IRON MOUNTAIN®

HEALTHCARE BEST PRACTICE GUIDE

YOU'RE ONLY AS STRONG AS YOUR WEAKEST LINK

How to account for human behaviour in internal risk management

INTRODUCTION

The turbulence of the past few years has compelled organisations to rethink their risk strategies, with a focus on ensuring long-term resilience.

Nowhere is this more evident than in the healthcare sector, where increasingly sophisticated cyberattacks are endangering patients' confidential data. Meanwhile, the vulnerabilities are multiplying as medical records move to digital platforms, telehealth booms, and medical internet of things (IoT) devices become increasingly commonplace. The ability to serve patients remotely and effectively whilst keeping their information security and compliance top of mind has never been more critical.

DID YOU KNOW?

In May 2021, a ransomware attack crippled Ireland's health service's IT systems, leaving most of the country's hospitals **without computers for over a week**[1].

In 2020, a ransomware hit on a hospital in Europe had **severe consequences for patients**[2].

But how do you protect your business in the face of such growing attacks?

One key area that is often overlooked is the threat from within. While mostly unintentional, human behaviour and errors put healthcare providers in jeopardy by risking lives and causing financial losses, not to mention significant reputational damage if there is a loss of sensitive medical information. At a time of such rapid digitisation, healthcare organisations have more to lose than most.

A recent IBM report estimates the average cost of a healthcare data breach at **$9.23 million**[3] per incident – more than any other industry.

That's why Iron Mountain commissioned a pan-EMEA study[4] pinpointing the potential risk management areas organisations should factor in linked to human weaknesses – with some surprising results.

Read on for insights and practical tips on how to manage risk across hybrid teams and build a resilient business strategy.

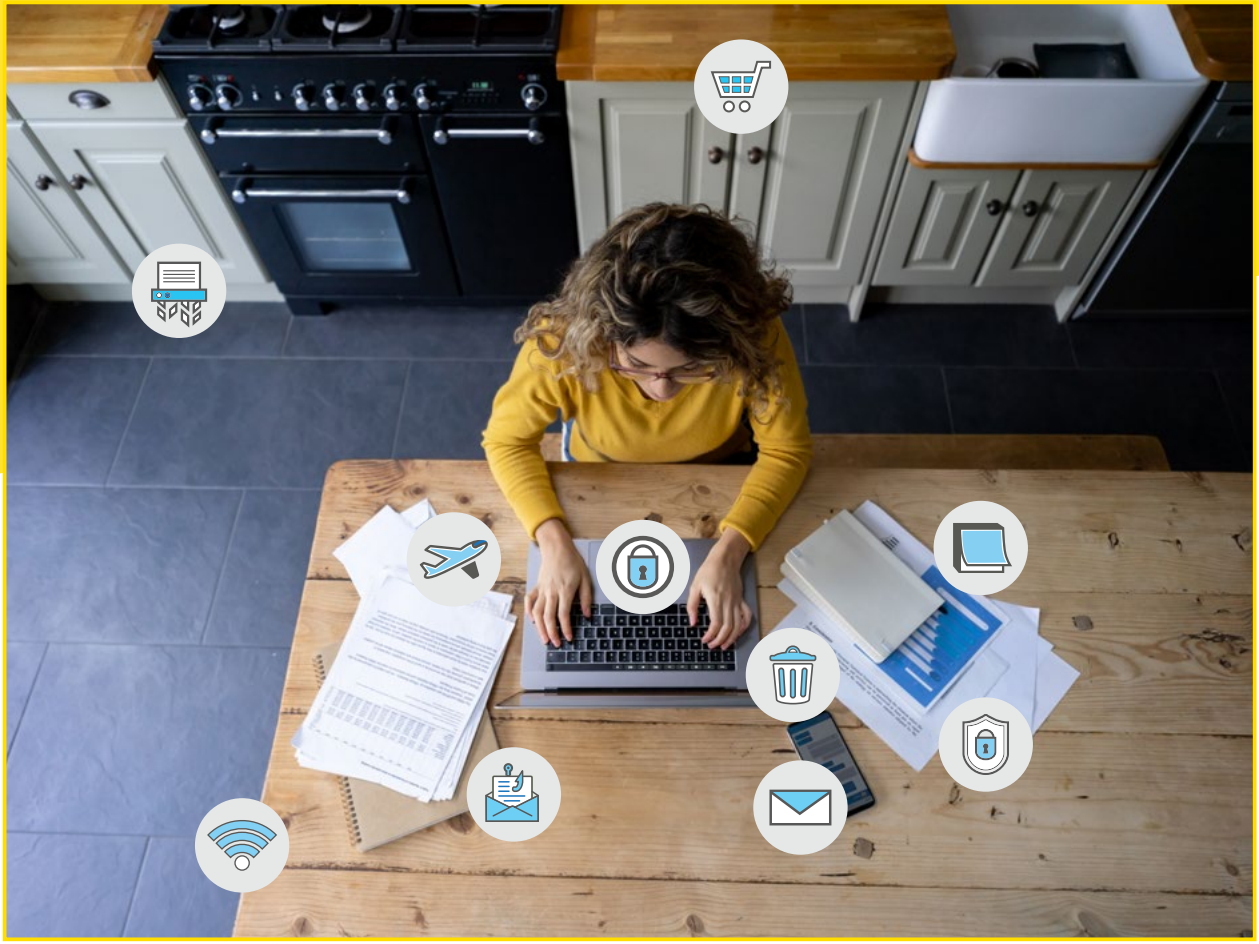
1. New Zealand hospital faces second week of disruption after major cyber attack.
2. 10 days after ransomware attack, Irish health system struggling.
3. IBM Cost of a Data Breach Report, 2021.
4. Survey of 11,000 employees in 10 countries, conducted in September 2021 by One Poll.

CHAPTERS IN THIS GUIDE:

Let's begin with the low hanging fruit.

Here are some of the surprising truths about how we work – at home and at the office.

How many of these are **you** guilty of?



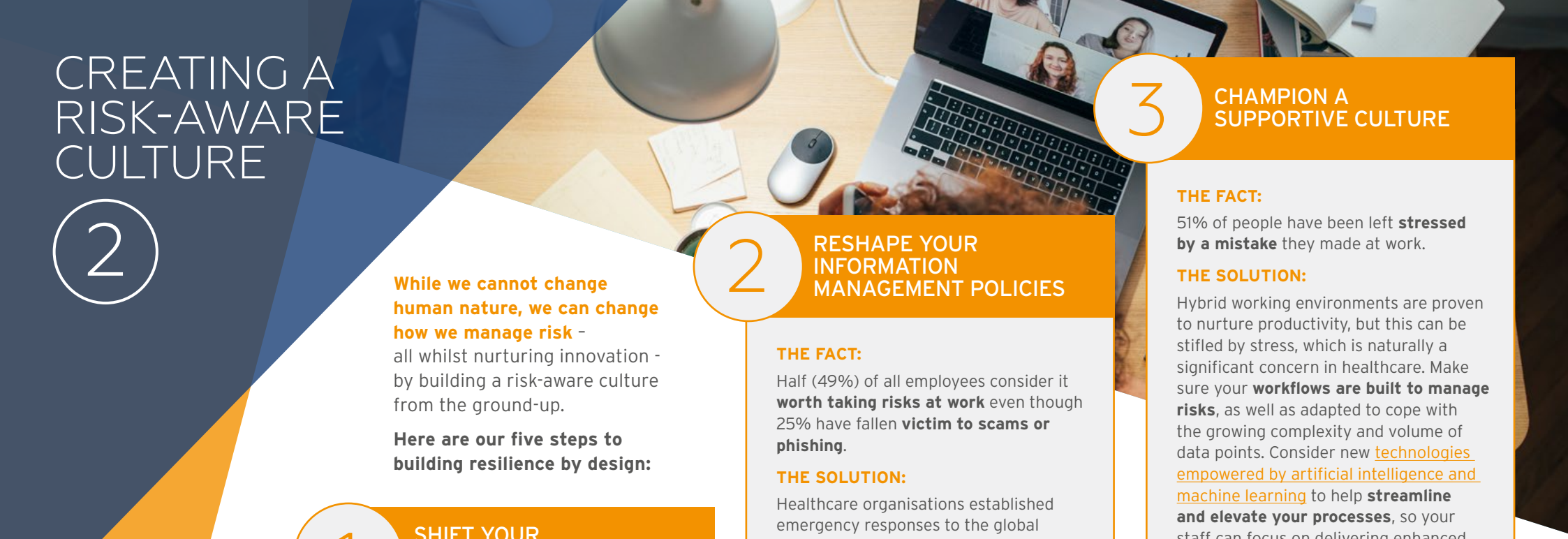
'CLICK' ON THE ICONS TO DISCOVER MORE!

Thankfully, these relatively simple issues are fixable. Consider:

- Sharing these statistics to highlight the issue without 'pointing the finger'
- Flagging the importance of a change in behaviour
- Highlighting the tools, training and support available to help
- Reiterating the difference between a calculated and an unnecessary risk
- Updating policies to ensure maximum understanding of, and accountability for, risk management

CREATING A RISK-AWARE CULTURE

2



While we cannot change human nature, we can change how we manage risk – all whilst nurturing innovation - by building a risk-aware culture from the ground-up.

Here are our five steps to building resilience by design:

1 SHIFT YOUR ORGANISATION'S MINDSET

THE FACT:

One in three employees (32%) claim to **have made a "critical" error at work** and 14% have taken a **risk that cost** their organisation money.

THE SOLUTION:

Begin by empowering every employee to become a risk ambassador, **embedding risk awareness within your culture**. Drill in a mentality that this is a fundamental employee responsibility. It's for the many, not the few.

GO AHEAD AND **TICK OFF THE BOXES** AS YOU GO THROUGH **YOUR STRATEGIC PLANS!**

2 RESHAPE YOUR INFORMATION MANAGEMENT POLICIES

THE FACT:

Half (49%) of all employees consider it **worth taking risks at work** even though 25% have fallen **victim to scams or phishing**.

THE SOLUTION:

Healthcare organisations established emergency responses to the global Covid-19 pandemic, but these have now shifted to long-term strategies built around virtual consultations and hybrid working. Think about **well-articulated information management policies** that apply to office, hybrid and/or remote employees, as well as vendors and contractors.

As healthcare providers hasten to digitise patient records, it is critical to ensure full **chain of custody** throughout all collection, transportation, **digitisation and disposition processes**.

3 CHAMPION A SUPPORTIVE CULTURE

THE FACT:

51% of people have been left **stressed by a mistake** they made at work.

THE SOLUTION:

Hybrid working environments are proven to nurture productivity, but this can be stifled by stress, which is naturally a significant concern in healthcare. Make sure your **workflows are built to manage risks**, as well as adapted to cope with the growing complexity and volume of data points. Consider new technologies empowered by artificial intelligence and machine learning to help **streamline and elevate your processes**, so your staff can focus on delivering enhanced levels of patient care and work through pandemic-induced waiting lists.

What is 'resilience by design'?

Resilience - or your organisation's ability to fend off attacks or other exceptional events – should never be an afterthought. It should be baked into every step of your business policies and processes.

CREATING A RISK-AWARE CULTURE 2

Post-pandemic tech integration

Over half (59%) of the data managers we spoke to **purchased new software** during the pandemic and two-thirds (62%) **implemented sharing tools** such as Microsoft Teams. These require embedding into information lifecycle management programmes, including **establishing retention periods for unstructured data**, such as patient chats and meeting recordings, as well as a centralised compliance and policy management systems adapted to today's more complex technology environment.

4 EVOLVE YOUR PROCESSES

THE FACT:

36% are more **security conscious** with work-related data at the office than at home.

THE SOLUTION:

With virtual consultations and digital hospital records quickly becoming the norm, ever larger volumes of data are being created. This requires you to **rethink information governance**: from access rights management, to digital information sharing, to data retention, and secure destruction, in line with prevailing legal requirements. As a first step, **consider creating a data map** to understand how data flows in and out of your organisation.

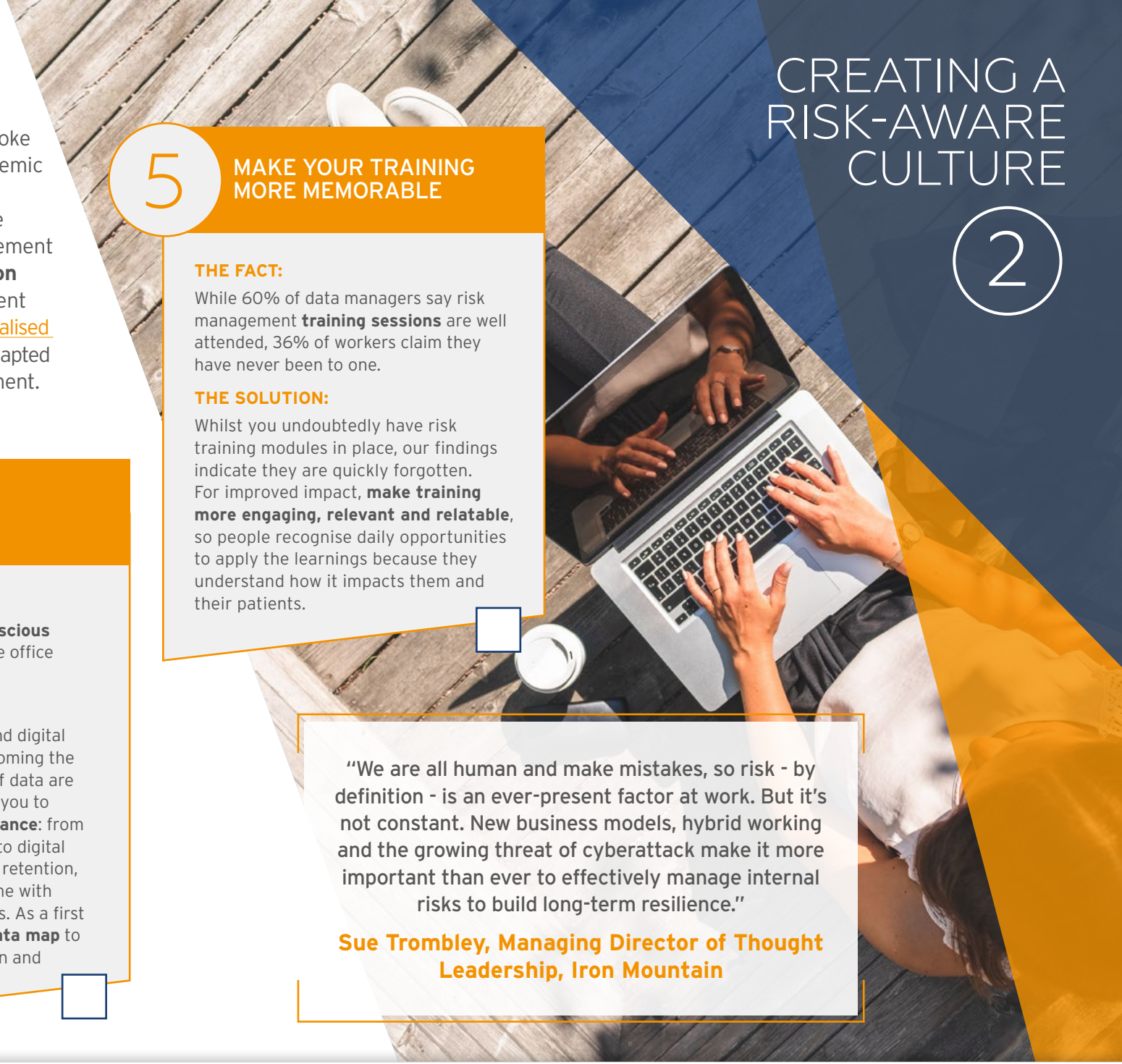
5 MAKE YOUR TRAINING MORE MEMORABLE

THE FACT:

While 60% of data managers say risk management **training sessions** are well attended, 36% of workers claim they have never been to one.

THE SOLUTION:

Whilst you undoubtedly have risk training modules in place, our findings indicate they are quickly forgotten. For improved impact, **make training more engaging, relevant and relatable**, so people recognise daily opportunities to apply the learnings because they understand how it impacts them and their patients.



"We are all human and make mistakes, so risk - by definition - is an ever-present factor at work. But it's not constant. New business models, hybrid working and the growing threat of cyberattack make it more important than ever to effectively manage internal risks to build long-term resilience."

Sue Trombley, Managing Director of Thought Leadership, Iron Mountain

EMBED YOUR STRATEGY WITH 'RESILIENCE BY DESIGN'

3

"An element of risk-taking can enable an organisation to innovate, but lack of awareness about everyday dangers can erode resilience. We advise empowering every employee to become a risk ambassador by embedding risk awareness within your culture. This creates a safe space in which individuals can innovate and organisations thrive."

Sue Trombley, Managing Director of Thought Leadership, Iron Mountain

According to our survey, **70%** of European data managers believe all employees are responsible for risk management.

For lasting impact, resilience should be baked into every step of your business processes, and reinforced by the daily actions of all employees – both clinical and administrative.

As healthcare providers work to rapidly digitise their operations, it is important to appreciate that the heightened threat of cyber-attack is likely to remain as we continue to recover from the ricochet of COVID-19.

This makes **hybrid working solutions embedded with 'resilience by design'** key to the long-term prosperity of any healthcare organisation. Solutions which, for example, allow secure information access from anywhere, streamline workflows for patient information processing, and help effectively manage the entire lifecycle of your data, regardless of its format or type. Solutions that enable you to **protect and improve the accessibility** of your information, while enhancing your clinical decision-making and improving patient care.

For support in addressing your evolving information management challenges and to discuss solutions to help you drive resilience in a hybrid working world, contact the team or visit ironmountain.com/uk/industries/healthcare-services.

ABOUT IRON MOUNTAIN

Iron Mountain Incorporated (NYSE: IRM), founded in 1951, is the global leader for storage and information management services. Trusted by more than 220,000 organisations around the world, and with a real estate network of more than 85 million square feet across more than 1,400 facilities in over 50 countries, Iron Mountain stores and protects billions of information assets, including critical business information, highly sensitive data, and cultural and historical artifacts. Providing solutions that include secure storage, information management, digital transformation, secure destruction, as well as data centres, art storage and logistics, and cloud services, Iron Mountain helps organisations to lower cost and risk, comply with regulations, recover from disaster, and enable a more digital way of working. Visit www.ironmountain.co.uk for more information.

08445 60 70 80 | IRONMOUNTAIN.CO.UK
R.O.I. 1800 732 673 | N.I. 08445 60 70 80 | IRONMOUNTAIN.IE

IRON MOUNTAIN®