, you need to consider how you are protecting your information.

The public cloud is a multi-tenant environment which inherently creates vulnerabilities. A singular problem within the infrastructure could adversely affect your data's security and have a knock-on effect for the entire company.

Why does your business need strong cyber security?

Small and medium businesses are particularly at risk of a cyber-attack as cyber criminals believe, often correctly, that SMEs are not doing enough to protect themselves. This makes them easy prey.

Understanding why you need strong security is the first step to protecting your business. At Apex, we understand that implementing the correct cyber security can appear overwhelming, but it is extremely necessary. Leaving your business open to attack is dangerous for you and your clients.

So, why exactly should your business adopt strong cyber security measures? Here are five key reasons:

Data protection

Your data is valuable and confidential, which makes it extremely appealing to cyber criminals. Adopting a strong cyber security strategy will protect against data breaches and loss, saving you time and money.

Compliance

General Data Protection Regulations (GDPR) came into effect in 2018, meaning that businesses have a legal duty to ensure the security of their staff and clients. If you breach GDPR, you not only place your business at risk, but you are liable to pay fines too.

Protect against downtime

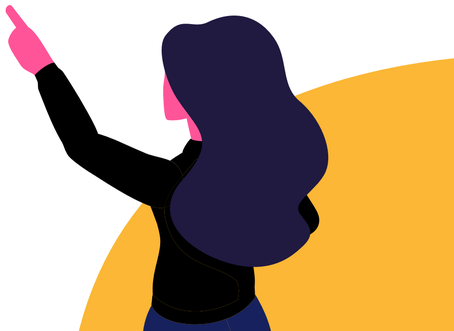
Suffering from a cyber-attack or data breach could reduce your business' operational capabilities, affect your service delivery or even place you out of action all together. Unexpected downtime is expensive for any company. Luckily, the correct cyber security can help to minimise it.

Save money

Data breaches, downtime, GDPR fines, client loss, lawsuits – these are all extremely costly for your business, and all potential outcomes if you do not implement the right cyber security measures. The cost of investing in strong cyber security and training your team is far less than the expense you will face if you suffer a cyber-attack.

Increase credibility

Your clients trust you with their sensitive, confidential data. If your business is the victim of a data breach you will damage your reputation and could potentially lose customers. On the other hand, demonstrating that you have the necessary cyber security provisions in place is a great trust builder, and will instil your clients with confidence in your company.



The benefits of a fully managed cyber security stack

While it is important to put cyber security measures in place for your business, you need to ensure that you are doing so safely and intelligently. Using different providers for different areas of your cyber security is problematic. Have you ensured that every area of your business is protected? Has each area received the same quality of security? Are there any gaps in your defence, or vulnerabilities left exposed?

When you choose an outsourced, fully managed cyber security stack, you can lay these worries aside. Your business will receive expert cyber security protection on all fronts, for a cost-effective price.

So, how could outsourcing your cyber security to a managed security services provider like Apex Computing, benefit your business?

Identify and understand vulnerabilities

A managed security service provider will help you to understand the current security risks and highlight any vulnerabilities in your IT infrastructure. From there, they can create a specific, tailored security support plan to protect your business.

Receive proactive support

Real-time, proactive monitoring helps to identify and prevent security threats as they occur. Using an RMM, Apex will monitor the real-time health of your anti-virus program, audit all your devices, monitor the status of Windows Updates and even more. This helps to ensure that your business is never exposed to cyber threats.

Benefit from expertise and leading tools

When you outsource your cyber security, you gain access to expertise from security specialists and products and tools from industry-leading vendors. Apex have partnerships with the best security suppliers to ensure that we can provide you with the highest quality solutions for the best possible price.

Real-time threat intelligence

Early threat detection and prevention is key to keeping your IT systems, and business, operational. Managed security service providers have specialist knowledge about the latest cyber security threats, making them better equipped to protect your business. When it comes to cyber security, your company will never be behind the times.

Protect your data

Managed security service providers employ a range of tools, software and processes to ensure that your business does not suffer a data breach. From educating your staff about cyber security, to providing advanced firewall solutions, to carrying out security audits, Apex will ensure that your business' assets have the best defence.

Rapid response to cyber-attacks

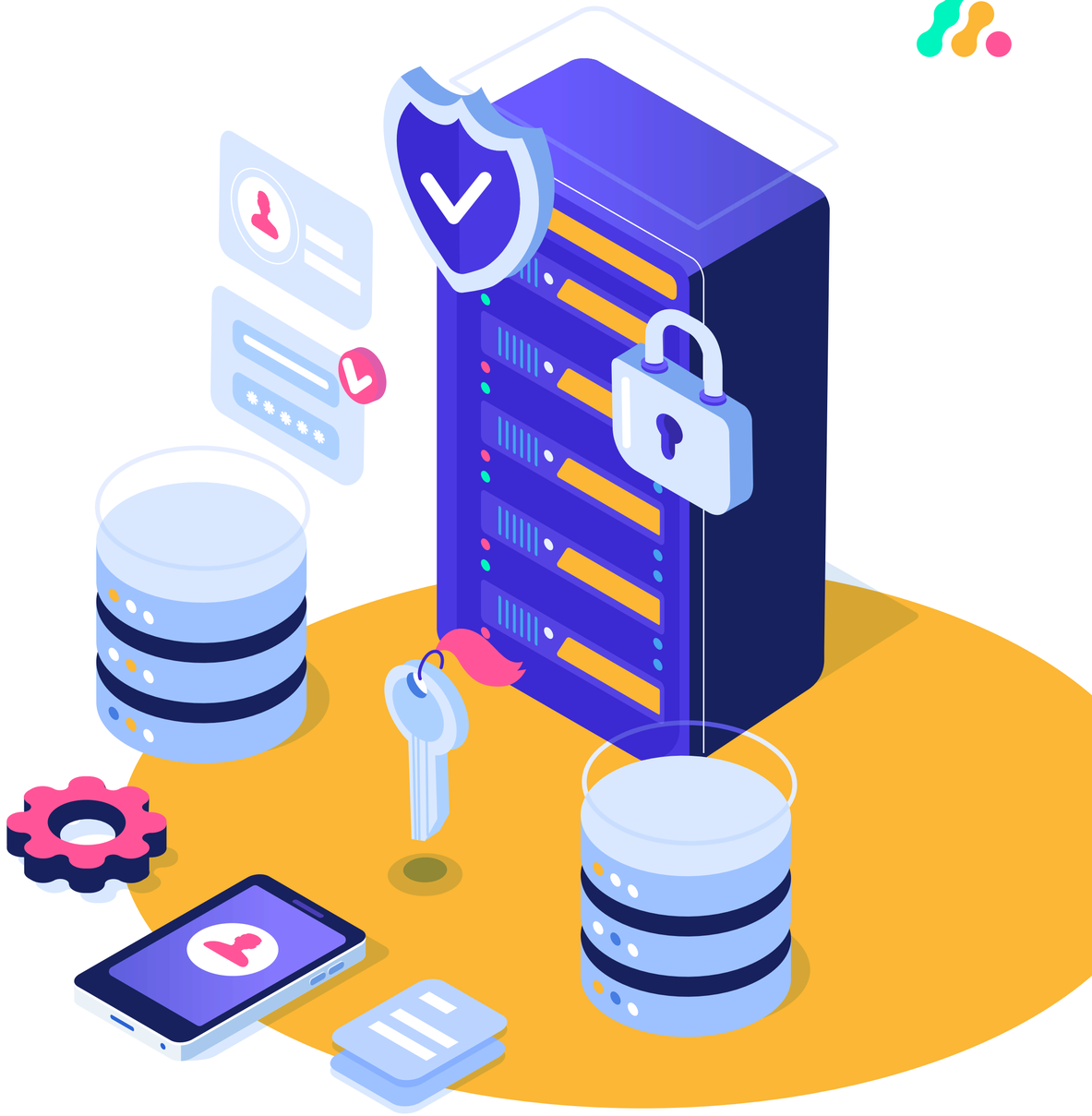
If a cyber-attack occurs, your business needs it to be contained and remediated efficiently to ensure that your IT systems remain functional and effective. Apex offer reliable support 24/7/365, so that you can feel confident that security assistance is available whenever you need it.

Apex’s managed security service

Apex’s team of dedicated, qualified IT experts offer full monitoring, support and management of your business’ cyber security. We can operate remotely or onsite according to your need. Whatever the problem, whatever the time, we can provide you with rapid assistance from a specialist security technician.

We offer three bespoke security packages: Basic, Standard and Premium so you can choose the level of cyber security support that is right for you. This system operates in a similar way to the Silver, Gold and Platinum Service packages from Apex that you will be used to. Introducing separate security packages allows your business full control of every aspect of its IT infrastructure. Everything is completely tailorable to your needs. For instance, if you need minimal overall IT support, but extremely strong cyber security, you might choose the Silver Service package alongside the Premium Security package. Alternatively, if you require more constant IT support, but only basic security services, you might prefer to select the Platinum Service and Basic Security packages respectively. It’s all in your hands.

As the threat landscape has developed, we want to offer you a more customisable cyber security experience. Introducing security packages on top of our existing service packages allows us to focus efforts specifically on offering your business the best possible protection. Plus, our range of add-on cyber security products and services, including security audits, Cyber Essentials accreditation, back-up solutions and more, ensure that your business is armed with the best defences no matter what your security concern is.



Apex’s managed security service

Monitoring

Apex will deliver full monitoring and management of your cyber security solutions. We monitor your anti-virus health and Windows updates across all three packages, and include Office 365 and Dark Web monitoring in our Standard and Premium packages. We also include monthly cyber security device and M365 cloud security reports, to keep you informed about the status of your protection.

Penetration Testing

We highlight areas of vulnerability in your business by carrying out in-depth penetration tests. These tests provide us with vital information that help us to prevent and manage risks. The health of your security systems is our priority.

Training

Your employees are your first line of defence against cyber-attacks. If they are not properly equipped, then your business is vulnerable. As part of our Premium security package, we educate your team through online cyber training and send phishing email testing to your staff, so they are prepared for the threats they may face.

Endpoint protection

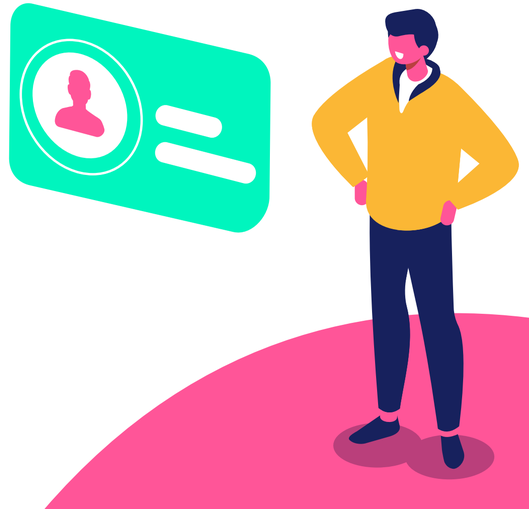
We understand the importance of protecting every device that your team uses and encrypting your data effectively. Our centralised protections make endpoint protection more efficient and secure. Our Standard and Premium security packages also include an endpoint ransomware protection tool to ensure that your employees can use any device with confidence.

Firewalls and Filtering

Apex offer advanced threat protection through robust firewalls and anti-spam email filtering. We inspect all traffic coming into your network and prevent attacks before they can reach your internal devices. We ensure that your security foundations are solid, before implementing more complex defences.

Secure VPN connections

Apex help to make your VPN connections more secure. Your team will access company data via a protected network, so they can work securely while remote, and ensure that sensitive data remains private.



Want to make your business cyber secure?

When it comes to cyber security, you can never be too prepared.
Your data is too valuable to leave anything to chance.

Ensure that your company is armed with the best possible defences today.

To find out more about how Apex's fully managed security stack could protect your business, book a strategy session with an Apex Computing cyber security expert today.

Book a meeting