FTI CONSULTING | CYBERSECURITY techUK TRAVERS SMITH

Data and the Digital Economy Series – managing cybersecurity risks to your business

traverssmith.com

Overview

Increased digitalisation means increased cyber vulnerability – as too many businesses are finding out, particularly after the huge increase in remote working and greater use of cloud technology. But cyber risks can no longer be categorised as special or something that will only affect technology focused businesses. It really is a question of when a business or organisation will face a cyber attack, not if. And the consequences, in terms of the theft of data or intellectual property and reputational damage can be immense.

Managing cybersecurity risks to your business: webinar

In a webinar hosted by Travers Smith with techUK and FTI Consulting on 22 April 2021, we examined the scale and nature of cybersecurity threats for businesses, the legal and regulatory risks associated with a data breach, and the steps businesses can take to mitigate these risks and prevent their data, systems and knowhow being compromised.

The webinar was chaired by Nicky Morgan, former Digital Secretary, now a consultant at Travers Smith and our speakers were Dan Reavill, Head of the Travers Smith Commercial, IP & Technology Department, Joshua Burch, Senior Managing Director and Head of Cybersecurity for EMEIA at FTI Consulting, and Sian John, Director SCI Strategic Growth Business Development at Microsoft and Chair of the techUK Cyber Management Committee.

This briefing sets out the broad points that were made and a recording of the webinar is available on our website.

The scale and nature of cyber threats for businesses

In the latest FTI Consulting Resilience Barometer™ report, 75% of G20 organisations said they had been negatively impacted by a cyber attack in the last year.

In March 2021, the UK Department of Digital, Culture, Media & Sport published their latest Cyber Security Breaches Survey. The survey found 40% of businesses and charities reported cyber breaches/attacks. This number is higher among medium-sized businesses and high-income charities. It was found that 23% of charities and 27% of businesses respectively experienced attacks once a week, most commonly from phishing and then from impersonation.

As Nicky Morgan said, "Businesses are now at the frontline of cyber security risks as they experience the effects of the risk and have to deal with them." This is an issue of national importance and she pointed to the National Cyber Security Centre's Board Risk Management toolkit on cyber security, and the Government's recently announced new National Cyber Force, as part of their Integrated Review on Security, Defence, Development, and Foreign Policy.

Joshua Burch defined cyber security as ensuring the confidentiality, integrity and availability of assets and data and the network and systems that carry them. Personal data and meta data are big assets for the world's most successful companies. Data also has big liabilities if it falls into the wrong hands. But the impact is much more than money – for example, intellectual property theft is a very real challenge as is reputational damage from the impact of a cyber security breach if a company responds poorly.

1m new strains of malware are detected every day and an estimated 4,000 daily ransomware attacks occur too. A single cyber breach costs in the region of 8m USD on average and a breach involving 50m personal data records could cost 400m USD.

Given the most common type of breach or attack reported by organisations in the last 12 months was phishing, Joshua noted that it is easier to "hack the human" which is a real threat. Nicky Morgan supported this by pointing to the cyber attack on Parliament where the attackers had targeted weak passwords to get into the parliamentary e-mail system.

The National Cyber Security Centre recently warned that ransomware has become more common. In 2020 the NCSC handled more than 3 times the number of such attacks than the previous year. Cyber capabilities which were only available a few years ago to nation states are now available to buy on the dark web. A Distributed Denial of Service attack (DDoS), which buys up websites and portals and jams them with traffic, can be bought online for 1000 USD.

The sudden shift to remote working environments has speeded up the evolution of cyber threats even further. Scams capitalising on the remote working situation infect systems and harvest credentials and we are also seeing fraudulent wire transfers more likely to succeed. From a survey of 2700 G20 organisations at C-suite level, 32% of companies lost customer/patient data, 28% were victims of phishing attacks, 26% lost IP, and 25% experienced ransom or data hostage situations. Businesses must therefore understand the current threats and determine how these threats have evolved since the pandemic – putting that another way, as Joshua said, "Cyber security is the tax we must pay for the benefits of digitalisation."

The legal and regulatory risks associated with a cyber attack

As the lawyer on the panel, Dan Reavill focussed on the legal ramifications of a personal data security breach. He also examined the intersection of data protection laws with traditional criminal laws in the world of computers and data usage, together with the situation where an employee might make an unauthorised use of an employer's data.

The core legal risk for an organisation which is on the receiving end of a personal data security breach, is of course data protection law, and the starting point is the General Data Protection Regulation 2016 (EU GDPR) and now the UK GDPR too, as well as the privacy laws of other jurisdictions whose data subjects might have been affected. We focus here on UK GDPR (GDPR) (the provisions of which are for now, aligned with EU GDPR), which include a series of fundamental principles that apply to any organisation that is holding and using personal data and falls within scope of the legislation.

One of the key principles is that all personal data must be processed in a manner that ensures an appropriate level of security for the personal data in question, and there are specific references to protecting against for example, unauthorised processing of personal data (such as hacking). Article 5 (1) (f) GDPR is core in terms of setting out the duty around security. This is supplemented by Article 32 which provides more detail on security requirements, and sets out a risk based approach requiring organisations to assess the risk of losing data or being on the receiving end of a security breach. This effectively means that where an organisation processes health data, or other special category data for example, a rather more stringent level of security needs to be adopted, compared to situations where an organisation is simply holding contact details for a handful of business contacts.

Both Article 5 and Article 32 come into focus when an organisation suffers a data security breach. Which can result, as Dan pointed out, in a situation where an organisation can be both a victim of crime (the cyber attack itself), and an offender of GDPR (because it failed to take appropriate measures to protect against such cyber attack), as a result of the same data breach.

The financial fall out, or direct legal costs for an organisation that has suffered a breach involving personal data, under data protection laws, is as follows – there are essentially two types of cost:

1. An organisation can be sued by an individual for the damage they have suffered as a result of the infringement by the organisation of GDPR. At the time of writing, the Supreme Court is hearing the appeal by Google LLC against the order of the Court of Appeal in the landmark case of Lloyd v Google LLC [2019] EWCA CIv 1599. Mr Lloyd is a former director for Which magazine, and brought the claim against Google on behalf of 4 million iPhone users for misuse of data collected through their Safari work around installed on iPhones. If Mr Lloyd is given the go ahead by the Supreme Court to bring the claim outside the jurisdiction of England and Wales (ie to serve out in the US), the repercussions could be huge, as the floodgates will be opened for this type of claim. Although the claim is based on breach of the former Data Protection Act 1998, the case highlights the considerable risks under GDPR in relation to damages claims and class actions.

2. There is also the possibility of having to pay a penalty issued by the regulator – in the UK – the Information Commissioner – for breach of data protection laws, and this is the type of cost/risk associated with a personal data breach that many organisations tend to focus on, including when negotiating contracts and in particular indemnity and liability provisions. Technically, contravention of data security provisions in GDPR does not result in the awarding of a criminal fine, but a civil penalty levied by the regulator in the UK (and in the case of EU GDPR, relevant member states). There are two tiers of penalties, and the key thing to note is that if an organisation contravenes the obligation in Article 5 (1) (f), it is then subject to the larger penalty, which in the UK is the higher of a maximum of £17.5 million or (more importantly for larger organisations), 4% of group worldwide turnover in the previous financial year.

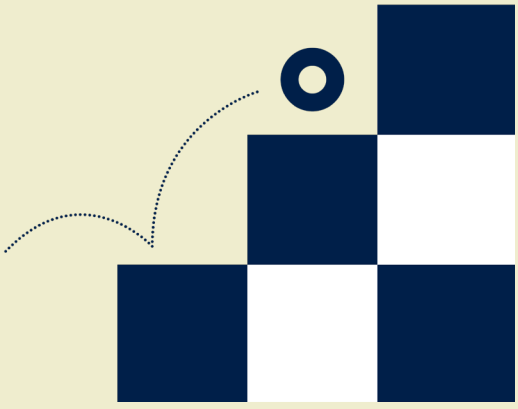
The most high profile data breach related penalties in the UK to date, are those recently awarded against an airline (£20 million), and a hotel operator (£18.4 million). An online ticket seller was also recently awarded a penalty of £1.25 million. In all cases bank and credit card details of customers were hacked. The way the parties reacted to the breaches and liaised with the Information Commissioner's Office (ICO), impacted the amounts awarded: the ticket seller was slow in acting when tipped off by the banks regarding fraudulent activity by a chatbot facility on its website, and the ICO took a dim view of the delay in rectifying their security shortcomings. Conversely, the main mitigating factors for the airline and the hotel operator, when calculating the penalties, was the swift and efficient response and remedial action that they took, and their preparedness for dealing with the fallout of the breaches, and this is one of the reasons why their penalties were reduced from the original figures suggested by the ICO in the summer of 2019.

Another angle to consider, is the situation in which an organisation may be responsible because of something an employee does. In last year's landmark decision in WM Morrison Supermarkets Plc v Various Claimants ([2020] UKSC 12, the Supreme Court found that an employer isn't automatically vicariously liable for the acts of a rogue employee in a data security context, though its important to note that this scenario was governed by the former Data Protection Act 1998, and was therefore pre-GDPR. (For further details of the judgement please see our briefing). The GDPR now includes, in the shape of Article 32 (4), a specific provision that all data controllers and processors must ensure that anyone acting under their authority who has access to personal data, only processes that personal data under the instructions of the controller or processor. One of the ramifications of this is that employers must only permit employees to process personal data for the purpose of their role.

That said, another way in which an organisation might be able to mitigate the financial fall out from a data security breach, is through the less well known route of persuading the regulator to shift its focus to any criminal activity carried out by individuals involved, rather than focussing on the contravention of the security requirements in Article 5 (1) (f). A recent case has shown that this tactic can be successful, particularly in circumstances where there is a rogue employee who has gone off plan to take or disclose personal data. By way of background, whilst GDPR is mainly made up of civil law penalties, there are a number of criminal provisions, including Section 170 of the Data Protection Act 2018 (which sits alongside GDPR) which states that it is a crime to unlawfully obtain personal data without the consent of the controller (which was originally designed in part to stop the activities of unscrupulous journalists and private investigators who were impersonating individuals and was also related to a phone hacking scandal).

However the Computer Misuse Act can come into play as well, if the circumstances lend themselves to it. In a recent case, the ICO decided that the acts of an employee who had obtained data without authority, were so flagrant, that it prosecuted under the Act (which effectively creates a crime of hacking), rather than under the Data Protection Act. The case related to the RAC, which keeps a database of road traffic accident details, including the contact details of those persons involved in the accidents. An employee extracted the data and sold it to an accident claims management business, which then bombarded the people involved in the accidents, with offers to sell their services. Both the employee and the recipient at the accident claims management business received eight month prison sentences for crimes under the Computer Misuse Act, suspended for two years, plus community service and confiscation orders.

Dan Reavill surmised that the ICO departed from the use of data protection laws in this case, because, in contrast to the GDPR, the Computer Misuse Act provides for custodial sentences. He also pointed out that an important factor in the case was the level of assistance provided by the RAC, which provided evidence to the ICO which made it easier for them to pursue the individuals in question. The case shows that where the circumstances lend themselves, the ICO can be persuaded to divert its attention away from the data controller and focus instead on criminal prosecution – albeit that this is only possible if the individual in question is identifiable, or where an employer knows who has carried out the crime.



Building cyber resilience

FTI Consulting's three main steps to protect businesses were:

1. Passwords are basic cyber security hygiene – businesses need to enforce their policies and procedures and ensure they are followed by staff and kept updated. Businesses also need good security monitoring and training for staff on VPN and multi-factor authentication as well as clear messaging from the leadership of an organisation in relation to the importance of cyber security.

2. Strive to become a cyber resilient organisation – focus on identifying and protecting assets, data and systems. Understand that the risk environment is constantly evolving. Businesses should perform an internal assessment and determine what their crown jewels are i.e. key technologies, proprietary software, key manufacturing facilities. Resilience needs to be practical and attitudinal across people, processes, and technology. A culture of resilience and a mindset to acknowledge cyber security is required, as it is an issue of when, not if a breach occurs.

3. Focus on third-party supplier management – most organisations underestimate their exposure. When signing an on boarding contract a business should be confident it knows where its data is. In 2014, a retailer suffered an attack which penetrated its third-party ventilation supplier, and then escalated the attack from the supplier to the retailer's checkouts. The attackers sold 70m customer details unnoticed on the dark web for months.

Managing cyber risks – a view from the frontline

Sian John was clear that managing cyber risks should not start with legislation nor a rigid checklist – the attackers are not 'working to checklists'. Sian identified that one challenge we have, as we move to using the cloud, mobile and remote working, is that security technology is based on architecture that is 20 years old. We need to look at the way people operate and bake security into the way people work.

Sian observed that when we think about cyber risk, we tend to treat it as something separate but "it's not a special risk...organisations will need to think about cyber risk as yet another one of their risks (like financial risk) but with a special element in it." It can also be physical, so businesses need to build cyber expertise into their entire risk management system.

Sian also backed the use of two, or better still multi-factor authentication stating that "90% of attacks Microsoft see...can be stopped by multi factor authentication...so if you do one thing today enable MFA." She also said that "15–20% of people when they get [an MFA] challenge will answer it on their phone even when they are not trying to log in, so don't blindly answer texts/challenges if you are not expecting it."

Sian's key advice is:

1. Adopt a zero-trust approach – this is not a product but a principle and approach in relation to designing your security environment. It means having no implicit trust for any connection, in that organisations and people should have zero standing trust for any connection. There are 3 principles to zero trust:

    a) Explicitly Verify: At the point anyone opens a programme or application they should have to explicitly verify that they have rights to access it – it is easy to give everyone access to everything, but Sian's advice is that access should only be given for what is needed. The device, the user and the context should all be considered in determining if the connection is allowed and any access should be conditional on a healthy connection.

    b) Least Privilege. Only give people access to what they need and no more. They should only have the rights to access data or systems that they need to pursue their role. An example of how this should change is in privileged access. In the Microsoft world there should be fewer 'global admins' with global access permissions in a business. The more 'global admins' a business has the easier it is for a hacker to get through via a phishing attack. These should not be routinely used for administration but other more focused admin privileges instead. So temporary rights and fewer privileges is better. Administrators should also not use the same account or device to administer the environment as they use to check their email.

    c) Assume compromise (not breach) – the difference between breach and compromise is that a breach means the attacker got in but doesn't mean they gained access to anything, whereas compromise means they did. Always assume someone has got in, then ask what is the business' exposure to risk.

2. Don't wait for the compromise to happen to work out how to respond – work out who will talk to the press, who will inform the regulator, who will decide when to turn off the email system – organisations should be pre-prepared.

Travers Smith LLP 10 Snow Hill, London EC1A 2AL +44 (0)20 7295 3000 | traverssmith.com