CYBER RISKS MUDDY M&A WATERS

As protecting data becomes an increasing area of focus, firms are adding cybersecurity to their due diligence protocol to fill knowledge gaps around a target firm's past and mitigate risk ahead of a merger or acquisition.

Mergers and acquisitions can swamp participating firms, giving hackers the perfect environment to make use of cracks in security.

"The role of [a] cybersecurity due diligence process is not well understood in the industry," said Viktor Andonov, president of technology consultant DataArt Bulgaria. "Currently there are no clear practices and no routine best prescribed approaches for companies to evaluate their future partners in the acquisition, which creates a lot of risk for all of these operations."

Dealogic data shows that 2015 churned out a record $3.8trn in M&A deals, but these numbers fail to paint the full picture. Some financial services firms see the rise of data and intellectual property as a main source of potential profit, and consider an M&A as a means to that end.

"Buying the company translates to buying the data," Andonov said. "[They're] trying to expand their market share, enter another segment or optimize the supply chain. They're buying past, present and future cybersecurity risks."

Karen Hornbeck, a senior manager at Consilio, agreed that data drives M&A in financial services and should be protected at all costs. "What companies are ultimately buying is information," Hornbeck said. "In some shape or form, they're buying the information the target has: intellectual property. Information is the lifeblood of a company, and what decisions are made on."

Despite the heightened importance and emergence of data as the primary incentive for some transactions, cyber due diligence continues to fall by the wayside as firms fail to deeply probe an acquisition target's information security protocol for potential flaws.

"In most companies, the concentration is on the deal rather than on the cybersecurity due diligence," said Kevin Hyams, a partner in charge of Friedman LLP's governance, risk and compliance services practice.

Hyams advises protection of a company's crown jewels. "Whether it's intellectual property or client information, whatever you consider, those must be protected with extra layers of protection," Hyams said. "Risk assessment is the name of the game."

Companies that have been penetrated by an outside source may be seen as less viable M&A targets, with cybersecurity flaws known to be an impetus for a quick exodus from a potential deal.

"There have been many deals that have been scuttled because they find traces of someone being in