Written evidence submited by TalkTalk plc (DEB 09)

Data breach reporting guidelines

Overview

The regulatory system for reporting data breaches in the UK is not fit for purpose. Government research shows 9 out of 10 large organisations have suffered data breaches, but the vast majority are under no obligation to report incidents, entrenching a corporate cover-up culture that leaves British consumers exposed.

As a result, the UK is experiencing an unprecedented wave of text, email and phone scams (see Annex 1 for key stats) which has caused the National Crime Statistics to rise for the first time in decades.

Forthcoming European regulation is notionally a step in the right direction, but extensive exemptions mean companies will still be able to conceal breaches from regulators and customers. Many of the UK's digital rivals around the world, in particular the US, already have more stringent, mandatory reporting obligations.

The Digital Economy Bill is an opportunity to create a more transparent, fit for purpose approach to cybercrime which ultimately protects future confidence in the UK's digital economy. Without this, there is a real risk that consumers and businesses are left vulnerable to a 21st century crime wave which disincentivises online engagement and commerce.

Ultimately, consumers must become more vigilant; and companies must do more to protect data. Both of these aims depend, however, on a regulatory framework which ensures responsible corporate behaviour in response to ever more frequent and sophisticated instances of cybercrime.

The Existing System (full details in Annex 2)

Two current pieces of regulation currently apply, but neither impose meaningful obligations on organisations:

- **Data Protection Act (DPA):** The DPA deals extensively with the protection of personal data, but there is no legal obligation on companies to report data breaches either to the ICO or customers. Any reporting is entirely at the discretion of companies.

- **Privacy and Electronic Communications Regulations (PECR):** PECR does include obligations on companies to report breaches to the ICO, but it only applies to telcos / ISPs, and only requires companies to "consider" informing customers. Even telcos and ISPs can exempt themselves from all obligations under PECR if reporting would make it more difficult for police to apprehend or prosecute the perpetrators of attacks.

The net impact of the DPA and PECR is that the vast majority of data breaches go unreported. IoD research from March 2016 showed just 28% of attacks were reported to police. Even fewer are reported to the ICO or consumers, meaning customers are never warned that their data has been taken and never advised on how they can protect themselves. The regulation actively enables a culture which prioritises protecting corporate reputation above protecting customers.

Forthcoming EU Regulation

At present, Government is putting great faith in the forthcoming General Data Protection Regulation (GDPR) to address the current gaps in UK law. When implemented in 2018, it notionally forces all companies to report breaches to regulators and customers. In reality, however, it contains such extensive caveats that companies seeking to conceal breaches will likely still be able to. For instance, when theoretically applied to the TalkTalk cyber attack in October 2015, at least two exemptions in the GDPR would have applied. This falls a long way short of the comprehensive regulatory system the UK needs.

Below are some top level concerns about the GDPR exemptions. Clearly there is a broader point around whether the Government actually still intends to incorporate into UK law post exiting the EU. DCMS is currently unable to confirm whether this will be the case. If the UK does intend to implement it, the current lack of detail around exemptions is concerning. Some of these may be resolved as part of the continuing process of development of the legislation, between now and 2018, however the UK is now unlikely to be a part of that process. The final mechanics and scope of those exemptions is therefore unclear at present, and also potentially outside the UK's control.

Exemptions **Data processors are exempt from any obligation to tell regulators about a breach if:**	
It is unlikely to result in a risk for the rights and freedoms of natural persons	Definition of this is open to interpretation. Does it have to be financial data? Would publicly available information such as name and address count? There's far too much ambiguity to give consumers genuine reassurance that this forces a culture of transparency
Data controllers are exempt from any obligation to tell customers about a breach if:	
It is unlikely to result in a high risk for the rights and freedoms of data subjects	As above
Appropriate technical and organisation protection were in place at the time of the incident	What would constitute appropriate protection? Would encryption of financial data count? Who judges whether appropriate protections were in place? Are companies marking their own homework? If our security team judged that they had taken reasonable measures, but were defeated by a very sophisticated attack, would they be able to exempt themselves by claiming that they had 'taken appropriate steps, but no one could be entirely safe'?

	If some sort of independent, external investigation is required to determine whether a company had taken appropriate protections, how long does that take? Is there a time limit? Could a company kick any disclosure into the long grass by announcing an exhaustive, 18 month review to determine this?
Notifying customers would trigger disproportionate efforts (instead a public information campaign or "similar measures" should be relief on so that affected individuals can be effectively informed)	This should not be a judgment call for businesses. There is a basic point of principle, which is that if a company has lost customer data, the customer deserves to know. It should not matter what temporary burden that places on the organisation. Arguably, the threat of a big administrative burden to notify customers is an effective deterrent that incentivises good corporate behaviour. Far from being something we should shield companies from, it is something we should be exposing them to. A public information campaign is insufficient for two reasons: - A large proportion of customers will likely not see it. No advertising campaign delivers 100% awareness. Nor even close. 20-30% would be a triumph for an advertising agency. - It would have to be generalised (X business has suffered a data breach, you may be impacted). That does not actually tell a customer whether they are impacted; what data has been taken; and what specific steps they need to take. That means fewer people will take the defensive steps necessary, leaving more customers vulnerable.

Finally, there is the issue of timing. We know that speed matters very much in these situations. The quicker customers act to change passwords and take other actions to protect themselves, the lower the risk of harm. However, in order to know whether any of the exemptions apply (i.e. whether the stolen data results in a high risk for the customers; whether appropriate technical protections were in place; and whether notifying people would be disproportionate) the business would need to know very precisely what had been

taken and how many people were impacted. As was the case with Talktalk, that can often take weeks or months to find out.

TalkTalk had the resources to hire a large team of security experts to work around the clock to understand the extent of the attack, and it still took over two weeks. A smaller company without a budget for this external support would take a much longer, similarly a company looking to keep an attack under wraps might logically opt to in-house such work rather than bring in external consultants. Therefore our view is that the GDPR actually provides an incentive for companies to delay notifying customers until they have done that work. That could mean companies knowing customers are at risk for long periods before feeling obliged to notify. This does not reflect the reality of a cyber attack experience, nor the incentives of companies in that situation. It is simply the wrong premise on which to base reporting requirements.

The Opportunity – Digital Economy Bill

The Digital Economy Bill is an opportunity to give the UK a fit for purpose regulatory system. Many rival digital economies already have effective mandatory reporting of attacks; it is crucial the UK follows suit with reporting obligations with far less extensive exemptions than the GDPR. Without it, the UK will fall behind our rivals and Britain risks being perceived as an international soft touch on cybercrime.

Failing this, Talktalk is also potentially interested in an extension of the current data protection legislation to all companies, at least as a stopgap before more modern, fit-for-purpose rules can be developed. This could be done through the Digital Economy Bill with relative ease and we are discussing with legal counsel how such an amendment might operate.

The Bill could also go further to impose specific obligations on telcos to better protect customers from 'scam calls'. Often the information stolen in cyber attacks in insufficient to steal directly from victims, but criminals are able to use fragments of information to scam customers. Often this involves pretending to be from a company, gaining their trust and persuading them to part with the details needed to steal from them. The Digital Economy Bill could address this by:

- **Imposing an obligation on telcos to block known scam calls:** Telcos can identify known nuisance and scam call numbers, but until recently TalkTalk was the only company blocking them at source (network level), before they reach customers. We currently block 70m known nuisance and scam calls to our 4 million customers each month. One other provider has followed our lead, but the vast majority have not. The Digital Economy Bill could address this and prevent criminal gangs (many based abroad) from targeting vulnerable UK customers.

- **Preventing telcos charging customers for their privacy:** The vast majority of providers offer a suite of privacy features to help customers to protect their privacy and block scam calls. Features include automatically blocking anonymous calls and enabling customers to bar the last number that called them. TalkTalk is the only major provider offering these tools for free. The Bill should explore banning the

practice of charging customers for these services to prevent telcos profiting from nuisance and scam calls.

Conclusions

The UK can be rightly proud of its status as leading digital economy, but without mandatory reporting and action to protect consumers, data breaches will continue to fuel online crime and damage consumer confidence in the digital world. A more robust Digital Economy Bill could address this, driving a culture change in how British companies manage cyber risks, creating a more transparent system that puts protecting the public first.

Annex 1

- According to **Financial Fraud Action**, fraudsters stole £755m from Britons during 2015 – a 26% increase on the year before. Losses due to online and telephone banking scams totalled £168.6m in 2015, a staggering 72% increase compared with the year before
- Figures from Financial Fraud Action UK (**FFA UK**) show 58% of people received suspicious calls last year, a year on year rise of 17%
- The **Office of National Statistics** reports 5.1 million incidents of fraud in England and Wales last year, with over 2 million individuals experiencing financial loss.
- Research from the **Money Advice Service** shows eight scam calls are placed every second from fraudsters purporting to be banks, utilities companies, even HMRC.
- Research from **Get Safe Online** revealed a 20% rise in 'phising' emails, calls and texts from criminals masquerading as trusted entities in order to access confidential information or steal money
- **Action Fraud** figures show 8,000 reports of 'phising 'scams a month in in May 2016

Annex 2 – Detail on Regulatory Requirements

Data Protection Act (DPA)

- There is no legal obligation to report breaches to the ICO under the DPA. It's at the discretion of companies.
- The ICO states: "Although there is no legal obligation on data controllers to report breaches of security which result in loss, release or corruption of personal data, the Information Commissioner believes serious breaches should be brought to the attention of his Office."
- "Serious breaches" are not defined by the ICO. Instead they urge organisations to consider the following when assessing whether it is a serious breach:
    - The potential detriment to data subjects – including emotional distress and exposure to financial and physical damage.
    - The volume of personal data lost / released / corrupted
    - The sensitivity of the personal data lost / released / corrupted

Privacy and Electronic Communications Regulations (PECR)

- The Privacy and Electronic Communications Regulations (PECR) does require organisations to report breaches, but this only applies to organisations that provide a service allowing members of the public to send electronic messages (eg telecoms providers or internet service providers).

- PECR derives from an EU Directive – commonly referred to as the ‘e-privacy directive’.
- PECR covers several areas:
    - Marketing by electronic means, including marketing calls, texts, emails and faxes.
    - The use of cookies or similar technologies that track information about people accessing a website or other electronic service.
    - Security of public electronic communications services.
    - Privacy of customers using communications networks or services as regards traffic and location data, itemised billing, line identification services (eg caller ID and call return), and directory listings.
- There is ambiguity even within PECR. The ICO states that "PECR do not define ‘electronic communications’.” Instead, the rules apply in different ways using specific concepts and definitions. There’s also ambiguity about how it applies to common modern services, such as public wifi. The ICO believes to a “service provider” would “generally have a formal and ongoing contract with the customer subscribing to the service”, so that would exempt a café or hotel that provides wifi. It’s a good example of how the regulations provide a lot of scope for subjective interpretation, and public wifi is hardly a niche case study. It’s a standard part of everyday life.

PECR Reporting Requirements:

- PECR requires that following a data breach, a company to:
    - reports it to the ICO;
    - “consider whether to notify your customers"; and
    - Record it in a company log.
- Reports to the ICO must be made in 24 hours. It must include:
    - The organisation name and contact details;
    - the date and time of the breach (or an estimate);
    - the date and time the organisations detected it;
    - basic information about the type of breach; and
    - basic information about the personal data concerned.
- If possible, reports to the ICO should also include full details of the incident, the number of individuals affected and its possible effect on them, the measures taken to mitigate those effects, and information about your notification to customers. If these details are not available for the initial report, organisations must provide them as soon as possible. Organisations must submit a second notification form to the ICO within three days, either including these details, or telling the ICO how long it will take the organisations to get them.
- The ICO states that under PECR, organisations should notify customers “if the breach is likely to adversely affect the personal data or privacy of your subscribers and users”. You do not need to tell your subscribers about a breach if you can demonstrate that the data was encrypted (or made unintelligible by a similar security measure). The ICO may, at a later date, decide you should have told customers and order you to do so. This leaves a lot of scope for organisations to dodge telling customers.
- The robustness of PECR is further undermined by a specific law and crime exemption (regulation 29). Comms providers are exempted from all obligations under PECR if complying would:
    - breach a provision of another enactment;
    - breach a court order;

    - be likely to prejudice the prevention or detection of crime; or
    - be likely to prejudice the apprehension or prosecution of offenders.

EU General Data Protection Regulation

- The GDPR regulations will be implemented in 2018 and will significantly reform data protection regulation in Europe.
- The GDPR introduces a standardised framework for security breach communication, regardless of sector.
- The GDPR has important exemptions.
- Data controllers do not need to report breaches to their supervisory authority if a breach is unlikely to result in a risk for the rights and freedoms of natural persons.
- Similarly, data controllers don't need to tell customers if:
    - The breach is unlikely to result in a high risk for the rights and freedoms of data subjects;
    - Appropriate technical and organisation protection were in place at the time of the incident;
    - This would trigger disproportionate efforts (instead a public information campaign could be relied on so that effected individuals can be informed).
- These exemptions will allow companies that want to avoid notifying customers to continue to do so. Arguably, either of the first two conditions could have applied to TalkTalk.
- There is also the issue of timing. In other to understand whether the first exemption applies, you need to know what data has been stolen. That actually provides an incentive for companies to delay notifying customers until a full investigation is complete. That leaves them exposed to criminals in the meantime.
- The GDPR is designed to strengthen reporting obligations and standardise obligations across different sectors. But the exemptions mean it falls a long way short of what is needed.

October 2016