FIGHTING BACK AGAINST FRAUD

Julian Crook *examines the importance of tackling document fraud through effective information management*

As organisations become increasingly inundated with massive volumes of business-critical information, decision makers are under growing pressure to find and implement solutions to ensure they effectively manage and control this information.

One of the most important considerations for any business is how to secure and protect sensitive information. The exposure of confidential information to unauthorised individuals can be expensive and time consuming, and places companies at significant risk. Defining and enforcing policies and processes for who is authorised to access, edit and approve specific documents is of paramount importance for companies of all sizes and in all industries.

Maintaining control of corporate information is a challenge for many, which owes much to the habits of people in the workplace. Lax security practices are often embedded into company culture opening the door to fraudulent activity. Alongside this, many companies have not yet implemented an information management system that ensures documents are only accessible to authorised individuals. However, by focusing on managing, archiving and storing documents in a way that ensures the most sensitive information is only accessible to the right people, these challenges are by no means insurmountable.

EMBRACING AN ECM SOLUTION THAT BALANCES SECURITY WITH EASE OF USE IS VITALLY IMPORTANT

The benefits of the cloud are many and well documented, and cloud-based services offer businesses a tangible opportunity to improve the way that they operate. Organisations using cloud applications routinely report achieving significant cost savings over their on-premises alternatives and enjoy greater levels of flexibility, agility and efficiency. But as anyone familiar with the cloud knows, it brings some challenges that must be managed.

An increasing number of employees are using consumer file-sharing solutions to collaborate with business partners, contractors, temporary staff and contacts in other companies. However, employee use of these solutions is often unregulated, uncontrolled and lacks the necessary security controls, workflow management and robust information management functionality that many businesses require.

Unauthorised employee use of file-sharing solutions represents a serious security and non-compliance risk because employees can store and share documents with third parties completely outside of an organisation's control. This can undermine an organisation's responsibility to protect its information assets and, in extreme cases, put it on the wrong side of regulators and other key stakeholders. When it comes to preventing document fraud, this needs to be managed carefully.

AVOIDING DOCUMENT FRAUD

The behaviour of employees themselves, and a lack of commitment by leadership to enforce a comprehensive security policy, can expose an organisation to document fraud.

Poor security practices are often embedded into a company's culture. Such behaviours include, but are not limited to: staff saving sensitive documents onto the hard drives of personal computers, sending documents to personal email addresses, accessing work resources on their own devices through insecure Wi-Fi connections, or making use of third-party sync-and-share applications, which may be prohibited in the organisation's IT security policy.

Such behaviours are commonplace: according to a survey commissioned by M-Files, 59 percent of IT decision makers polled said that their employees use personal devices and/or file-sharing apps to access and share company information. While convenient for employees, working in such a way means sensitive documents are being taken beyond the security perimeter of the company, into applications and environments that could be vulnerable to compromise by fraudsters.

It is not just employees that are responsible for this. Despite the fact that many organisations have a formal information security policy in place, these are worth very little if they are not enforced and if staff are not adequately trained and instructed in how best to follow a policy. Without this, and without any suitable alternatives to third-party file-sharing applications, employees are left with little other option but to take matters into their own hands.

How can organisations make the case for their employees to adopt a formal information management system for managing and sharing documents and files instead of continuing to use unsanctioned file sharing and sync solutions? Management and IT teams must show a top-down commitment to the company-wide use of a single, unified solution for managing business information, and make sure that employees understand the security and productivity benefits it provides to the business.

Closely linked to the practice of employees taking IT matters into their own hands is Shadow IT, and the problems it can create in terms of leaving an organisation open to document fraud and data breaches. In short, Shadow IT is the use of IT systems and solutions to access company information without explicit approval from IT leaders. A key example of this is when employees use cloud services, such as their personal file sync-and-share applications, without the approval – or knowledge – of their IT department.

The same survey by M-Files revealed that 22 percent of IT decision makers did not know if their employees were using cloud services without their knowledge or approval. This underlines the inherent dangers of Shadow IT: by allowing this to happen, a significant amount of employee activity is being conducted outside the control of the IT department. In the event of a data breach, this makes its impact much more difficult to mitigate.

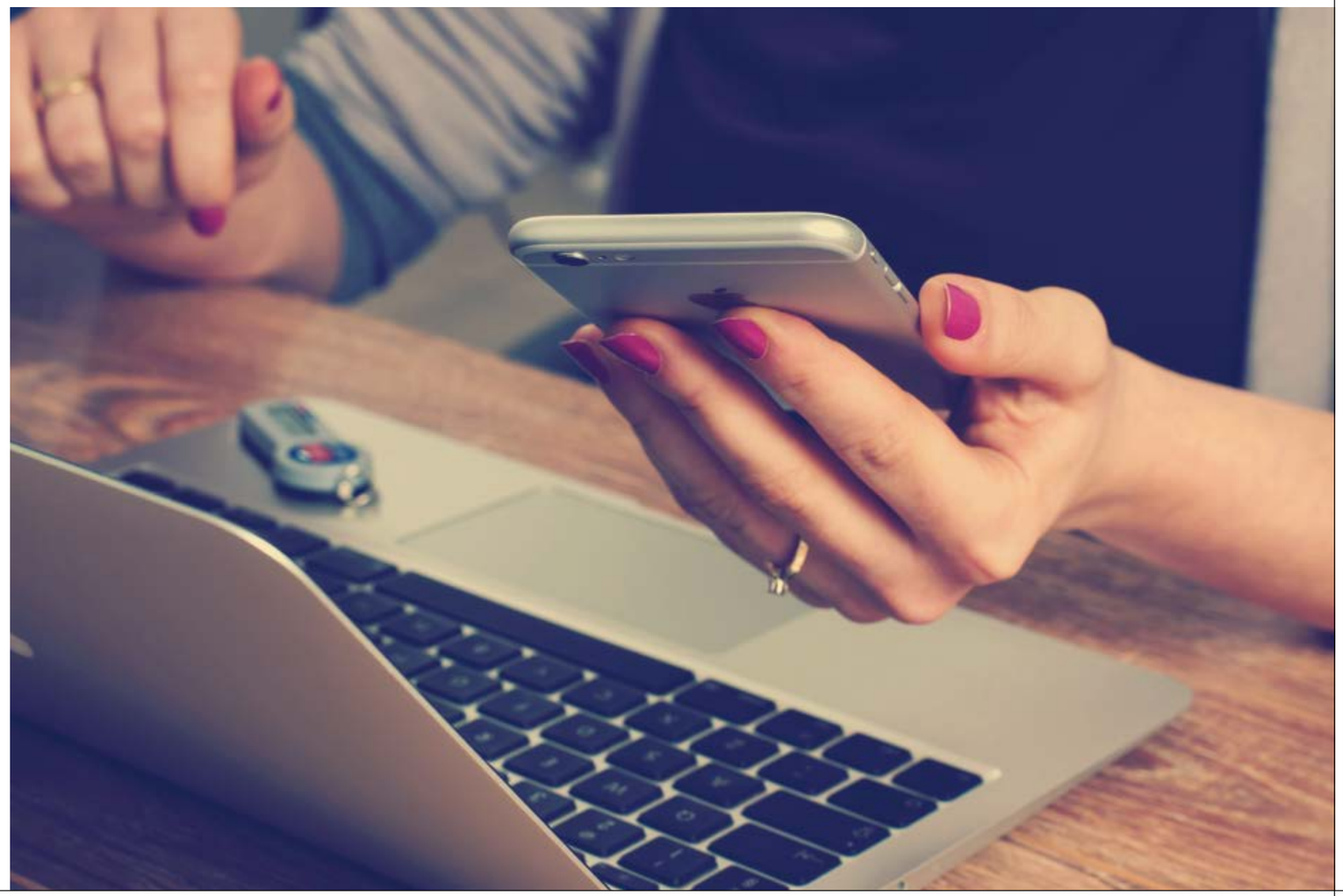
Steps should be taken to implement technology that makes finding and sharing information faster and easier

TACKLING DOCUMENT FRAUD

Although document fraud is a clear concern for organisations, there are ways it can be combated. The first of these is to work towards engendering a culture change in the way employees handle data. This is no easy task, and requires a co-ordinated approach by business and IT leaders to discourage the irresponsible sharing and use of documents.

In the case of those that use file-sharing apps in their everyday work, it is difficult to restrict employee access to technologies that may make their jobs easier. However, better education on the dangers of unsanctioned file sharing will make employees more aware of the potential consequences of their actions, and will help them better detect if fraud has occurred.

This educational approach will also be effective in eradicating other ingrained behaviours, including the saving of sensitive documents onto hard drives of personal computers, documents being sent to



Picture credit: Getty

personal email addresses and employees accessing work resources through insecure Wi-Fi connections.

For such an approach to work, simply introducing a new security policy and telling a workforce to obey it will not suffice. Equally, steps should be taken to implement technology that makes finding and sharing information faster and easier. When companies equip their workforce with easy to use solutions for finding, sharing and managing information, employees will no longer need to rely on their personal solutions to do so.

Finally, businesses worried about the possibility of document fraud should take some time to look at their current approach to information management.

USING THE CLOUD INVOLVES A SERIES OF CHALLENGES THAT MUST BE MANAGED PROPERLY

For companies that have an enterprise content management (ECM) system in place, many legacy systems are often no longer able to adequately cope with the volume and diversity of sensitive documents that a company possesses. This can have security implications, both in the sense that assigning the correct document permissions can be more difficult due to the complicated nature of permissions models, and equally how complex, non-intuitive ECM systems are often shunned by employees in favour of unauthorised third-party applications.

Furthermore, many organisations still rely on an antiquated file folder-based approach for storing and managing electronic documents. This poses several challenges and issues since there are many times when a document can logically be stored in more than one folder, increasing the risk of potential document fraud.

With a modern ECM solution, businesses can equip themselves with technology that is optimised to deal with ever-increasing types and volumes of sensitive content. An ECM solution that uses metadata holds a unique advantage here in that it enables data to be managed intuitively, based on what it is rather than where it is stored. This allows for efficient and effective labelling, storing and archiving of the most sensitive data, thereby significantly reducing the risk of document fraud. Most crucially, metadata can be leveraged to assign the correct viewing and editing permissions, meaning that access to sensitive information is restricted purely to those that are supposed to see it.

Reducing the risk of document fraud requires a unified approach, with a vision that is embraced by both the IT department and employees. A key part of the battle lies in encouraging workers to ensure they conduct their document handling activities in a more secure manner, which can be achieved through regular training and education on the dangers attached to the use of unsanctioned third-party applications and services. If this level of awareness can be reached, businesses are off to a good start.

To stand the best possible chance of winning the war, organisations need to fight fire with fire from a technology perspective. Convenience is a key part of creating an efficient, productive workplace, so the technology available should reflect this. Embracing an ECM solution that balances security with ease of use should be a crucial consideration for any company looking to tackle the issue of document fraud ●

Julian Crook is Vice President of UK Business at M-Files responsible for sales, marketing and services in the UK. Julian has more than 20 years' experience in the IT industry, working in a variety of senior business development, marketing, product management and consulting roles for blue-chip and early-stage technology companies.

Convenience is a key part of creating an efficient and highly productive workplace