SPECIAL REPORT

No company is immune from data security threat

There is often a disconnect between the financial services and fintech sectors

⊙ Wed, Jul 13, 2016, 09:42 | Updated: Wed, Jul 13, 2016, 17:01

Brought to you by
The Irish Times

Data security is a keystone of the financial services industry. One security breach can destroy the reputation of a financial institution. But the rapidly emerging fintech sector is throwing up serious challenges in this all-important area. And the issue is as much related to cultures as it is to technology.

On the one hand there is the cautious, conservative, and quite slow moving world of banks and financial institutions while on the other there is the fast moving, dynamic, entrepreneurial environment of the software and technology companies which are moving into the financial services area.

This can lead to culture clashes based on mutual misunderstanding.

"It's interesting," says Deloitte head of financial services David Dalton. "One of the things we do is figure out how to help large financial services companies engage with fintech firms without getting into the technicalities of security. How the financial services firms protect themselves is through very complex legal procedures and agreements and these tend to be anathema to the fintech start-ups so it can be very challenging."

This disconnect can lead to a lack of awareness among fintech firms of the regulations and security requirements which apply to them. In the UK, the Financial Conduct Authority (FCA) is leading the way in bridging this dealing with this issue. "The UK is leading on regulation," Dalton points out. "The FCA is actively engaging with the fintech industry and has created a regulatory sandbox which allows for experimentation in a safe environment. The UK is very much at the forefront of this when compared to other locations."

"What the FCA sandbox means is that if a fintech firm makes a misstep then they can be reasonably comfortable that the FCA won't move against them," explains Peter Oakes, founder of fintech industry advisory service Fintech Ireland.

He doesn't accept, however, the characterisation of the technology end of the industry as being somehow laggardly when it comes to regulation and security. "There are two schools of thought on this," he notes. "The first is that the technology industry hasn't been subject to financial services regulation and doesn't understand security as a result. The other school is that this is ridiculous; the technology industry writes the code for financial services clients to provide technology and data security."

He very much favours the latter view. "I have walked into banks with small start-up firms and discovered flaws in their procedures. Banks just aim to meet the standards. Tech firms tend to go beyond them. In many instances the technology firms break through the ceiling."

This is set to become a much bigger issue for all involved with the introduction of the Payment Services Directive which requires banks and financial institutions to allow third-party payment providers have access to customer accounts once they have the customer's permission. This will present security issues for all involved.

Indeed, Magnet Networks chief executive Mark Kellett points out that developments such as this are going to force more firms to rethink their position in the market and their approach to security.

"There is a whole cohort of firms who don't realise they are in the fintech sector. These include insurance brokers, credit unions and so on. They deal with our pensions, savings, cash transactions and store data on customers and their finances but they don't view themselves as part of the fintech ecosystem.

"This has to change. They have to start looking at their external connections to the internet and ask what their service providers are doing to protect them as well as their internal systems and everything that is connected to their networks and which might be vulnerable to attack."

David Dalton agrees. "One of the things you have to recognise is that no one is immune. Everybody has been hacked. No bank or company is immune. One thing they have to do is to have the plans in place for how to deal with the consequences of an attack."

This article appears in Future of Fintech, a special report available in The Irish Times newspaper and irishtimes.com/specialreports on Thursday, July 14, 2016.

READ MORE

» Fintech sector is strong but challenges lie ahead

» Digital strategy key to business growth

» European regulation by year end

» How to get closer to your customers

» Fintech has a place within financial service ecosystem