The power of three

Martin Birch, ibml's chief executive officer explains why security is the 'must sort' job for companies and their BPO service providers, with ibml giving security the highest possible priority when developing its capture solutions

In the world of document management outsourcing three parties are involved: the customer, the BPO providing services and the capture solutions provider. This three-way relationship is arguably at an inflection point with the security of information assets now the hottest organisational imperative to grapple with.

Research by AIIM shows that for 60% of the largest organisations the potential impact of a data leak is 'high', with 13% of respondents ranking it as 'disastrous'. With the average cost of each one running into millions - $7.2 million in the USA according to research by the Ponemon Institute - it's a wakeup call to many organisations.

You don't have to look far to see examples of this in the UK. In January 2018, the Information Commissioners Office fined Dixons Carphone £400,000 after one of its computer systems was compromised and unauthorised access gained to the personal data of over 3 million customers and 1,000 employees.

The NHS has a torrid history of data breaches too with the WannaCry ransomware attack one of the most serious. This infected 40 NHS trusts in England and Scotland and caused carnage as computers were 'locked down' by the hackers resulting in outpatient appointments being cancelled and A&E departments asking non-urgent cases to stay away.

GDPR, as everybody knows, has upped the stakes of responsibility and, should firms breach data protection rules, fines are severe at up to 20 million euros or 4% of global revenue whichever is greater. Clearly the regulations have real teeth and crucially enterprises can't pass the buck if they outsource - they are responsible for data breaches, not their BPO partner.

Yet, while the external hacker events get the press column inches, a lot of data breaches are internal and come from staff opening, seeing or downloading data they shouldn't. Organisations are making a mistake by neglecting basic security protocols. Of course, they need to protect themselves from external threats but they mustn't forget about unauthorised internal access. It doesn't matter whether someone is on your network illegitimately, or they're supposed to be there in the first place because they are an employee, it's the same problem - data can get out.

The impact of this is compounded by the fact that, on average, 250 days pass from the time a data breach incident occurs to the moment it's found - that's a whopping nine months.

The reality is that information security

- certainly in the context of an outsourced document management relationship - is not being taken seriously enough, data is still not being protected properly with end-users now opening themselves up to a hornets' nest of issues because of the regulation changes.

BPOS NEED TO GET SECURITY SMART

Until recently most BPOs were primarily focused on document volume throughput, price and meeting service level agreements (SLAs). That's completely understandable as competition is rife and margins super tight given profits are pennies on the page. Information security within BPOs often hasn't been top of mind creating a whole raft of security vulnerabilities:

- **Prying eyes and poor visibility of operator activities.** In most scanning environments, operators have network or file system rights to where images are written, opening the door for them to read sensitive information outside the scanning application. In addition, fragmented and often antiquated document imaging systems makes it difficult to track their activities.

- **Sensitive information contained in log files.** The humble log file is a standard feature on almost every OS, application, and server platform. But amazingly, most people don't realise what their application log files actually save, which can result in protected data - like a MICR line from a bank cheque - being kept in an unencrypted text file in an unmonitored location. This makes a nonsense of any security provisions in place and could lead to companies being hacked.
- **Images written a local hard drive.** Most scan clients write images to a local hard drive prior to sending the data to a network file repository with the (local) files then deleted. The issue is that these deleted images are pretty easy to retrieve using standard recovery tools, with all the obvious security implications.

- **Unencrypted data and no encryption while data is in motion.** Although mandatory under Payment Card Industry rules where there is personal or credit card information involved, many firms have yet to make the leap to full disc encryption. This is certainly true with document management systems which have lagged behind due to the impact on performance. And few systems encrypt information while it travels between the scanning, post scan indexing, validation and quality control stages making it vulnerable to data thieves.

The point is that people aren't thinking enough about security when it comes to scanning and, when they do, it's viewed - a bit like buying insurance - as an additional cost of doing business rather than for the real and obvious benefits it offers.

When you're talking about security and trying to defend yourself, hackers only have to be right once whereas the security systems have to be right all of the time. Firms have spent time first securing their online payment systems or back end CRM databases. They must now consider front-end processes too which have a lot of human touch points and therefore security breach possibilities.

Data security has to cover from the moment that paper arrives in a BPO's facilities to the time images are deleted. It's a cradle to grave challenge. Security has to include every process, every document transformation, every time data goes from one system to another and everyone who touches the document in the chain. You have to think about how data is protected irrespective of where it is in the pipeline. And this should include any offshore partner a BPO might use as part of it service delivery solution.

CUSTOMER SECURITY STRATEGIES MUST INCLUDE THEIR BPO

But it is not just down to the BPO. Many companies haven't got their security and compliance personnel engaged and thinking about risk management at the digitisation stage. They ought to.

They need to avoid security being just seen as a 'check box' activity where you go through the motions. They can't assume or hope that the BPO is doing a good job from a data security perspective. Hope isn't a strategy. You have to know it is being done properly.

Enterprises need to work out a security vision which covers the whole paper digitising process from arrival to deletion which protects the whole enterprise end to end and includes document outsourcing.

Firms need to be proactive and spell this out in their contractual agreements with their BPO partners just as if they were managing their data internally. Why? Because the same data protection obligations and fines apply. This needs to cover everything: physical security, staff training, enforcement, along with disaster recovery and business continuity planning. Firms need to monitor this carefully to ensure delivery.

And ultimately, clients need to be willing to pay. Security systems, software and expertise don't come for free and, to date, it has been hard for BPOs to charge for this. This is set to change with the impact of GDPR: the business risk of not securing data is now so great that to pay a bit more for peace of mind is a commercial 'no brainer'.

CAPTURE SOLUTIONS ARE CENTRAL TO SECURITY

This leads us on to the capture solution provider, who also has a crucial role in the whole protection puzzle. Remembering that data security is all about trying to make it more difficult for data to accidentally get out or for

"DATA SECURITY HAS TO COVER FROM THE MOMENT THAT PAPER ARRIVES IN A BPO'S FACILITIES TO THE TIME IMAGES ARE DELETED. IT'S A CRADLE TO GRAVE CHALLENGE. SECURITY HAS TO INCLUDE EVERY PROCESS, EVERY DOCUMENT TRANSFORMATION, EVERY TIME DATA GOES FROM ONE SYSTEM TO ANOTHER AND EVERYONE WHO TOUCHES THE DOCUMENT IN THE CHAIN. YOU HAVE TO THINK ABOUT HOW DATA IS PROTECTED IRRESPECTIVE OF WHERE IT IS IN THE PIPELINE. AND THIS SHOULD INCLUDE ANY OFFSHORE PARTNER A BPO MIGHT USE AS PART OF IT SERVICE DELIVERY SOLUTION."

someone to get to it, security needs to be invisible to scanner operators otherwise - if it places an extra burden upon them - they'll find a workaround because it's quicker and easier. That's just human nature. And one has to also solve the issue of how to keep the people who are supposed to have legitimate access to the data from misusing or misappropriating that data.

This means choosing an advanced capture solution which has built-in processes and safe guards to do this, such as:

- **No image or metadata written locally.** Scanner endpoints are an obvious weakness so you don't want data to be stored on the host scanner PC. Advanced systems don't do this - only temporary images are stored before being written to the network.

- **Least privilege by design.** Ideally, network users should not have access to files and metadata outside of the application and applications should utilise a service account or some other form of impersonation so that the local user does not need access to data stored on back end servers. This limits their access.

- **Comprehensive data encryption.** Support for full disc encryption, metadata encryption, IPSec to ensure data in motion is protected along with native image encryption which prevents anyone downloading information to a portable USB drive as data is only readable using the capture application.

- **Sanitised log files.** Advance capture systems sanitise log files so no sensitive information is ever contained.

- **Fail secure audit logging.** This tracks every activity within the document capture solution, including any data creation, deletion, change or access. And if the system can't audit you, you won't be able to access it either. These log files are obviously critical for regulatory compliance. In conjunction with least privilege by design, comprehensive data encryption, and sanitised log files, this ensures that sensitive data can only be accessed through the capture platform and only if audit logging is available ensuring that the audit log is comprehensive.

In addition, any quality capture solution should be audited by a qualified third party provider, such as Veracode, to assess and identify possible software vulnerabilities so that flaws are dealt with quickly. Making public these scores should give peace of mind to any BPO or customer using their services that the solution they are purchasing or using is best in class and - of course - secure.

Ultimately, therefore, the end-user customer, BPO and capture solution provider must all play an equal role in facing up to information security challenge. You can't delegate security. The three parties have to be actively involved, everyone aligned, clear on requirements and working together to minimise risks, ensure data security systems are installed, working and checked so that compliance rules are met. It's really the only way information management security will ever work.

More info: www.ibml.com