timeless

Your Free Extensive Guide...

How To Keep Your Business Cyber Secure

Table Of Contents

Introduction

Technology has revolutionized the way businesses can operate and compete in the modern world. With the rise of new digital technologies and the ever-growing knowledge base we know as the Internet, it has become easier than ever to streamline your operations, automate your processes, reach new markets, and engage with your customers. Not only leading to improved customer experiences and more efficient systems but increased profitability throughout your business.

While these advancements in technology are incredibly useful for businesses, it offers ample opportunity for cyber criminals to find and exploit new vulnerabilities within this new technology, finding weaknesses within their systems and networks that can be exploited, exposing your business to cyber threats that can cause irreparable damage, making the investment of cyber security evermore relevant.

But what is cyber security and why is It so important?

Part One

What is Cyber Security?

Cyber security is the practice of taking proactive action to protect your computer systems, networks, and sensitive data from being stolen or exploited by those with unauthorized access.

It involves a range of strategies designed to safeguard your digital devices, data, and networks from viruses, malware, and hacking attempts that can often cause data leaks and significant financial and reputational damage to your business, which can often be incredibly difficult to recover from.

60%

of all small businesses that experience a data breach close within 6 months of the attack.

Why is Cybersecurity Important?

Cybercriminals specifically look for vulnerabilities within technology to steal sensitive data. Whether financial, employee, or customer data, the details within your business can be stolen and sold for a high price on the dark web, potentially causing chaos within your business. Not only is data theft often irreversible, but a business can also be faced with Ransome requests where cyber criminals expect a large sum of money to be paid to return the stolen data.

Even when retrieved, businesses can be left with hefty fines under the data protection act when data is misused, and the correct procedures are not followed. The safety and protection of your digital assets and data is your responsibility and is essential in promoting the longevity of your business, therefore investing in a robust and layered cybersecurity model should be your number one priority.

Part Two

What risks do you welcome when cybersecurity is not your priority?

When your cyber security is not proactively managed by an IT provider, your business accepts a multitude of risks associated with the vulnerabilities within technology that can leave your data and systems in the hands of cybercriminals. These risks include:

1. Data Breaches

Data breaches are one of the most common cyber-attacks in the world. Just in the UK, one small business is successfully hacked every 19 seconds, which is often the result of poor password management and user access control. Data breaches leak sensitive information including personal, employee, financial or customer data which can lead to identity theft, financial loss, and reputational damage. Not only are you putting your data on the line, but the data of your customers and clients too.

2. Reputational and Financial Damage

A lack of cyber security infrastructure can make your organisation appear careless and negligent, not only that, but if your business is hacked and experiences a data breach, your customers and clients are put at risk too. The average remediation cost of successful a ransomware attack on a UK Enterprise is £700,000, most businesses will never recover from such a loss. There are also legal and regulatory consequences that can occur when a business is found to be negligent by the ICO under the Data Protection Act 2018.

3. Malware and Virus Infections

Accidentally downloading malware or viruses onto your computer system can cause irreparable damage. It is as simple as clicking an attachment on an email which can be spread throughout your network to corrupt and delete data. These malware attacks can disrupt your daily operations and run deep into the core of your business.

4. Phishing and Engineering Attacks

Your employees are your business's greatest asset, this also makes them the number 1 target for cybercriminals. Phishing campaigns and social engineering attacks encourage your employees to click on unsafe links, leading them to fraudulent websites or webpages that install and run malware quietly in the background on their computers. Clicking on a suspicious link or accidentally downloading malware is all that is needed to cause serious damage to your business, making cybersecurity security training incredibly important.

Part Three

How can Cyber Security future-proof your business?

A robust and proactive cyber security approach includes layers of protection to help avoid data loss if a breach occurs. This involves vulnerability detection and management, something a dedicated IT can manage to ensure your business is cyber secure. To keep the impact of successful cyber-attacks to a minimum, vulnerabilities within your technology and systems within your business must be appropriately managed.

A lack of internal controls, outdated operating systems, and a lack of network protection are all vulnerabilities that can be easily exploited by cybercriminals. Hackers can gain illegal access to your systems and expose your data, not only hurting your business but hurting your client's business too. releasing your clients and customers' personal and financial data all over the dark web for anyone to use and purchase is a massive breach of GDPR law and can make your business liable for compensation of all affected customers.

In this way, data breaches can be incredibly expensive and often cripple blooming companies.

Firewalls

Firewalls are network security devices that monitor incoming and outgoing network traffic and that determine whether to allow or block certain connections based on a previously defined policy. Firewalls have been considered the first line of defence in network security for over 25 years.

Firewalls create a barrier between secure and controlled internal networks and more vulnerable outsider networks such as the Internet. While there are many different types of firewalls, firewalls essentially provide granular control over your network traffic to enforce security policies that suit your business while minimizing the risk of security breaches.

Suspicious activity including abnormal access patterns, suspicious file changes, unauthorised port access and changes reported by the end user (such as: pop-ups, slow devices, and unauthorized toolbars) are all examples of suspicious network activity that your organisation needs to account for.

It's easier for cyber criminals to intercept communication between systems and breach your network if poor encryption is used. Unencrypted information, if leaked, can cause severe cyber security compliance issues, and can lead to massive fines from regulatory bodies.

Data Encryption

Data encryption is an important line of defence in your layered cyber security architecture. It makes your data inaccessible to malicious or negligent parties by using an encryption algorithm to make your data unreadable. This can only be broken with large amounts of computing power and can only be made readable again once decrypted.

Essentially, your file is converted into a new language that cannot be read without an encryption key, which only your business has access to. Once the file is delivered, it can be decrypted, and your file will be retrieved.

Anytime you send a file over the Internet, there is a chance hackers can intercept this file and breach it. Therefore, sensitive files and customer data should always be encrypted when sent via the Internet.

Endpoint Security

Endpoint security aims to prevent entry points of end users' devices, such as laptops and mobiles, from being exploited by cybercriminals. If a device is connected to a network, it is considered an endpoint. These security systems protect the endpoints on either a network or in the cloud. As endpoint security has evolved from your traditional antivirus software, these solutions can now provide comprehensive protection from sophisticated malware and zero-day threats.

Endpoint security is considered the first line of defence against cyber threats. As technology evolves, and the threat landscape becomes more complicated, endpoint protection is vital in protecting your business from cyber-attacks.

Multi-factor Authentication

Multifactor authentication (MFA) is an important security feature that provides an extra layer of protection in your cyber security architecture by requiring additional authentication methods before allowing access to your accounts. Where traditional authentication methods rely on the end user's username and password, MFA uses security tokens either in the form of fingerprints, face ID, or one-time passwords to provide an extra layer of security before login. This prevents cyber criminals from accessing your account even when your password has been compromised.

DNS Protection

DNS (Domain Name System) protection adds another layer of security between your employees and the cyber threats lurking on the Internet. It filters out unwanted traffic and adds suspicious URLs to a blacklist. Hackers can alter the DNS information of a website to point communications to their servers rather than an authorised server. This redirection can allow hackers to steal your data, launch phishing attacks or introduce malware onto your computer. By using DNS protection, you can prevent successful phishing campaigns and stop your endpoints from accessing inappropriate content and conversing with malicious infrastructure.

Dark Web Monitoring

The dark web consists of hidden websites beyond the reach of the general public that can only be accessed using special software. These websites are not indexed by search engines and are often associated with illegal activities. The dark web provides anonymity for its users which makes it difficult for enforcement agencies and government bodies to regulate it. While cybercriminals use the dark web for illicit activities, there are however legitimate reasons for using it, such as providing access to information in countries with strict censorship. Dark web scanning and monitoring is an important part of your cyber security structure that will search through databases on the dark web for any of your personal information that is available for sale.

This protects your business and personal credentials from identity theft and fraud and alerts you to any sensitive information that has been leaked. Being able to monitor and prevent this breach of sensitive data is an incredibly important task in protecting your business, one an IT provider should manage.

Cyber Security Awareness Training

While your employees are your best asset, they are also the main target for cybercriminals. If your team fall victim to a phishing campaign, they can trigger a data breach or download malware onto their computers. It is as simple as clicking a suspicious link. Cyber security training raises awareness about all the threats and opportunities cyber criminals look for to steal your data or damage your business.

To avoid data breaches and maintain a solid cyber security structure, employee awareness training is a must.

Email Security

As email is a massive source of customer communications, it becomes a target for cybercriminals. Most phishing campaigns and malware attacks are spread through email, with dodgy attachments or suspicious links that can erupt into major cyber security issues if clicked and downloaded. Email security services aim to protect you against impersonation and spoofing emails that aim to harvest data by tricking the end user in believing that they are speaking to a reliable contact.

Full Disaster Recovery

While some services provide options to back up your data, investing in a cloud-based cyber secure backup is yet another important factor in protecting your business. Backing up all of your important information enables a fast recovery of your business operations in the event of a system failure. Creating a disaster recovery plan also helps to minimize downtime when issues occur. This can help prevent a loss of revenue and reduces the impact on your customers.

Many industries also have regulatory requirements for disaster recovery planning and must hold a disaster recovery policy to remain compliant. Overall, disaster recovery is critical for businesses to ensure that they can recover from unforeseen events or cyber threats that may occur.

Part Four

Timeless IMS Cyber Security Guarantee

At Timeless IMS, we recognize how difficult and complex it can be to ensure your business is cyber-secure. As the cybersecurity sector is riddled with technology-focused jargon, it can be difficult to understand what is required to make your business cybersecure and even harder to implement.

We offer our clients a comprehensive support model with a multi-layered set of services with the sole aim to proactively protect your business's assets and data. We aim to grant our clients with peace of mind that their business will never be breached under our services in our new cyber secure guarantee. If a breach does occur, Timeless IMS will cover the cost of any remedial work to get the data back.

To find out more about our Cyber Security Guranatee terms and conditions,
contact us: www.timelessims.co.uk/contact/

Part Five

Conclusion

Security is a moving target. Cybercriminals get more advanced every day. In order to protect your data as much as possible, it's essential that each and every employee makes cyber security a top priority. And most importantly, that you stay on top of the latest trends for attacks and view the newest prevention technology. While this can be a lot to manage, investing in an IT company to manage your risks and secure your business is a vital step in protecting and future-proofing your business growth.

To find out more on how Timeless IMS can help solve and manage your cybersecurity, contact us: www.timelessims.co.uk/contact/

Your Checklist to Cyber Security

Integrate our checklist into your cyber security architecture to futureproof your business and protect your data.

- [ ] **Network Security**
  Protecting your internal network from viruses and malicious activity from the internet, protecting all network devices and their data.

- [ ] **Password Management**
  Ensures maximum strength passwords without having to remember them

- [ ] **Multifactor Authentication**
  An additional layer of authentication on your accounts, preventing unauthorised access.

- [ ] **Malware Protection**
  The bare minimum needed in order to protect your device

- [ ] **DNS Protection**
  Prevents you from accessing malicious or spoofed websites, protecting you and your credentials.

- [ ] **EndPoint Security**
  Protects your local device, includes sandboxing to test for malicious downloads in a false environment to stop any malware before they ever become an issue

- [ ] **Data Encryption**
  To keep your data secure on lost or stolen or intercepted data

- [ ] **Backup/ Disaster Recovery**
  Allows your business to recover data after a breach or employee misuse

- [ ] **Email Security**
  Protects your email account from phishing, spear-phishing and ransomware nuisance emails

- [ ] **Cyber Security Training**
  Ensures your employees have the knowledge to spot any phishing attacks or scam emails they may encounter, proactively protecting your business through employee education.

Copyright Notice

Published by:
Timeless IMS Business Limited
Registered in England, Gladstone
House 77-79 Highstreet, Egham, TW20 9HY
under company number 07236106
'Timeless' and 'Timeless IMS' are trading names of Timeless IT Business Limited
TEL: 0800 328 2852
Email: sales@timelessims.co.uk
Web: www.timelessims.co.uk

Legal Notices

While all attempts have been made to verify information provided in this publication, neither the Author nor the Publisher assumes any responsibility for errors, omissions, or contrary interpretation of the subject matter herein. This publication is not intended for use as a source of legal or accounting advice. The Publisher wants to stress that the information contained herein may be subject to varying state and/or local laws or regulations. All users are advised to retain competent counsel to determine what state and/or local laws or regulations may apply to the user's particular situation or application of this information.

The purchaser or reader of this publication assumes complete and total responsibility for the use of these materials and information. The Author and Publisher assume no responsibility or liability whatsoever on the behalf of any purchaser or reader of these materials, or the application or non application of the information contained herein. We do not guarantee any results you may or may not experience as a result of following the recommendations or suggestions contained herein. You must test everything for yourself.

Any perceived slights of specific people or organisations is unintentional