DigitalXRAID
CYBER SECURITY EXPERTS

| 0800 090 3734
| info@digitalxraid.com

10 Top Tips to Improve Your Organisation's Cyber Security

Why do you need to think about cyber security?

Cyber security is often overlooked, and this means that many organisations are vulnerable and open to attack. The NCSC (National Cyber Security Centre) has reported a record number of cyberattack incidents over the last 12 months, with 20% of these attacks linked to health.

This rise in cybercrime means that organisations must be focusing on cyber security, however, with many businesses unable to prioritise their security due to a lack of in-house expertise, they are susceptible to breaches and other cyberattacks.

If a cybercriminal successfully gains access to sensitive data, it could create lasting damage to an organisation's reputation. The reputational plus financial losses a business could face are huge, including fines and loss of business.

Overlooking cyber security is something that your organisation cannot afford. Below are ten tips to improve your cyber security, with many being methods and steps you can implement today.

Top Tips To Improve Your Cyber Security

Encrypt Your Data

1

The impact of Covid-19 means that in today's climate, more employees are working from home on laptops and personal devices, as organisations are making a permanent move to remote and hybrid working practices. The way we work has changed permanently, and it is important that your security is not overlooked.

Both work, personal and IoT home devices should have all data stored in an encrypted format to ensure all information remains protected and trustworthy. Another consideration would be to have employees use a VPN to safeguard the security of their devices and WiFi, minimising any vulnerabilities and ensuring your organisation is secure.

Check Your Passwords

2

How strong are your employee's passwords? Worryingly many businesses still have relaxed attitudes about their passwords and in general do not have a strong password policy in place. This leads to simple easy-to-hack passwords for accounts which store critical data.

Implementing strong password policies is one of the first steps you can take to strengthen your security. It costs your organisation little in time and money but will ensure strong security and protection for sensitive and valuable data.

If your employees are still working in an office, make sure they never write down their passwords and leave them at their workstation. All passwords should be complex with a mix of numbers, symbols, and letters, and employees should change them every 90 days to ensure safety.

Use a Password Manager

3

It can be confusing when you have dozens of passwords to remember, and often to reduce the confusion users reuse the same or common passwords, which creates vulnerabilities and leaves your company open to attack. Password managers offer a more secure way of coping with password overload; they help users create and securely store the credentials they use to access services such as usernames and passwords.

A password manager means it is easier for staff to use unique passwords that are harder for hackers to guess, your staff don't need to remember as many passwords, and you benefit by understanding how passwords are used in your organisation as well as protecting your company from hackers.

Use MFA (Multi Factor Authentication)

4

Multi factor authentication (MFA), also known as two factor authentication (2FA), ensures that only you, the real owner of your username and account, can log on using the identity which matches your password. Passwords can be unreliable, and an MFA provides additional assurance that you are a genuine employee with permission to access your account.

Why should you be considering MFA for your organisation? It is an easy way to implement data and account protection, as well as being a low hassle means of significantly increasing the security of your accounts and organisation.

Check User Permissions

5

Double check that users have the necessary permissions, system privileges or data access rights. The repercussions if users are given the incorrect permissions could be severe, and the impact of misuse could leave your organisation open to attack. All users should only be provided with reasonable level of system privileges that are required for their role.

Any higher permission access should be carefully controlled and managed to mitigate any potential misuse. It is also important to remove any accounts which are no longer being used as attackers may use redundant or compromised accounts to carry out attacks. If an attacker has access to a privileged system, they could make changes to security controls to enable further or future attacks, causing a much larger breach in the future.

Policies and standards should be established to manage accounts from creation. A corporate password policy should be developed, and all user privileges should be limited to ensure security and continued monitoring of accounts.

6 Pay Attention to Insider Threats

When you think about hackers targeting your organisation, you probably think about outsiders. However, have you considered insider threats? Disgruntled or ex-employees, or insider threats with no direct harmful intent due to a lack of staff training and knowledge, could damage your organisation.

In fact, insider threats can come in all forms, and are often just as dangerous as outsider threats. It could be something as simple as an employee accidentally clicking a link in an email, to an upset employee purposely causing vulnerabilities in your organisation, leaving you open to attack.

It's important you keep an eye on insider threats, visualise threats not just on the outside but internally as well. Reward employees with incentives and keep their morale high, as well as remembering to update staff on any changes and keep them properly trained.

7 Back-Up Your Data Regularly

A crucial part of security that your organisation should already be enacting as part of your overall IT security strategy is data back-up. With secure backups in place your business can survive accidental file deletion as well as phishing and ransomware attacks.

Back-up data should be stored in a secure remote location away from your organisation's place of business. This ensures that if your business is attacked by cyber criminals you can recover any lost data or critical information quickly. There are other repercussions to being breached, but with a secure off-site data back-up in place you can have peace of mind that access to your company's data can be restored in a timely manner.

8 Is Your Staff Cyber Security Training Up To Date?

It's important to remember that anyone who has a password and username in your organisation is responsible for keeping data secure. Employees must be reminded that they should not share their logon information with anyone, including outside parties.

You are probably already aware that your software and programmes should be updated and patched regularly to ensure your computers and devices are adequately protected. However, while organisations often remember this, they often forget the importance of staff cyber security training.

Phishing attacks and ransomware are on the rise, especially over the last 18 months, as more employees are working from home. Cybercrime is increasing, and it is important your employees understand phishing emails, how to report them, and how to stop any potential attacks your business may face.

9 Never Conceal or Hide Mistakes

Alongside the last tip around training, is including education that if employees make a mistake, they need to report it immediately to their manager or IT department so that your organisation can act immediately to limit any losses.

If your company is breached or attacked, do not ignore the issue. Act quickly and it will be solved sooner and hopefully before you suffer unrecoverable consequences to your business.

Ensure that you test your security regularly, and at a minimum install an antivirus and anti-malware system to protect your company from malicious actions. If you conduct a security audit with a professional, it will reveal unexpected weaknesses in your organisation's cyber security.

The correct training, admitting mistakes, and regular security checks, will make sure your company is as safe as it can be.

Invest in Cyber Security

10

The thought of spending money on security before an attack has happened can be off putting for organisations with multiple other priorities. However, many companies with sensitive business credentials and data are starting to acknowledge the importance of cyber security and their role in advocating it.

Investing in cyber security guarantees your organisation is protected from cyberattacks, and that you have systems in place to mitigate the effects of any breaches before they happen. If you are a public sector organisation there will also be compliance and regulations that you need to follow. However, if you are a private organisation, there are still business best practice standards to follow and stakeholder confidence to provide, especially if you work closely with government organisations.

It's important that your organisation is continuously protected from cyberattacks and hackers. Security audits, as well as putting in place policies and procedures to mitigate the repercussions of any breaches, will ensure that your company is doing everything it can to prove it recognises the importance of cyber security and protecting the organisation now and in the future.

Outsourcing to a 24/7/365 cyber security managed service will save you money and will cost your organisation less than employing teams and tools in-house. A cyber security provider also means less internal work, which gives your business more time to focus on your other priorities, confidence you are receiving the best cyber security protection, as well as providing confidence to your board, stakeholders, and customers.

Need support to protect your business?

DigitalXRAID are dedicated to providing our clients with state-of-the-art cyber security solutions. With our cutting-edge tools and techniques, we'll protect your business 24 hours a day, 365 days a year.

We have a top-down approach and will perform a thorough analysis of your organisation's security protocols, systems, and processes with full detailed and comprehensive reports. Our team of experts are here whenever you need us, and we also offer a free incident support helpline if your organisation has been breached and you need us in an emergency.

All our cyber security analysts are fully certified and accredited experts, who can execute a deep dive into your security and complete an extensive examination of any weaknesses and vulnerabilities your organisation may have. We understand all businesses are different and all our solutions are tailored specifically for your business and can construct a service that will fit your company's needs.

We'll shield you from cyber threats, safeguard your digital assets and ensure you stay two steps ahead of the criminals.

Get ahead of the competition. Improve your security by contacting our experts today.

Call us: 0800 090 3734

Contact us

www.digitalxraid.com