November 2016

Briefing

SMARTER LEGAL BUSINESS MANAGEMENT

Sweeten your offer

Legal business on a fresh, more fruitful formula for employee engagement and brand loyalty

INDUSTRY INTERVIEW

Sharing in safety

Geoff Hornsby, general manager of iManage EMEA, offers his independent view of legal's likely IT security needs in 2017

This year has been a rollercoaster of a year for business risk managers – and 2017 needs to be a year of action on the IT front to match. It's time to stop merely talking about the challenges of matching a need for greater mobility with appropriate security, and start deciding specifically what to do about it.

That's the world according to Geoff Hornsby, general manager, EMEA, at iManage.

"Ransomware is increasingly impacting people's day-to-day lives, and it can also do serious damage to their businesses," he says. "So smart firms across sectors are starting to move from storing data on their own systems to placing trust in a document management system to provide them with the right level of protection."

Suspicious signs

Moreover, business hacks have made headlines several times in 2016 – and with the Panama

For more information, visit: www.imanage.com

"If you've bought a cloud document management system that people find too difficult to use, they're probably still storing files in other places."

Papers breach, legal has had a big incident of its very own. Businesses can now easily picture their dealings or customer data dragged through the pages of the press. But ironically, says Hornsby, firms should really assume they are being targeted – and that there is an increasing risk that they could be breached in 2017. With attacks on law firms increasing, it's probably a case of when, not if. The smart money is on systems that can monitor suspicious activity to secure files once a breach has actually taken place.

"If a hacker is successful in phishing a lawyer, compromising their password, that hacker can then see every bit of data. It doesn't matter if they are using bring your own key (BYOK), or have the highest possible levels of security. All they need is the user log-on. So what firms actually need is a system to help them limit the danger with knowledge of precisely which pieces of data have been looked at, when, and by whom."

Adding pressure, the EU General Data Protection Regulation (GDPR) – which firms are likely to comply with regardless of Brexit's path – will now demand businesses notify their clients of a breach within 72 hours. "It's crucial that even the slightest unusual activity is recognised in real time, and can quickly be flagged to the managing party," says Hornsby.

It's a bit like being alerted to suspicious activity on your credit card. "A system should, for example, identify that you've never actually worked during a weekend before, never dialled in from Estonia before, or never looked in that practice area for a document before. Within a short time, we can say 'that's weird, close it down'.

"It's not just a rules-based system. It's about taking a 'fingerprint' of each user, with individual alerts based on that person."

So yes, legal technology now needs to be GDPR-ready – and it may also need to go quite a bit further. Hornsby says more collaborative working processes – both internally and with clients – means 2017's firms must invest in more than secure storage.

"Firms need work product management," he says. "There's the document management, the secure sharing with clients, compliance with GDPR, and finally the safe destruction of data."

Putting people first

Another hard fact to swallow is that when that hack does succeed, it'll probably be because of one of your own employees.

"You can put high walls around your data centres. You can put barbed wire and armed guards around your cloud implementations. You can have BYOK and all the cloud security certificates in the world – and we've got them – but if someone steals your password and the hacker has entry to the data, the weak link is the human being," Hornsby says.

One of the biggest wins, therefore, is persuading people to use systems in line with your risk management requirements – to follow policies and question suspicious activity for themselves. The next step is to implement a system that watches the activity of users, and spots the examples of unusual behaviour.

"Having a DMS obviously helps in reducing the threat – but if you've bought a cloud document management system that people find too difficult to use, they're probably still storing files in other places," says Hornsby. "Then it's easy for hackers to find and corrupt data, or hold it to ransom.

"Our recent project, White Rabbit, was to listen to our community and make the iManage product work the way that lawyers themselves work, including on the move. Many of its features are about making it easy to use, and so reducing the need for training.

"What's important isn't that your file is saved in the cloud – everyone is in the cloud. What's important is whether the user interface encourages people to use that system – and whether the organisation has the focus to drive it forward to the next generation."

PHOTOCREDIT: JONATHAN GOLDBERG