IRON MOUNTAIN®

INFORMATION COMPLIANCE

DISCOVER WHY A WELL-TRAINED WORKFORCE COULD BE YOUR BEST LINE OF DEFENCE WHEN IT COMES TO SECURING YOUR ORGANISATION AGAINST INFORMATION BREACHES

THE GREAT DIGITAL MYTH: TECHNOLOGY IS A PANACEA

Believing that technology is the answer to our problems could explain why 59% of businesses react to data loss by investing in technology.* Research echoes what Records and Information Management (RIM) and compliance teams already know: investment in compliance training programs is low compared to IT security systems.

Technology is a vital part of every organisation's cyber-defence and records management, but no system is 100% secure. And human error looms large. 25% of businesses claim that more than 60% of financial losses come from accidental breaches.* When it comes to information compliance, people are your first line of defence.

JOIN THE 1%

A mere 1% of organisations consider information risk to be everyones' responsibility.* An understanding of the influences on employee behaviour is more likely to improve internal compliance protocols and processes than trying to make technology into a magic wand or investing more money in the problem.

The best defence against an information breach may be well-trained people at all levels of your organisation who take responsibility for information security and promote best practices. A variety of training methods such as e-learning, face-to-face or bite-sized sessions will reach more people and clarify information-handling responsibilities and guidelines. The aim is to make more employees alert to risks.

With good training, they will be empowered to take the right actions and know when to ask for support. Information security and awareness training could be an investment that will pay for itself many times over.

COMPLIANCE TRAINING 101

Where the basics are concerned, there's work to be done. If organisations are serious about improving information compliance, comprehensive training programs should be at the heart of their efforts.

For the greatest impact, training programs should include information risk training for all staff – including induction and refresher courses. Senior managers and the C-suite should be part of the training and agree to lead by example. If they are committed to managing information securely, others will follow. A focus on individual responsibility will enable employees to understand their role in relation to the risks (and benefits) of information compliance. Internal communications should target specific employee behaviours, and provide guidance on how to manage data that may be subject to privacy laws.

HAVE YOU GOT THE MEASURE OF COMPLIANCE?

Even when organisations have an information compliance training program in place, measurement can be lacking. Measurement helps you to understand how effective training is, highlights priority areas and lets you make a case for increased support from business leaders. Regulators expect to see evidence of information risk and compliance training. So the more you can prove its effectiveness, the better.

One last word on the 1%: there's a strong argument for building information security-friendly behaviours in daily routines. For example, clear desk policies, secure offsite records storage, communication programs and data sharing beyond IT. These small but simple changes together, can make a big difference.

* Research sourced from PwC's report "Put your risk into perspective".

** Research was undertaken for Iron Mountain by Opinion Matters who surveyed a total of 4,006 workers in mid-market companies.

IRONMOUNTAIN.CO.ZA