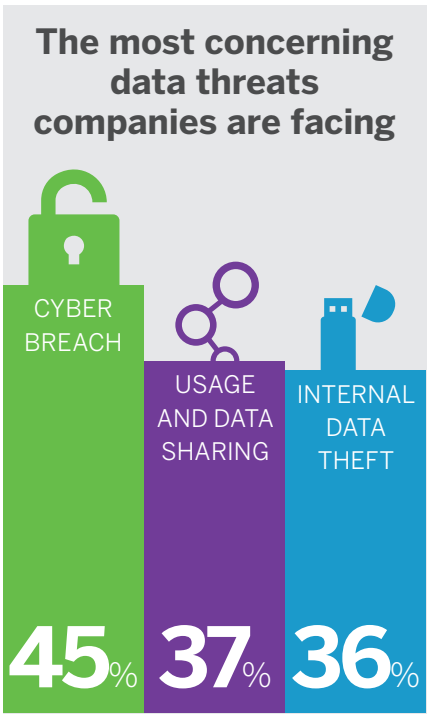
CRISIS MANAGEMENT

GDPR Breach Crisis: are you prepared?

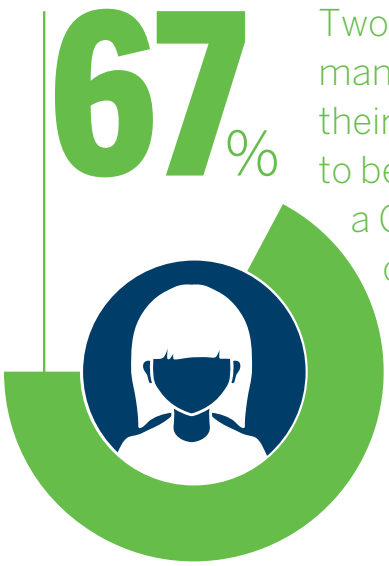
The GDPR compliance deadline might have passed but over two-thirds of UK firms acknowledge they are at risk of a GDPR breach crisis. While data mapping and updating privacy policies are an important aspect of GDPR preparedness, many companies will struggle to respond to GDPR breaches and incidents.



The deadline for compliance with the new General Data Protection Regulation (GDPR) passed on 25th May 2018, yet many firms are not yet fully compliant and are adopting a wait and see approach to the enforcement of the new regulation. Some have taken more drastic measures and suspended operations in the EU. In a recent Financial Times report, many companies were unprepared for the surge in requests regarding usage of their personal data. This is often due to poor information governance and an over retention of personal data, which compounds and become increasingly difficult and expensive as the volume and complexity of data growth is exponential.

One of the critical risks around over-retention of personal data is a data breach. There has been a rapid increase in data theft incidents with an average of 122 data records currently being compromised per second. Within two weeks of the GDPR implementation deadline, more than 1,300 "concerns or complaints" and 60 breaches of personal data were lodged with the regulator in Ireland, the Data Protection Commission. According to the Financial Times[1], the UK Information Commissioner's

1 Companies under strain from GDPR Requests, Financial Times, 2 July 2018



Office received 1,106 data protection complaints in the three weeks after the new rules were introduced and reports of data breaches have also risen. These are only two of the Data Protection Agencies (DPAs) in Europe, so when considered across the EU, the figures will be significantly higher.

Two-thirds of companies feel vulnerable to attack

FTI research based on over 500 responses from UK-based business managers in large companies shows that two thirds (67%) consider their organisation to be vulnerable to a GDPR-related crisis event. Added to this is a finding that over a third (37%) believe that they will only be compliant a full six months after the deadline. This is despite the fact that breaches are on the rise.

"With more than 100 million records breached in this year alone, when it comes to breaches, it's not a matter of whether, it's a matter of when," says Paul Prior, Digital Transformation leader at FTI Consulting. "Managing a crisis properly is the first stage of the process of mitigating further financial and reputational loss. Companies need to understand whether the problems that have occurred are due to the way they put their procedures into practice or whether they're because of the underlying design of those procedures. They must also establish the root cause of any personal data breach and manage the communications, training and technology implications effectively."

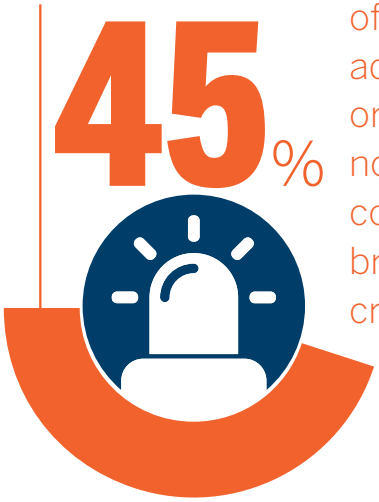
Many organisations have completed the first phases of compliance, for example, assessment, data mapping, updated privacy policies and a legal basis for processing and are now transitioning to business as usual (BAU). They are not preparing for GDPR breach crisis events which can arise from data breaches, data loss or theft, inappropriate data sharing or even data ransom. Companies are also focused on securing their data centres but often forget about the basics. Something as simple and frequently occurring as an untidy desk could also spiral into a GDPR crisis event. Other routine events such as a regulatory inquiry or a data subject request can quickly become public knowledge. With the advent of social media and increased global awareness around privacy, any of these events can quickly spiral out of control. This is especially important given the increased burden that GDPR places on organisations as they manage data.

GDPR – managing data versus being crisis-ready

GDPR changes the way in which companies are permitted to collect, process and share data which significantly elevates the standard of transparency and care for which they will be held accountable. Consumers have new rights over their data that they are increasingly aware of, while privacy campaigners are becoming more active and vocal and have a global impact.

"Understanding the difference between managing data effectively under GDPR and being prepared to handle a crisis occurring because of the increased regulation and subsequent risk around data is crucial," says Sonia Cheng, European Information Governance and Compliance leader at FTI Consulting. "GDPR has changed the landscape completely. Companies are still thinking of customer data as theirs to monetise and do with as they please, but GDPR requires them to put their customers front and centre, with many more rights over their own data. This is a new concept."

"Given this awareness of the threat of a GDPR breach related crisis, it's particularly worrying that nearly half (45%) of those asked admit that their organisation is unprepared to cope with such an event," says Paul Prior. "These figures suggest that this unprecedented increase in the level of regulation and the associated risk has much of the C-suite unsure of how to respond."



Lack of certainty

This lack of certainty is breeding fear and anxiety among business leaders and those directly responsible for data with nearly half (45%) reporting that their organisation is "panicking" about compliance. This rises significantly in the TMT sector to nearly two thirds (62%).

"We're finding that firms are also becoming aware of the impact that a GDPR breach crisis could have on them," says Charles Palmer, Global Head of Telecom, Media & Technology (TMT) in FTI Consulting's Strategic Communications segment. "They realise that it has implications for their client relationships, their financial situation and their reputation."

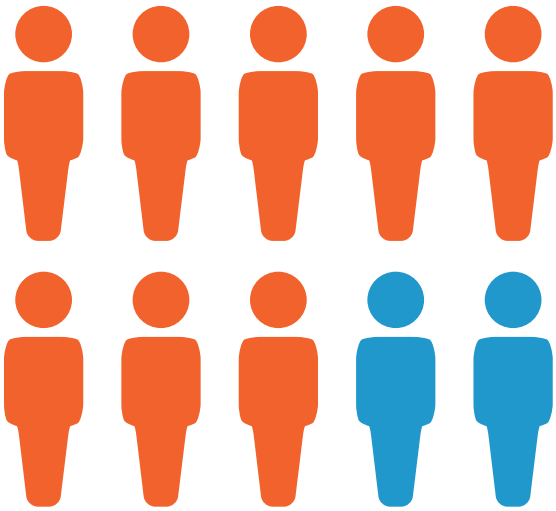
Nearly eight out of ten (79%) of large UK companies say that this would damage their reputation and a similar proportion believe that it would entail a financial loss to their turnover, on average by 5%, as a direct consequence of a GDPR breach event.

"This is a very large sum by any standards and would naturally prompt serious concern among shareholders," says Charles Palmer. "It shows that business leaders are aware of the direct financial impact that a GDPR breach crisis could have but also the critical nature of the response. A playbook for the first 72 hours is critical as is a clear understanding of the impact on all of a company's stakeholders. This initial response will be the basis for rebuilding trust and confidence - get it wrong and a company's licence to operate is compromised."

A serious effect on client relationships

As well as the effect on the licence to operate and the share price, large UK companies are aware that they could suffer long-term damage because of the impact on client relationships. On average, they would expect to lose 17% of their clients because of a GDPR breach crisis. Not surprisingly, industries that rely heavily on data are particularly vulnerable here with over a fifth (22%) of those in the banking, financial services and insurance sectors expecting to suffer in this way and over a quarter (27%) for the technology and telecoms sector. Retail businesses anticipated a lower loss of clients (13%), but in an industry that is currently struggling economically, even this relatively modest figure would still have significant negative consequences.

Nearly eight out of ten (79%) of large UK companies say that this would damage their reputation



Whatever their sector, companies are struggling to understand the variety of different threats that they face. A cyber breach, cited by 45%, is the subject of most concern, followed by usage and sharing of data (37%) and internal data theft (36%), according to the findings. "These figures demonstrate that many firms still aren't aware of the extensive range of risks that they face, many of which are new or more severe than before," says Sonia Cheng.

"A breach could be inappropriately used data, for instance, or even a lost laptop," she explains. "But business leaders need to understand the difference between a standard incident and a full-blown GDPR crisis where they may require support to undertake a forensic investigation or manage reputational damage."

The lack of an appreciation of the difference between a breach and a crisis is borne out by the degree of complacency revealed in the survey. Among those asked with 78% agreeing that it is unlikely that their organisation would be fined for breaching GDPR and nearly two thirds (65%) believing that "As long as you show you're taking steps to be compliant, organisations won't be fined." Sonia Cheng says. "In this new world of data protection, this approach is not good enough."

Firms are taking some action – but it's not enough

Despite the fact that nearly half believe that they are unprepared, firms are taking at least some action. Nearly two thirds (64%), for instance, are establishing a response team. However, only around half (54%) are regularly reviewing their response process while less than a quarter (22%) have taken out cyber insurance and under a third (32%) have performed table-top exercises with crisis management response teams.

"Forward-thinking companies are realising the benefits of these simulations," says Charles Palmer. "The best way to identify the effectiveness of procedures and systems is to run them through an authentic crisis event. The increasing number of organisations that we work with come away from these exercises with a detailed knowledge of what they need to fix and how they can fix it."

Sonia Cheng is encouraged by the fact that some companies are now taking action. However, many are still not proactive enough, she says. "When it comes to breaches and other threats they need to think about prevention rather than cure. This involves running their systems as if there had been a serious breach in order to put them through their paces. They also need to develop and test messages to customers, shareholders and regulators."

Business leaders need to do more than paper-based compliance. "They need to understand what a real crisis would look like to them in all of its severity so that they can assess and analyse how best to respond," she adds. "GDPR has transformed the world of data management and regulation as well as risk management more than many people realise. Now, is the time to move beyond the theories, and transform best case scenarios to stress-tested crisis readiness."

Managing a GDPR crisis

Among the key actions that organisations should take are:

RESPOND

Take immediate actions when a potential breach has been identified.

- Identify and train a "red button" team to determine the scope and potential impact of the crisis
- Develop and refresh an external and internal communications strategy
- Monitor coverage

RESOLVE

Deploy the critical technical and communications elements to identify and contain the crisis.

- Analyse data and investigate cause and impact
- Enhance resilience
- Continue stakeholder communications and monitor coverage/reaction
- Refresh GDPR training

REBUILD

Develop and implement recovery plans to limit the lasting impact of the crisis, return to business as usual, and better prepare the business for the future.

- Restore reputation
- Perform comprehensive GDPR risk assessment and implement new technology as required
- Establish third party monitoring
- Develop a new employee engagement strategy around personal data
- Incorporate lessons learnt into policies and procedures
- Assess cybersecurity and implement a new programme

The research and findings referred to in this paper were conducted online by the Strategy Consulting & Research team at FTI Consulting from May 17th- 21st 2018, with n=502 UK-based business managers in large companies.

Sonia Cheng
+44 (0)20 3727 1783
sonia.cheng@fticonsulting.com

Charles Palmer
+44 (0)20 3727 1400
charles.palmer@fticonsulting.com

Paul Prior
+353 (0)8796 65296
paul.prior@fticonsulting.com

FTI CONSULTING™

EXPERTS WITH IMPACT