IS YOUR BUSINESS CYBER AWARE?

Take our Cyber Security Health Check to identify ways your business can reduce risk and improve defence against potential attacks.

IN 2018...

17%

...of breached small businesses took a day or more to recover

42%

...of small business suffered at least one breach or cyber-attack

25%

...of small businesses had no cyber security policies or risk management measures in place

£894

...was the average (mean) cost of all breaches to small businesses

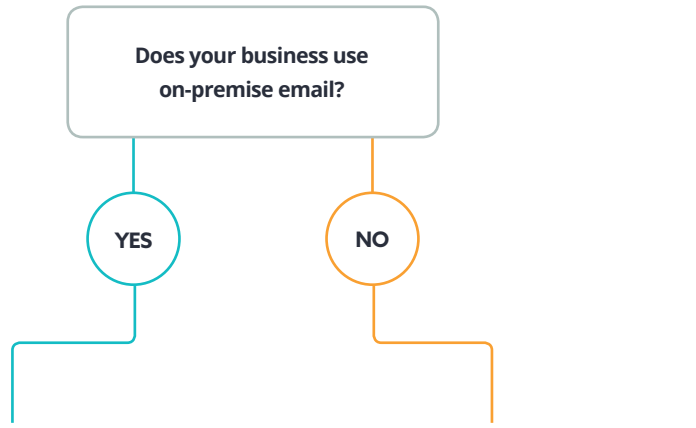
Source: Cyber Security Breaches Survey for Micro and Small Businesses, ONS, 2018

EMPLOYEES OF SMALL ORGANISATIONS WERE...

...more likely to be hit by email threats - including spam, phishing, and email malware - than those in large organisations

Source: Symantec Internet Threat Report, 2019

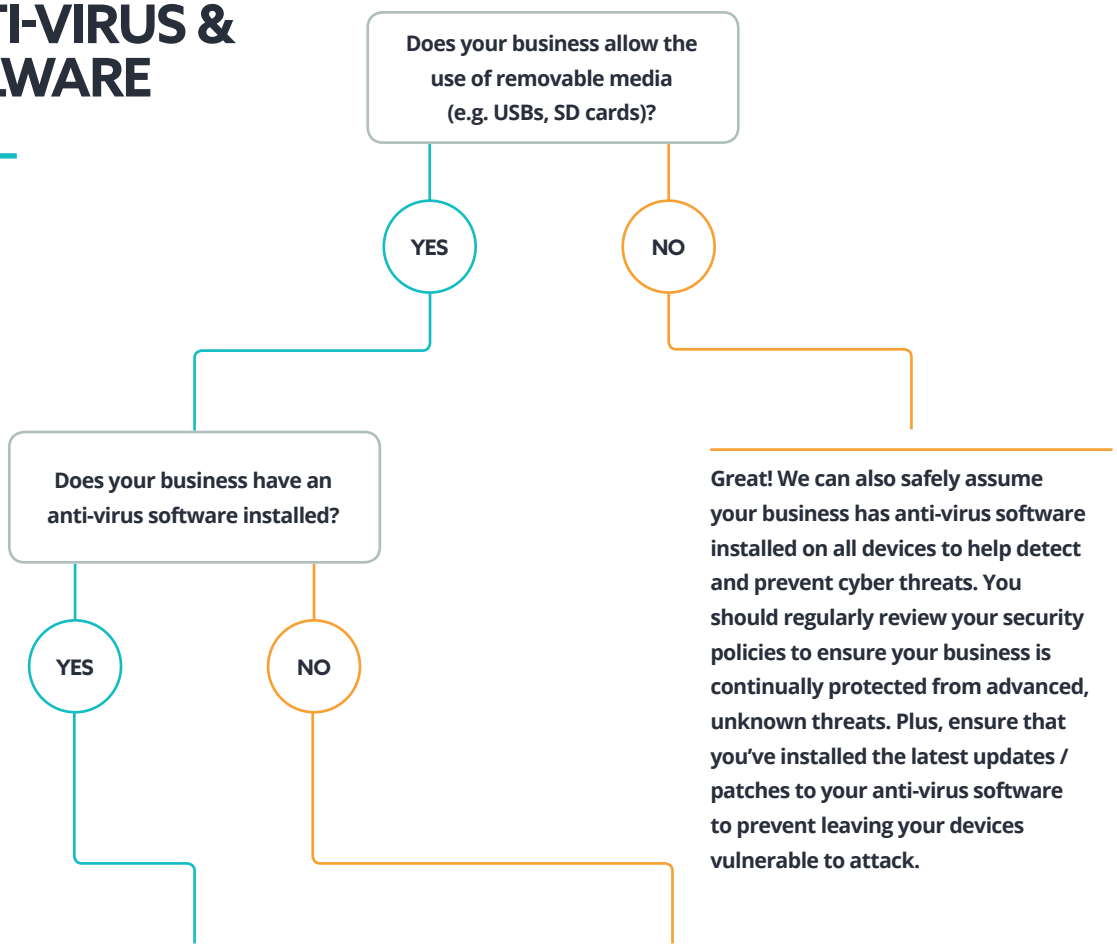
PART 1
SPAM & PHISHING



We recommend transitioning to a cloud-based email such as Office 365 or Hosted Exchange. Not only is it more cost-efficient than on-premise email, your systems are always up to date with the latest security patches. Consider adding a customisable email spam filter onto your mailboxes such as Advanced Threat Protection (ATP) for Office 365 or a third-party email security solution such as Email Safeguard by Symantec for Hosted Exchange to help block cyber threats.

You're probably using Office 365 or Hosted Exchange. While Office 365 will stop the most basic of cyber threats, you should consider attaching an email security solution that blocks both known and unknown threats such as: Advanced Threat Protection (ATP), Email Security for O365 by Vade Secure, Email Safeguard by Symantec (can be used with O365 or Hosted Exchange) or a third-party Email Security solution for Hosted Exchange.

PART 2
ANTI-VIRUS & MALWARE



66%

OF ORGANISATIONS CONSIDER INSIDER ATTACKS OR ACCIDENTAL BREACHES MORE LIKELY THAN EXTERNAL ATTACKS.

Insider Threat Report 2018, Cybersecurity Insiders

PART 3 SYSTEM BACKUP

Do you perform a system backup on a regular basis? (Including servers, workstations, remote devices, VMs etc.)

YES

NO

In the event of data corruption, or a cyber attack, your business data may be irretrievable or could be held to ransom by cyber criminals. It's vital that you perform continuous system backups. We recommend cloud-based backup storage for servers, workstations and mailboxes such as: Acronis Backup Cloud, Azure Backup & Disaster Recovery, Veeam Backup, SkyKick Cloud Backup (O365) or Dropsuite Hosted Exchange Backup.

Is this stored in the cloud?

YES

NO

Does it follow the 3-2-1 backup rule? (1 x backup on-site, 1 x backup off-site, 1 x backup on removeable / storage media).

YES

NO

Do you regularly review your backup process?

YES

NO

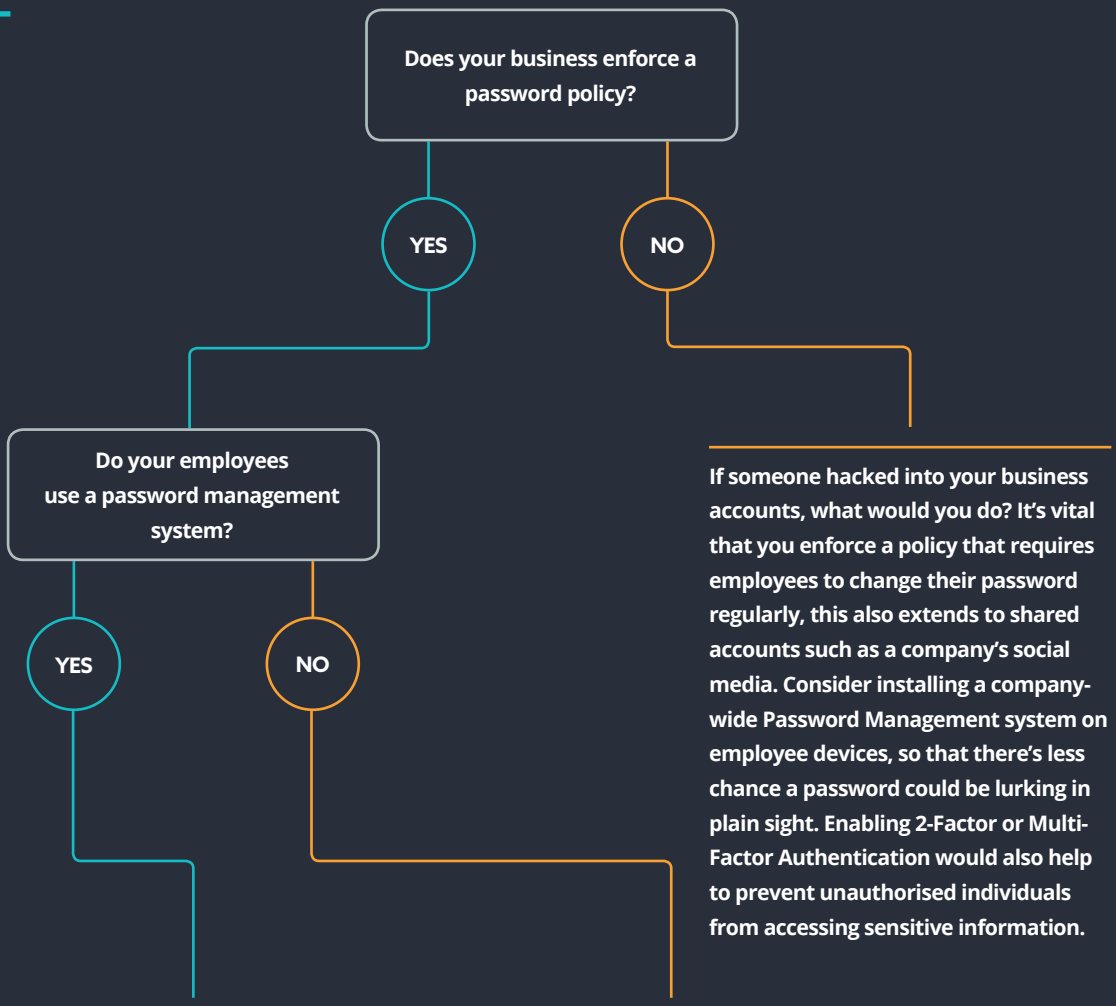
Great – as long as you have more than one system backup you're in a good place. However, we do strongly recommend you store at least one of your backup copies in cloud storage either with Acronis Backup Cloud or with Azure Backup and Disaster Recovery. Not only is it more cost-efficient, it limits data risk, giving you a quicker route to painless restoration.

If your business is attacked and your most recent system backup fails, what do you try next? Following the 3-2-1 backup rule is a good way to ensure your business can recover in the event of on-site data corruption. Having at least one copy backed up in the Acronis Backup Cloud or the Azure Cloud is a cost-efficient way to recover from a cyber breach with fast and painless data restoration.

Great – we advise running Disaster Recovery drills so that you know how long it would take to get your business back up and running from a potential cyber breach. Take note to regularly review your current backup solution.

If your business suffered a cyber breach and your backup failed to restore, what would you do? Regularly reviewing your backups and running Disaster Recovery drills to ensure your business gets back up and running will help to identify potential gaps in security.

PART 4
PASSWORD MANAGEMENT



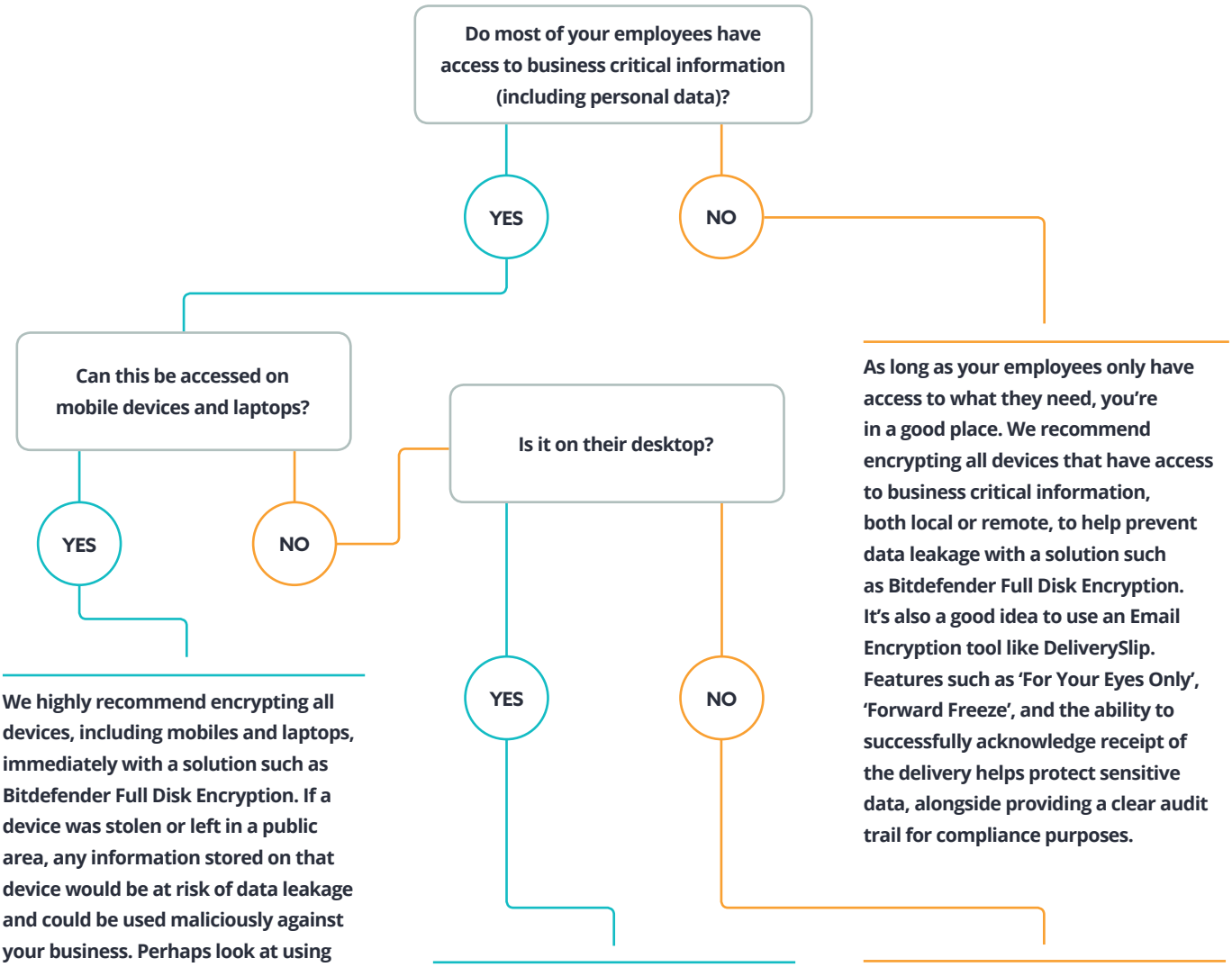
If someone hacked into your business accounts, what would you do? It's vital that you enforce a policy that requires employees to change their password regularly, this also extends to shared accounts such as a company's social media. Consider installing a company-wide Password Management system on employee devices, so that there's less chance a password could be lurking in plain sight. Enabling 2-Factor or Multi-Factor Authentication would also help to prevent unauthorised individuals from accessing sensitive information.

Great – we recommend using 2-Factor Authentication or Multi-Factor Authentication when accessing devices and apps to prevent unauthorised individuals from attempting to view sensitive data. Consider changing passwords regularly when an employee leaves the business to prevent insider attacks.

A Password Management System is a great way to help employees remember their account details for different areas of the business. There are many available (free and paid), such as: LastPass, KeePass, Dashlane or 1Password.

Many of these also come with Multi-Factor Authentication to help prevent unauthorised access.

PART 5
ENCRYPTION



We highly recommend encrypting all devices, including mobiles and laptops, immediately with a solution such as Bitdefender Full Disk Encryption. If a device was stolen or left in a public area, any information stored on that device would be at risk of data leakage and could be used maliciously against your business. Perhaps look at using DeliverySlip to encrypt emails on mobile devices.

As long as your employees only have access to what they need, you're in a good place. We recommend encrypting all devices that have access to business critical information, both local or remote, to help prevent data leakage with a solution such as Bitdefender Full Disk Encryption. It's also a good idea to use an Email Encryption tool like DeliverySlip. Features such as 'For Your Eyes Only', 'Forward Freeze', and the ability to successfully acknowledge receipt of the delivery helps protect sensitive data, alongside providing a clear audit trail for compliance purposes.

Unfortunately, your business is still susceptible to external or internal attacks if workstations are left unencrypted, particularly if you work in an open plan office. We recommend encrypting devices as soon as possible with a solution such as Bitdefender Full Disk Encryption.

In this case, we recommend reviewing your security policies regularly. You should ask yourself why you allow the majority of your employees access to business critical information if they don't need it. If you do not encrypt devices, employees could make copies without your knowledge or email it to an external contact, so consider a solution like Bitdefender Full Disk Encryption.

NEED BETTER PROTECTION?
CONTACT US TODAY FOR ADVICE ON SECURITY SOLUTIONS.