WHITE PAPER

ACCESS ALL AREAS

IRON MOUNTAIN®

WHAT INFORMATION DO YOUR EMPLOYEES HAVE AND WHAT ARE THEY DOING WITH IT?

THE BLURRED WORKING ENVIRONMENT

The last decade has seen profound changes in the way people work. Boundaries between work and personal life have blurred. The idea of closing the office door at the end of the day and leaving everything securely locked behind until you return has been consigned to the past. Hot-desking, remote working and video-conferencing have all become part of everyday life for millions of people around the world.

At the same time, the digital revolution has resulted in exponential increases in the quantity of information available to employees. Never has it been easier to copy something and send it to a colleague sitting at the next desk, or halfway across the world. We share, we upload, we download, we invite people to follow us, and we frequently swap between personal and business devices.

Information management struggles not only to keep up with the developments in technology, but in the way it is adopted and used by people. Put bluntly, the architecture organisations deploy in order to protect their information often seems designed for an era that no longer exists.

INADVERTENT SECURITY BREACHES

Whenever the popular media tackles the subject of information security, it tends to focus on the lone hacker breaking into an organisation's server and spilling its secrets across the internet. While attacks such as these can be devastating for the victims involved, considering the amount of information that travels around the world every day, they are relatively uncommon.

The far greater danger comes from people who are authorised to have access to information and through their behaviour, intentionally or unintentionally, create data breaches. Whether it's the confidential personal file left lying on a photocopier, the top secret strategic review inadvertently emailed to an entire address book or a memory stick containing next year's marketing strategy sitting on a desk amongst some loose change and a set of car keys, there are countless daily instances of employees thoughtlessly creating the potential for information breaches.

Most of the time they are lucky and nothing bad happens, but when it does the consequences can be catastrophic for the individuals and organisations concerned.

I NEVER MEANT ANY HARM: AN EXAMPLE FROM EVERYDAY LIFE

Imagine the following conversation towards the end of a typical work day:

Manager: "Have you finished that market analysis presentation you're working on?"

Employee: "Almost there, I'm just going to go over it one more time tonight."

Manager: "Let me see it before it goes out, will you?"

Employee: "Of course."

An exchange like that could happen in any office around the world. At first glance it seems benign; nothing more than a manager keeping an eye on a employee's progress. It's only when you start to scrutinise the chain of information that the risks become apparent.

The starting point in this information journey is the report or presentation generated and compiled by the employee. Drawing upon his or her access to confidential data, the subordinate writes the report and saves it on the company's system. So far so good.

With the deadline looming, the subordinate decides to email a copy to themselves so they can access it on their personal computer and add some final touches at home. Suddenly, a confidential document, which until now had been protected on a secure server, is sitting on a private laptop and an ISP personal email account. From home, the subordinate sends a copy to the manager's private email, cc'ing a couple of colleagues in the process. Later that evening one of those colleagues happens to be in a taxi, when his phone slips out of his trouser pocket down the back of the seat.

These types of information security breaches happen every day. All because a conscientious employee wanted to do their very best on an important piece of work. Everyone involved has the best intentions, no one wants to do anything to hurt the company or its people.

But, if that can happen when people mean no harm, imagine the damage that's possible when they do.

OWNERSHIP AND INTELLECTUAL PROPERTY

One of the problems with ownership and intellectual property is the disjunction between what the law states and what many employees believe to be true. It is surprising how many people assume that if they have been involved in creating a piece of intellectual property, whether it's a presentation, a client database or an analysis of a set of figures, they own that property.

In fact, the law in most European countries states the opposite. If you, as an employee, create a piece of information on company time, on company equipment, using data obtained from that company, ownership of that intellectual property remains with the company, regardless of your intellectual contribution to that piece of work. From a legal perspective, your contribution has been acknowledged and recompensed through the salary paid to you for your time and effort.

What this means is that there are thousands of people out there who think they own intellectual property or have the right to certain information when they don't. This can become a huge problem if they leave their current employer and decide they would like to take "their work" with them. Think of the implications of someone taking a sensitive and highly confidential piece of competitor analysis from their old firm to impress their new boss at a rival organisation.

The answer, clearly, lies in education. If people know a piece of information they have worked closely on does not belong to them and it is therefore not lawful for them to take it with them when they move on, they are less likely to attempt a data security breach, even if they perceive the situation to be counter-intuitive and unjust.

WHEN IT'S TIME FOR SOMEONE TO GO

Most people are familiar with the image of the employee who has just been fired being escorted from the company's premises by security, holding a cardboard box containing a few personal items, locked out of all systems while the termination meeting was still in progress, their security passes invalidated by the time they reach reception.

It sounds dramatic, and to some it may seem excessive, but such a response has been created out of necessity. Whether it is because they feel they will need it in their next role, or an attempt to harm their former employer out of revenge, there is strong evidence to support the notion that employees who leave on bad terms will often attempt to take confidential information with them. Organisations have a duty to themselves and their shareholders to protect themselves against it as best they can.

THE CONSEQUENCES OF JOB-HOPPING FOR INFORMATION AND HR PROFESSIONALS

The idea of a job for life is long gone, and it's well known that employees, especially those in their 20s and 30s, are likely to move frequently between employers as they develop their careers, often changing jobs or companies every two to three years.

Job-hopping presents those charged with responsibility for an organisation's information with two specific problems. The first is to ensure that when employees leave, they do not take any confidential or secure information with them. This has been covered elsewhere, and the appropriate steps to take will depend upon the way and the terms on which the employee is leaving.

The second issue concerns the information the organisation holds on the employee themselves. This will most likely, but not exclusively, include HR files, personal records, performance reviews, possibly confidential medical records, as well as other data accumulated during the employee's time with the organisation.

When the employee leaves the company, HR and Information Managers must ensure that the correct steps are taken in line with current legislative requirements to securely dispose of that information at the correct time. It should not be just left lying around, either on a system or in a paper folder gathering dust in some archive. If you don't already have a policy designed to address this issue with specific steps, dates and action points, you should think seriously about creating one.

How should organisations respond to the access employees have to information?

Obviously, employees need information in order to be effective and do their jobs properly. This need has to be balanced against the organisation's need to protect information that gives it a commercial or competitive advantage, such as intellectual property or market information, or data it is required to keep secure by law, such as customer databases and employee records.

In an ideal situation, everyone should have access to the information they need to perform at their peak level, and the information is secured and disseminated in such a way that it never goes any further than that.

The following are steps organisations can take to move towards this goal:

1. Educate Your People

Most people are careless or sloppy about information because they don't think of the implications of a data breach. They think it will never happen to them. Educate your people about the information they have access to, and their responsibilities to protect it. If people understand why it's a bad idea to copy a confidential document onto a private laptop so they can work on it at home, they are far less likely to do it.

2. Develop Realistic Information Policies

Organisations need to develop realistic policies that protect their information without impeding individuals' ability to do their job. Otherwise employees will just see these policies as an inconvenient imposition by a centralised management that's out of touch with the reality of the modern business world, and find ways to subvert them.

If you don't want field-based employees copying data from a secure server, make sure they have a laptop securely linked to that server. If you're uncomfortable about people using personal mobile phones and emails for company business, you need to provide them with suitably secured business ones.

3. Protect Information Across All Platforms

We put this last because resorting to the technology is the response most people reach for first, thinking an even more secure system will solve any problem, leaving them nothing more to do. As we have discussed, there's far more to it than that. However, it is still essential that organisations protect their information across all the platforms used by their people by ensuring they have systems that are secure and up to date.

THE NEXT STEP

Reaching a place where employees have an instinctive awareness of information security and respect for the data to which they have access takes time, not to mention a commitment from the very top levels of management.

Many organisations turn to a trusted partner to assist them in the process. At Iron Mountain we protect, manage and store documents for over 230,000 customers worldwide, from FTSE 100 companies to smaller specialist businesses.

If you'd like to discuss how we could help you, we'd be happy to hear from you. Call us on +35777778666 or visit www.ironmountain.com.cy

SHARE THIS GUIDE:

ABOUT IRON MOUNTAIN

Iron Mountain Incorporated (NYSE: IRM) provides information management services that help organisations lower the costs, risks, and inefficiencies of managing their physical and digital data. Founded in 1951, Iron Mountain manages billions of information assets, including backup and archival data, electronic records, document imaging, business records, secure shredding, and more, for organisations around the world. Visit the company website at www.ironmountain.com.cy for more information.