

IBM trio boost Alvarez & Marsal's investigations practice

Waithera Junghae, 12 October 2016



Pavel Treskin, James Donnelly and Richard Aitchison
Credit: Alvarez & Marsal

Three former data specialists at IBM, who recently joined professional services firm Alvarez & Marsal, talk to GIR about the biggest cybersecurity challenges companies face today.

On 3 October, Alvarez & Marsal (A&M) announced it had hired James Donnelly as a senior director and Pavel Treskin and Richard Aitchison as directors in its disputes and investigations practice in London. Donnelly joined A&M on 11 July, Treskin on 15 August and Aitchison on 5 September. At IBM, all three executives advised companies on data protection, data compliance and eDiscovery matters.

A&M has launched a new information governance service that will offer companies and law firms advice on how to develop effective procedures to manage and protect sensitive data.

Speaking to GIR, Donnelly said the trio joined A&M because of its “excellent reputation in the industry”.

“The opportunity to introduce a new service to the disputes and investigations team in Europe that addresses the needs of both corporate and legal clients is one that we relish,” Donnelly said.

At A&M, Donnelly, Treskin and Aitchison will advise companies on complying with data laws, including the General Data Protection Regulation (GDPR) which EU member states are required to implement by May 2018. Companies that breach the GDPR can be fined €20 million, or 4 per cent of annual turnover, whichever is greater. They will also advise on securing highly sensitive data, HR information and financial and credit card information and cyber security matters.

GIR Global Investigations Review

According to Donnelly the biggest cybersecurity challenges companies face today are related to internal security breaches. He said that 98% of tested web apps are vulnerable to attack, 90% of large organisations report suffering a security breach and 93% of data protection breaches are caused by human error.

“Despite public discussion attributing external hacks to major leaks, the biggest threat to an average company remains from the inside – the employee who bypasses security controls, either carelessly or maliciously, when performing their job,” he said.

Aitchison said that one of the biggest challenges facing companies is ensuring there are adequate controls in place to avoid data breaches such as the Yahoo! breach in 2014. In September, Yahoo! revealed that a “state-sponsored actor” stole details of 500 million email accounts in one of the largest data breaches in history.

Treskin said that under the GDPR, a company will need to report a breach to the Information Commissioner’s Office (ICO) within 72 hours.

“If ignored, the reputational damage can be catastrophic, excluding the additional audits that the ICO will need to undertake for the good of public interest,” Treskin said. “There are challenging times ahead for all of us, so having an awareness of the potential risk of the data we hold is now paramount.”

IBM did not respond to a request for comment.