INDUSTRY INTERVIEW

Late to the third party?

As the General Data Protection Regulation finally arrives – and means business – firms can no longer put off addressing their responsibility to fully understand exposure to third-party risk, says Sean O'Brien, managing director of DVV Solutions

By the time you read this sentence, the European Union's General Data Protection Regulation (GDPR) will finally have been actioned and be in full effect. Law firms, like everyone else, are now required to demonstrate effective processes in their handling of personally identifiable information (PII) data, or themselves risk both the highly publicised new financial penalties and (harder to measure) potential long-term brand damage.

Sean O'Brien, managing director of DVV Solutions, says one key area of due diligence at most risk of underinvestment is the requirement to thoroughly risk-assess your full data supply chain.

"As businesses outsource an ever-increasing number of functions and services – albeit for justifiable commercial efficiencies – their level of exposure to cybersecurity risk significantly increases while their control of it diminishes."

"Businesses show a tendency to prioritise the risk of penetration into the organisation through more direct means of attack, focusing expenditure on securing devices and internal networks," he explains. "While third-party risk is often recognised, the time and resources applied to it are disproportionately low."

This is backed up by research. For example, Bomgar's 2018 Privileged access threat report finds that two-thirds (66%) of businesses claim they could have experienced a breach due to third-party access in the last 12 months. And although three-quarters (75%) of businesses have seen supplier access to their networks increase, a third (33%) believe they spend too little time on monitoring third-party access.

"The problem is immaturity of process," says O'Brien. Businesses just aren't approaching risk in the right way. Ask yourself: What percentage of our data processing do we perform ourselves, and how much is outsourced? Then, critically: Is our spend on understanding and mitigating risks to our data and systems from third parties proportional?"

PHOTO CREDIT: SIMON BRANDON

Six steps to third-party GDPR compliance

- Identify all your third parties, subcontracted data processors and their data/system access
- Centralise your third parties into a single inventory
- Perform detailed GDPR assessments and collect relevant artefacts, for example via questionnaire
- Verify and validate third-party information, typically via onsite assessments for critical suppliers
- Act on GDPR risks, ensuring a clear audit trail of requests, actions and outcomes
- Continuously monitor third parties and report on changing risk profiles.

Mind the procurement gap

In legal there may also be a structural issue. "We often come across larger firms with decentralised procurement processes. We even see no procurement process whatsoever – with partners purchasing IT services with little or no due diligence," says O'Brien. "It is all too common to find firms don't even know who all their suppliers are, the services they provide and the access they have. This all makes it impossible to get a firm grasp of risk and the regulatory compliance of the data supply chain, but regulations such as GDPR have raised the stakes," he says.

While standards and frameworks such as ISO 27001 exist, they are not designed to specifically address third-party risk. However, some larger firms are now beginning to follow the rather better example from the banking world, he says.

Financial institutions have collaborated with membership organisation Shared Assessments to develop global standards in third-party risk assurance, including standardised information gathering (SIG) questionnaires and standardised control assessment (SCA) criteria.

As a member of Shared Assessments, DVV Solutions is able to realise its value. "With standardisation comes efficiency. Our clients can benefit from a globally recognised, third-party risk toolset built by their peers," says O'Brien.

One step ahead of uncertainty

Still, if you haven't done so already, where to begin?

"When outsourcing a process involving PII you need to evidence responsibility for how that data will now be managed in a contractual form," he says. There are also key understandings to be reached in said contract, such as jurisdiction of data storage, access rights, and any further sub-contracting. "You may find you have fourth or even fifth parties to consider, with liability reaching right down the chain," says O'Brien.

For more information, visit:
www.dvvs.co.uk

DVV Solutions offers risk assessments of the controls third parties have in place, recommending remedial actions where required. But O'Brien warns: "Risk never sleeps. Periodic assessments provide a clear attestation from suppliers, but just reflect points in time. What happens in between? And how do you monitor data processors you have no contractual right to audit? Continuous monitoring is now becoming a critical element of third-party risk programmes, providing visibility of the threats and risks posed by all downstream suppliers." DVV Solutions' Supplier Threat Monitor platform provides a constant, validated stream of risk information for the entire supply chain across five risk domains – data, operational, financial, brand and regulatory.

Complete once, share many

If you're thinking that all sounds like a lot of work – O'Brien agrees. That's where 'shared evidence networks' come in – systems designed to avoid needlessly repeating good due diligence and managing the spiralling risk pool more efficiently.

Tailored to the legal market specifically, DVV Solutions has launched the Legal Vendor Network (LVN) where members can both view existing supplier risk assessments and populate their own repository. "Many industries, including legal, have a common pool of third parties and suppliers, meaning we are asked to assess the same business several times over by multiple clients," he says. "However, with each third party's permission, we can now store standardised assessments and share them with other clients on-demand."

"LVN is a much faster and simpler way of managing time-consuming workloads for all parties concerned. By greatly reducing the effort required to complete and collate survey responses, more time can be focused on what's important: eliminating control gaps and reducing overall risk."

GDPR is definitely a "game changer" in the world of third-party risk, he adds. "Firms should be responding to the threat of large fines to drive a third-party management programme that assures the security and privacy of their customers' PII data, and ultimately benefits their own business."

In theory, those slow to prepare for May 2018 have already had to switch up a gear and will be at a distinct commercial disadvantage. As we now enter the very first days of the age of GDPR, it may be time to put such a proposition to the test.