Doing business in the digital age: the privacy problem

As businesses are propelled into the digital age, they are becoming increasingly aware of the value of leveraging data across their enterprise and ever more understanding of the challenges faced by holding such information. FTI Consulting considers how businesses are increasingly under pressure to negate the commercial and reputational impact of cyber threats whilst complying with encroaching government intervention.

> *"There are two types of business in the capital: those who have been hacked and those who don't know they've been hacked."*
>
> *Matthew Richardson Barrister, specializing in cyber-security and intellectual property*

European officials are set to approve regulations that replace a patchwork of 28 laws relating to the use of personal data. The UK government is pressing ahead with provisions to collect personal communications data and require businesses to support in the pursuit of communications information.

This comes at a time where industry is accelerating digital transformations across sectors and government is heralding the use of data to build smart cities and drive public sector efficiencies.

Also accelerating is the risk posed by data to companies and consumers. The Global State of Information Security Survey 2016 found that in 2015, 38% more security incidents were detected than in 2014.

It is with this in mind – where data breaches are the new normal and the value of the records held by companies could prevent serious crime – that businesses are being squeezed by the negative impact of cyber-security threats and the fastening hands of regulators seeking to constrain and exploit consumer and company data at the same time. With an ever more connected business landscape, data privacy must be on the agenda for every company board.

The views expressed herein are those of the author(s) and not necessarily the views of FTI Consulting LLP, its management, its subsidiaries, its affiliates, or its other professionals, members of employees.

A sensitive cyber landscape

2015 saw significant increase in cyber-security attention, made essential by the scale up in cyber threats this year. With a decrease in spending on cyber-security products between 2010 and 2012, possibly impacted by the financial crisis, cyber-crime skyrocketed. According to the Global State of Information Security Survey 2016, security budgets increased by a quarter this year. This is in part due to the higher profile cyber-security has in society. FTI Consulting recently hosted an event on this subject with Matthew Richardson, a barrister specialising in IP, commercial and cyber-crime, where he told an audience of London business representatives that there are two types of business in the capital: those who have been hacked and those who don't know they've been hacked.

In the wake of cyber-security breaches such as the incident experienced by TalkTalk and the realisation that it is not only financial services companies at the victim end of hackers' efforts, businesses and organisations across various sectors are redirecting resources to steel themselves against breaches.

Hackers are targeting universities, as well as hospitals and medical companies, emboldening concerns around the collection of student data, patient information and intelligence held by organisations about citizens. It is widely expected that the next major breach may be of a mobile payments company, part of a booming industry where new entrants are considered to have weak security.

The regulatory landscape

The double edged sword that is the digital revolution is beginning to weigh heavy for businesses, which are subject to increasing controls and calls for compliance by governments. The European regulation set to be confirmed this week will require businesses to allow for the right to be forgotten, forcing companies to remove data about EU citizens that is either no longer relevant or out of date. The laws will also increase scrutiny on these businesses, which may be fined for the misuse of user data and will be responsible for limiting access for young consumers and perhaps most significantly, requiring companies to inform national regulators within three days of any reported data breach. Compliance will be expensive, burdensome and will slow down innovation (for larger and less agile companies), but may also have serious reputational repercussions for businesses which fall victim to cyber-attack, as proven by the TalkTalk case study this autumn. Companies must be prepared for these incidents, ready to employ damage control strategies.

In the UK, the Home Secretary Theresa May's Investigatory Powers Bill goes further, enshrining in law the obligation of companies to assist the authorities in assisting security operations, often in bypassing encryption. Internet and phone companies will have to maintain permanent capabilities to cooperate with government.

A data-driven future

With the Government seeking access to data through back doors, consumers will become less willing to share data, depreciating the value of business data on the whole, leading to greater demand for end-to-end encryption and jurisdictional shopping.

It is a hard task for businesses to make reassurances that data is not only securely and responsibly protected, but it is a force for good: smart application of data can solve social problems like financial exclusion and drive forward innovation – particularly in areas such as healthcare and energy. The OECD has a pillar of work dedicated to data-led innovation.

In order to make such assurances, businesses must remind government of the potential of data for good whilst making reassurances about corporate efforts to secure it.

This can include leveraging the opportunities presented by the cyber threat challenge like investing in biometrics and more personalised security programmes.

Only when coordinated can government and industry fend off cyber threats whilst staying on the path to a data-rich future.

John Gusman is a consultant at FTI Consulting

The views expressed herein are those of the author(s) and not necessarily the views of FTI Consulting LLP, its management, its subsidiaries, its affiliates, or its other professionals, members of employees.

About FTI Consulting

FTI Consulting LLP. is a global business advisory firm dedicated to helping organisations protect and enhance enterprise value in an increasingly complex legal, regulatory and economic environment. FTI Consulting professionals, who are located in all major business centres throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges in areas such as investigations, litigation, mergers and acquisitions, regulatory issues, reputation management and restructuring.

CRITICAL THINKING
AT THE CRITICAL TIME™

www.fticonsulting.com

©2015 FTI Consulting LLP. All rights reserved.