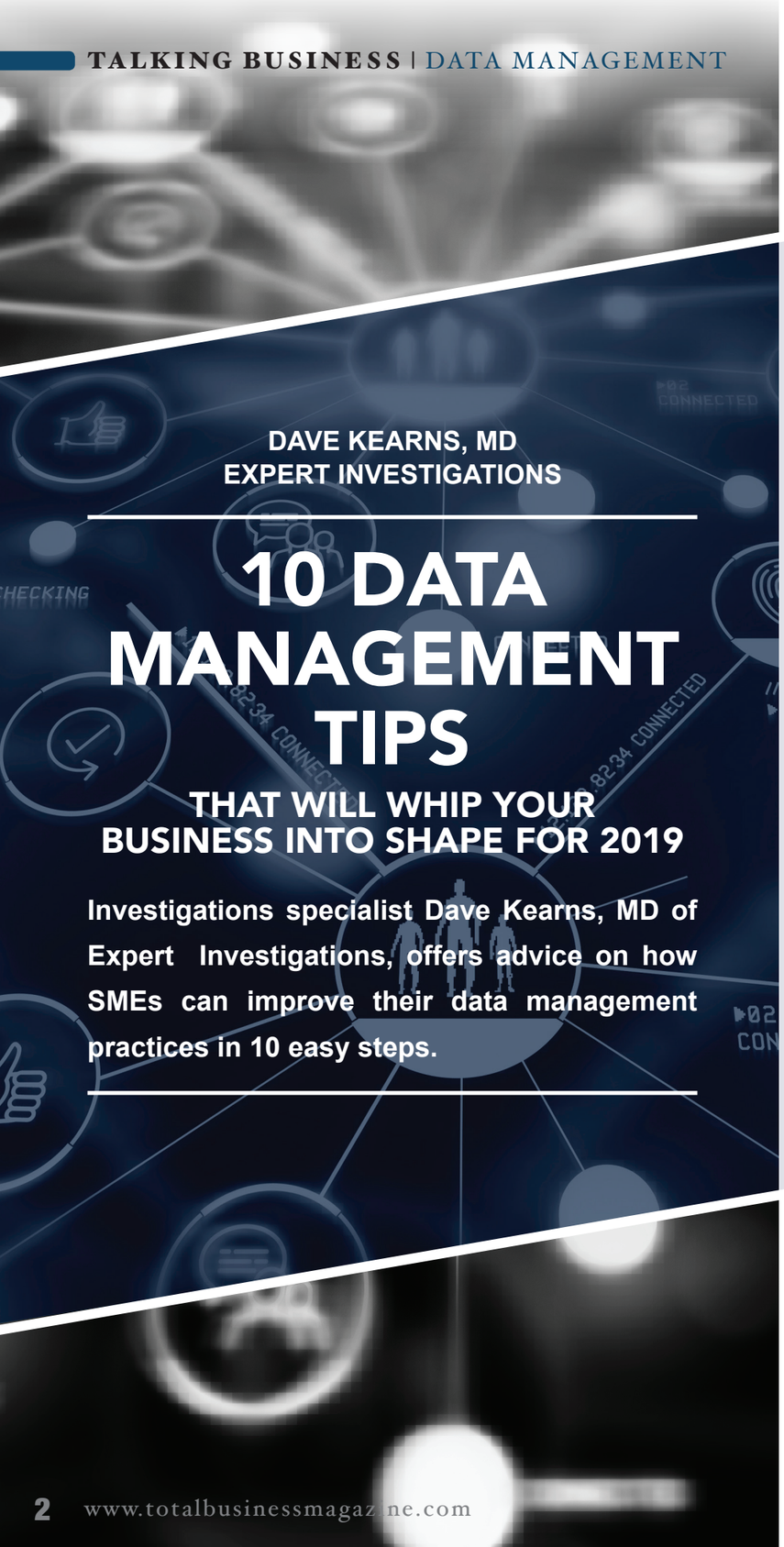

DAVE KEARNS, MD
EXPERT INVESTIGATIONS

10 DATA MANAGEMENT TIPS

THAT WILL WHIP YOUR BUSINESS INTO SHAPE FOR 2019

Investigations specialist Dave Kearns, MD of Expert Investigations, offers advice on how SMEs can improve their data management practices in 10 easy steps.

Bupa Insurance Services recently hit the headlines when an employee stole information relating to 547,000 international health plan customers and offered it for sale on the Dark Web.

The healthcare giant was fined £175,000 by the Information Commissioner's Office (IOC) for "failing to recognise that customers' personal data was at risk and for failing to take reasonable steps to secure it." In short, Bupa didn't have effective security measures in place to protect their customers' personal information.

Similarly, Morrisons is likely to make a huge payout as a consequence of a data leak of the personal information of thousands of members of staff, which was posted online by a disgruntled employee. Although the former auditor was prosecuted and jailed for eight years, in October, the Court of Appeal upheld the High Court Ruling that Morrisons is liable for the malicious actions of is a former employee.

The retailer is now taking its case to the Supreme Court and the judgement is expected to result in an increase of class action cases against companies that have had a data breach of some kind.

However, data security isn't just an issue for larger businesses with dedicated IT and security staff in place to do battle with fraudsters, it's also a considerable risk factor for smaller businesses too.

Recent findings reveal that SMEs are more vulnerable to employee data theft than larger companies as their directors are reluctant to believe that their company could be a target or that their employees may be dishonest. This naivety is a huge business risk as negligent employees remain the number-one cause of data breaches for smaller businesses, according to a recent survey by a US IT consultant.

So here's what you can do to tighten the reins on your firm's data management practices in 10 easy steps:

1. Categorise and understand sensitive data

It's crucial to categorise your data and understand how it can be of value to dishonest employees. You may automatically identify R&D as sensitive, but also consider large customer lists, banking details or even information from medical procedures. A private dental practice will have data that is as sensitive and vulnerable as a housing association holding tenants' personal details.

Once you have identified your sensitive data, consider seeding databases with false clients and suppliers so that any mass mailing would potentially alert you to the misuse of your data.

2. Control and enforce access levels

Only allow employees access to data that they need to carry out their duties. For instance, the marketing team doesn't need access to accounting or operational details and vice versa.

3. Mitigate risk around passwords

Poor password handling is a common mistake within SMEs. Enforce strong passwords and ensure that they are changed regularly. Make sure that when an employee leaves the company that his or her passwords are changed to prevent others from using their access. Many systems come preconfigured with administrator access with default passwords. Make sure that all default passwords are changed and restricted to named individuals.

4. Review activity around sensitive data.

Use covert monitoring software to identify when large amounts of data being downloaded, sensitive files accessed outside working hours and repeated failed password attempts to access confidential data.

However, reviewing activity isn't enough. Use of personal PCs, laptops, mobile phones and USB devices to access or store company data should be prevented where possible. Identify ways of locking out USB devices or logging their activity. Additionally, prevent the use of private web-based email or cloud storage accounts as they can be used to move significant amounts of data quickly, with little traceability.

5. Enforce the security message

Employees may naively consider data theft insignificant and should be alerted to the repercussions of such actions in the following ways: Data security policies should be driven and communicated from the top of the organisation as well as being included in contracts. Employment contracts should also detail the communications policy and enforcement.

Employees need to understand the implications of data misuse and data security breaches as well as the sanctions they may face, such as civil or criminal prosecution and heavy fines.

Also consider creating a digital forensic readiness policy to help investigate breaches.

6. Validate your backups

Now more than ever, with GDPR in effect and external fraudsters ready to attack your data, it's critical that all data is securely backed up and validated. An employee stealing data could have significant financial and PR implications, but if this data is not backed up and lost forever, the implications for your business could be catastrophic. Use a backup system, for instance, that ensures you can only ever lose half a day of new data. Ideally, the backup should be held at a remote location and be encrypted.

7. Check employee movement

When an employee resigns or moves to another department of the business, make sure that there is an action plan in place to prevent damage to or loss of data by that employee. Employees normally submit their resignation once they find a new job. Ask yourself the following questions: Would your data be of value to them in their new role? Are they starting self-employment using your data?

Customer, supplier, accounts and contractor lists all have value. An action plan should be followed to ensure the security of your data and to prevent or disrupt that employee from stealing your data. It may be operationally possible to deny access or to at least monitor that employee's activity more closely.

Consider securing a forensic image of laptops, USB devices and company mobile phones when a user leaves, especially if they are in a senior position.

Repossession of company laptops, USB storage devices and mobile phones should be effected immediately when an employee is being dismissed. Mobile phones should be placed into 'airplane mode' to prevent remote wiping.

8. Conduct exit interviews

Once an employee has tendered their resignation, an exit interview should take place to give you some indication of the risk of data theft. An employee who is moving to a completely different job (proven in writing) where your data will be of no use to them poses less of risk to the business than an employee moving to a competitor.

Be aware that the employee may be misinforming you or even looking to use your stolen data on exiting the business for a single financial transaction with a proposed sale of that data.

9. Crime prevention measures

Support data security with conventional security measures. Whilst you may have systems that prevent access on personal data devices, such as laptops, consider security measures such as CCTV, electronic access controls on server rooms and that records are maintained for a useful length of time (monthly overwrites of CCTV footage or access logs may well lose you vital evidence).

Not only will conventional measures secure vital evidence should a data theft occur, but they will also act as a prevention and disruption tool. If you have external-facing IT systems they should be subjected to penetration testing to identify, quantify, rectify and mitigate any risks to your company infrastructure.

10. Prevent shared access rights

Be extra vigilant with controls to those who have access to all areas. This is usually members of the IT department. They will typically be aware of all the control measures and security systems in place and, therefore, understand how to bypass them, disable them or create a credible alibi. IT technicians should have their own individual login and security credentials and shouldn't have shared access rights to any part of the system. All support requests should be logged by the IT dept and the user.

For more information about the risks that dishonest employees pose to your business, download my free booklet It's Time to Act at www.davekearns.co.uk/the-process