BDO

CYBER RISK GOVERNANCE

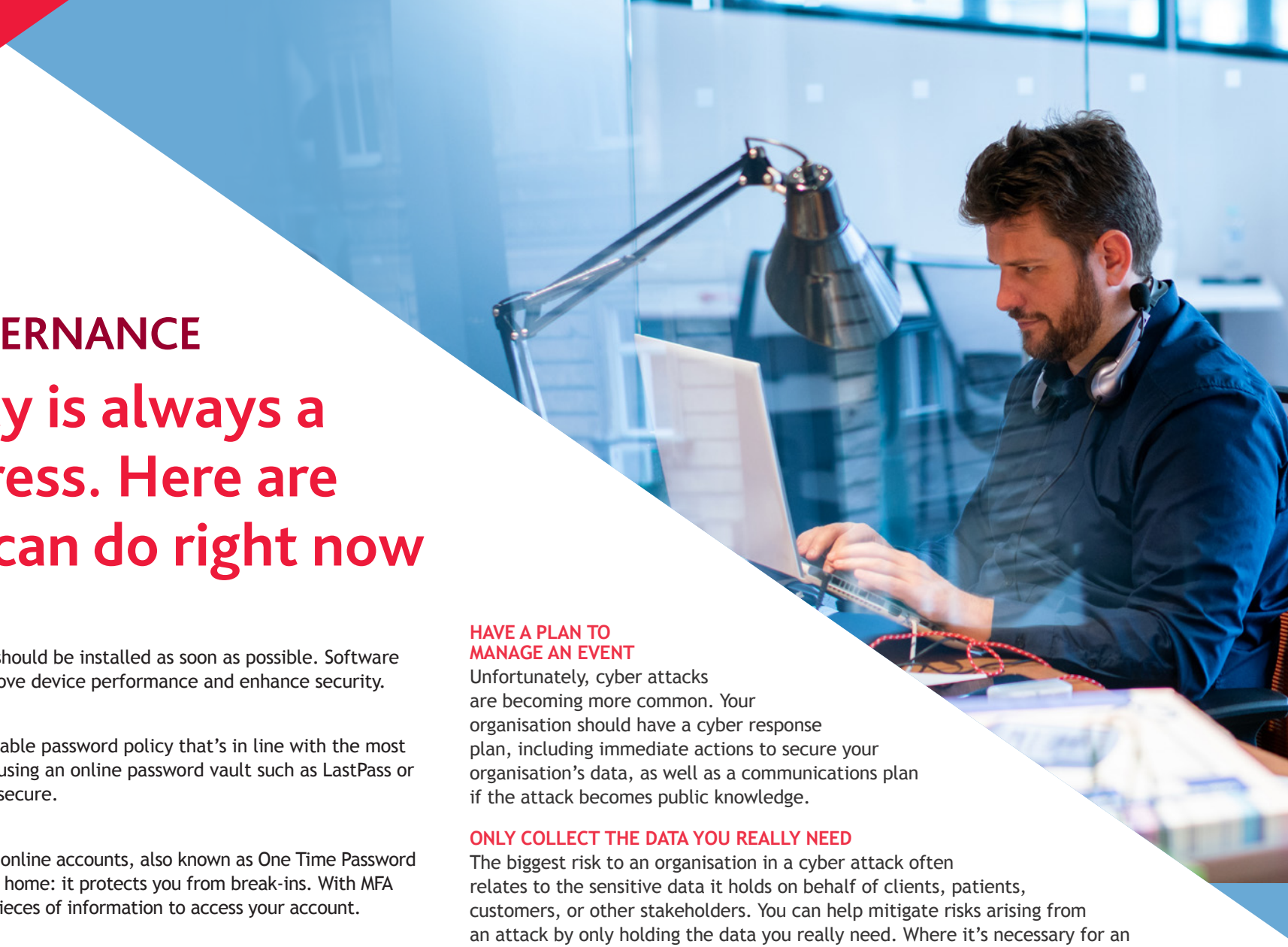
Knowledge is power: Assessing the robustness of your organisation's cyber security

Organisations typically hold a significant amount of data with varying levels of sensitivity. That data is often critical to an organisation's operations, as is the security of that data. Keeping it safe means avoiding the risk of cyber attacks and the repercussions that can result from an attack.

There is no single framework that will apply to all organisations due to their different sizes, nature of operations, and technology structures. However, for individuals responsible for governance, we consider the following questions useful to ask of yourself and your in-house or external IT team to assess the robustness of your organisation's cyber security:

- Does your organisation meet the relevant statutory and regulatory requirements?
- Has your organisation quantified its cyber exposure (including data held by third parties) and tested its financial resilience?
- Does your organisation have a documented improvement plan to keep exposures within your agreed-upon risk appetite?
- Does the board regularly discuss information supplied by management regarding your organisation's cyber resilience?
- Are there incident response plans in place that have been recently rehearsed, including at board level?
- Are the roles of the people responsible for managing cyber risk clearly defined?
- Have you received independent assurance of your organisation's cyber security posture?

BDO



CYBER RISK GOVERNANCE

Cyber security is always a work in progress. Here are 8 things you can do right now

KEEP SOFTWARE UP TO DATE
Operating system and software updates should be installed as soon as possible. Software updates are like a car service: they improve device performance and enhance security.

MANAGE PASSWORDS
Your organisation should have an enforceable password policy that's in line with the most recent best practice guidance. Consider using an online password vault such as LastPass or 1Password to help users keep passwords secure.

MULTI FACTOR AUTHENTICATION
Multi-factor authentication (MFA) on your online accounts, also known as One Time Password (OTP), is what a security screen is to your home: it protects you from break-ins. With MFA activated, you need to provide multiple pieces of information to access your account.

TRAINING
Ensure your organisation runs a cyber security training programme to keep all users regularly trained on common practices used by cyber criminals to steal data. As well as ongoing training for existing users, this should be included in induction training for new users.

BACK UP YOUR DATA
Regular backups and test recoveries help reduce the damage of data loss if your organisation is subject to a cyber attack.

HAVE A PLAN TO MANAGE AN EVENT
Unfortunately, cyber attacks are becoming more common. Your organisation should have a cyber response plan, including immediate actions to secure your organisation's data, as well as a communications plan if the attack becomes public knowledge.

ONLY COLLECT THE DATA YOU REALLY NEED
The biggest risk to an organisation in a cyber attack often relates to the sensitive data it holds on behalf of clients, patients, customers, or other stakeholders. You can help mitigate risks arising from an attack by only holding the data you really need. Where it's necessary for an external party to hold your organisation's or customers' data, ensure you have an appropriate due diligence framework to verify their security levels and controls.

SECURE YOUR DEVICES
Ensure your IT team has guidelines in place for remote working and encourages good habits when users take their devices off-site. This includes avoiding the use of public Wi-Fi networks where possible, locking devices when not in use, and shutting down and securing devices overnight or when they're not needed for extended periods of time.