How to prepare for data breaches? Lessons learned from recent incidents

Received: 26th August, 2018

Paul Lanois
is a global privacy, data protection and information security professional, and is an attorney admitted to the Bars of the District of Columbia (DC-USA), New York (NY-USA) and the Supreme Court of the United States (SCOTUS). He regularly publishes articles on technology law and is frequently invited to speak on such topics. He has spoken at numerous conferences across the USA, Europe and Asia. He has been recognised as a Fellow of Information Privacy (FIP) by the International Association of Privacy Professionals (IAPP) and is a Certified Information Privacy Professional, with concentrations in Asian law (CIPP/A), US law (CIPP/US), European law (CIPP/E) and Canadian law (CIPP/C). He is also a Certified Information Privacy Manager (CIPM) and a Certified Information Privacy Technologist (CIPT). He was an associate professor at the University of Cergy-Pontoise in France and an attorney at major international law firms (Simpson Thacher & Bartlett, Allen & Overy and Linklaters). He graduated from the University of Paris-Sorbonne (France) with a Master's degree in business law and a postgraduate degree in private and public economic law. He also holds an LL.M. degree from the University of Pennsylvania Law School (USA) and a Certificate in Business and Public Policy from the Wharton School at the University of Pennsylvania.

E-mail: paul.lanois@outlook.com

Abstract It seems like every few weeks there is a report of a new data incident having taken place: recent high-profile examples include FedEx (February 2018), Under Armour/MyFitnessPal (March 2018), Panera Bread (April 2018), Adidas (June 2018), MyHeritage (June 2018), Macy's (July 2018), Timehop (July 2018), Reddit (August 2018) and T-Mobile (August 2018), just to name a few. So, what should organisations do in relation to cybersecurity incidents? More specifically, what can happen when the board or senior management is not appropriately engaged nor response plans properly practiced or otherwise followed? What can we learn from previous security incidents that have taken place? This paper examines some real-world cases of what can happen following a security incident.

KEYWORDS: data breaches, GDPR, cybersecurity incidents, security incidents

INTRODUCTION

It seems like every few weeks there is a report of a new data incident having taken place: recent high-profile examples include FedEx (February 2018), Under Armour/MyFitnessPal (March 2018), Panera Bread (April 2018), Adidas (June 2018), MyHeritage (June 2018), Macy's (July 2018), Timehop (July 2018), Reddit (August 2018) and T-Mobile (August 2018), just to name a few.

According to a 2017 BDO Cyber Governance Survey conducted in August 2017, more than three-quarters (79 per cent) of public company directors report their board is more involved with cybersecurity than it was in 2016.[1] 'The continuing year-over-year increases in board involvement and investments in cybersecurity is extremely positive, but the percentage of businesses with breach response plans in place – although much improved from two years ago – is still far below where it needs to be,' Eric Chuang, managing director of cyber incident response at BDO USA, said in a statement. Organisations are not the only ones falling victims to ransom cyber-attacks, as shown by the recent attack against the city of Atlanta.[2] In addition, unless you have been living out in a distant, remote planet in a galaxy far, far away, you have probably heard a lot about the new European General Data Protection Regulation (the 'GDPR') and the fact that it has already entered into effect (on 25th May, 2018). In particular, article 32 of the GDPR specifically requires organisations to 'implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk', which the GDPR expressly mentions includes 'the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services' and 'the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident'.[3]

So, what should organisations do in relation to cybersecurity incidents? More specifically, what can happen when the board or senior management is not appropriately engaged nor response plans properly practiced or otherwise followed? What can we learn from previous security incidents that have taken place?

Let us look at some real-world cases of what can happen following a security incident. This paper does not intend to cover every major data breach incident (there are just too many of them and many are unreported); rather it focuses on some of the largest incidents to try to find lessons that can be learned.

Please note that this paper also does not intend to second-guess decisions that were taken during a period of crisis with little time to weigh the pros and cons (that would be unfair especially due to the time pressure and the benefit of hindsight). Likewise, the purpose is not to criticise or bash any organisation for a data incident having taken place, but rather to provide real-world illustrations as to what may happen when a data incident takes place so that others may learn from such incidents.

DIXONS CARPHONE (2018)

On 13th June, 2018, British electrical and telecommunications retailer Dixons Carphone announced a hack of its systems in which at least 5.9m payment cards and 1.2m records containing non-financial personal data (such as name, address or e-mail address) may have been compromised.[4] The company indicated that approximately 105,000 non-EU issued payment cards, which do not have chip and pin protection, have been compromised, and the relevant card companies were subsequently notified so that they could take the appropriate measures to protect customers. Shortly thereafter, the National Cyber Security Centre announced that it is working with Dixons Carphone and other agencies to understand how this data breach has affected people in the UK and advise on mitigation measures.[4,5] On 31st July, 2018, Dixons announced that their investigation had identified that approximately 10m records containing personal data may have been accessed.[6]

Fallout

The Information Commissioner's Office (ICO) announced that it is liaising with the National Cyber Security Centre, the Financial Conduct Authority and other relevant agencies to ascertain the details and impact on customers.[7] On 31st July, 2018, the ICO noted that the number of affected records is 'significantly higher than initially stated' and that they 'will take time to assess this new information'.[8]

This is not the first time that the company has been investigated following a data breach: in February 2018, the ICO had already issued a fine of £400,000 against the company,[9] one of the largest fines issued by the ICO, for an earlier data breach that took place in 2015 and which led to the personal data of over 3m customers and 1,000 employees to be compromised. At the time, the ICO found that the company had seriously contravened the Seventh Principle in the UK's Data Protection Act 1998, which states that 'appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data'.[10] The maximum fine available to the ICO is £500,000 under such privacy law, whereas the maximum amount has substantially increased recently following the entry into force of the GDPR.

Lesson learned

While not all businesses hold millions of customer records, they all need to be prepared to face a cyber event. Notifying the relevant data protection authority – which under the European GDPR must be done within 72 hours of discovering a breach – is crucial.

TSB (2018)

When British retail bank TSB was acquired by Spanish bank Sabadell in 2015, it outlined its plans to move TSB's IT systems, which were hosted by Lloyds, to its own in-house core banking platform, Proteo. On 19th April, TSB announced through its Twitter feed that it would be upgrading its online systems between Friday 20th and Sunday 22nd April, 2018.[11] The company warned customers that some services, such as online banking, would not be possible during the two-day upgrade period; however, once the scheduled downtime was over, customers complained that they were still unable to access their accounts or to make any payments. According to news reports, up to 1.9m customers lost access[12] to online banking services, with some being locked out of their accounts and experiencing money disappearing from accounts. Six days after the incident first arose, customers were still reporting facing issues with online banking and TSB hired IBM to help resolve the issues. Some customers complained that they were unable to login to their online banking account for eight weeks.[13]

Fallout

After TSB called IBM to help resolve the issues,[14] Reuters reported that IBM's 'early findings' concluded that testing was relatively quick, did not show sufficient evidence of the system's capacity and did not apply the criteria needed to prove it was ready.[15] It further quoted IBM's report as stating the following: 'In a similar situation when IBM partnered with a financial organisation to migrate to a new core banking platform ... multiple trial migrations were conducted, rolled back and then remediated prior to launch.' It appears that TSB lost 12,500 customers in the aftermath of the IT failure.[16]

The reported issues with online banking have also attracted scrutiny from regulators. In addition to the UK's ICO,[17] the Financial Conduct Authority (FCA) is said to have already confirmed to be investigating the issue.[18] On 2nd May, TSB's chief executive appeared in front of the Parliament's Treasury Select Committee, where he was grilled about when normal service will resume for its customers.[19] MPs stated that they had 'lost confidence' in TSB's chief executive as a result of the IT issues and questioned whether he should remain in his post.[20] Nicky Morgan, chair of the Treasury Select Committee, further stated: 'I am deeply concerned by TSB's poor communications about the scale and nature of the problems it has faced; by its response to customer fraud; and by the quality and accuracy of the oral and written evidence provided.'[21]

Lesson learned

It is crucial to always be open and transparent about issues with the regulators and the public as a crisis unfolds. In addition, trial migrations should always be performed before deploying any updates or rollouts of a new system or software.

ORBITZ (2017)

Orbitz, a subsidiary of online travel agency Expedia, announced in March 2018 that hackers may have accessed personal information used to book travel through the site and other companies serviced by Orbitz. According to the company's official statement,[22] the investigation showed that the breach may have occurred between 1st January, 2016 and 22nd December, 2017 for its partner platform and between 1st January, 2016 and 22nd June, 2016 for its consumer platform. Orbitz determined that the personal information that was likely to have been accessed may have included full name, payment card information, date of birth, phone number, e-mail address, physical and/or billing address and gender. No evidence was found of unauthorised access to other types of personal information, including passport, social security numbers and travel itinerary information, however.

Fallout

According to media reports, about 880,000 payment cards may have been compromised.[23]

Lesson learned

This incident highlights the importance of updating or replacing outdated legacy systems as they can present significant security risks. A lot of organisations combine new and old IT systems in order to make use of new technologies, but maintaining legacy systems as the foundation without updating and securing them could be an easy target for hackers.

UBER (2017)

In November 2017, it was revealed that hackers had stolen 57m driver and rider accounts (including phone numbers, e-mail addresses and names) from Uber and that the company had kept the data breach secret for more than a year after paying a US$100,000 ransom.[24] According to Bloomberg, Uber's 2016 breach occurred when hackers discovered that the company's developers had published code that included their usernames and passwords on a private account of the software repository Github.[25] Those credentials gave the hackers immediate access to the developers' privileged accounts on Uber's network, and with it, access to sensitive Uber servers hosted on Amazon's servers, including the rider and driver data.

Fallout

Uber's handling of the hacking raised questions of a cover-up and a lack of transparency. Uber's chief security officer was asked to resign while an in-house information security attorney was fired following the incident. According to media reports, the hacking is the subject of at least four lawsuits, with Attorneys General in five states (New York, Connecticut, Illinois, Massachusetts and New Mexico) investigating whether Uber broke state laws on data-breach notifications.[26] In addition, the United States Attorney for the Northern District of California has begun a criminal investigation into the matter. It was also reported that the Pennsylvania attorney general has filed a lawsuit against Uber for violating the state's data breach notification law, which says hacks should be disclosed within a 'reasonable' time frame.[27] Regulators in the UK, Australia and the Philippines are also said to be looking into the matter.[28]

Uber had previously entered into a settlement agreement with the Federal Trade Commission (FTC) in August 2017,[29] where it agreed to implement a comprehensive privacy programme and obtain regular, independent audits. Following the revelation of this data breach, Uber agreed in April 2018 to expand the settlement it reached with the FTC, whereby the new provisions in the revised settlement include, among others, requirements for Uber to submit to the commission all the reports from the required third-party audits of Uber's privacy programme. 'After misleading consumers about its privacy and security practices, Uber compounded its misconduct by failing to inform the Commission that it suffered another data breach in 2016 while the Commission was investigating the company's strikingly similar 2014 breach,' said Acting FTC Chair Maureen K. Ohlhausen.[30] 'The strengthened provisions of the expanded settlement are designed to ensure that Uber does not engage in similar misconduct in the future.'

Uber also had to face a US Senate hearing on 6th February, 2018. Lawmakers, consumer groups and security researchers at the hearing said that paying uninvited cybercriminals was giving in to extortion, and it was a mistake by the company to pay up. Senator Richard Blumenthal said that Uber engaged in 'a form of obstruction of justice' and suggested that Uber's actions could constitute aiding and abetting the hackers.[31]

Lesson learned

Upon learning that it suffered a potential breach, an organisation should immediately hire outside counsel to lead an investigation. This would ensure that it is advised of the applicable notification laws and liability schemes in the relevant jurisdictions. Such investigation would examine the causes and effects of the breach and determine whether notification to regulators or consumers is required. In addition, if one decides to pay a ransom, it is best to be transparent about it.

DELOITTE (2017)

In September 2017, it was revealed that Deloitte had suffered a cyber-attack that resulted in the theft of confidential information, including the private e-mails and documents of some clients. Deloitte issued a statement on the topic and stated that 'very few' clients were affected,[32] whereas some reports indicate that 'as many as 350 clients' may have been impacted.[33] According to the *Guardian*, on 27th April, Deloitte hired the law firm Hogan Lovells on 'special assignment' to review what it called 'a possible cybersecurity incident'. It appears that the attackers used an admin account hosted on Microsoft's Azure cloud that was only secured with a single password and did not have two-factor authentication enabled. Not much information has been made public regarding this data incident.

Fallout

The New York State Attorney General's office is said to be investigating the breach, and there has been a lot of media attention surrounding the incident.

Lesson learned

Be accurate about the details of a breach in your press release, since all information disclosed will come under scrutiny. In particular, any indication on the number of individuals affected will be scrutinised if that number were to change further down the lane.

EQUIFAX (2017)

In September 2017, Equifax announced a cybersecurity breach, which it claims to have occurred between mid-May and July 2017, where cybercriminals accessed approximately 145.5m[34] US Equifax consumers' personal data, including their full names, social security numbers, birth dates, addresses and, in some cases, driver licence numbers.

Equifax also confirmed at least 209,000 consumers' credit card credentials were affected. Equifax took 40 days to report the breach. In February 2018, it was revealed in a document submitted by Equifax to the US Senate Banking Committee that the hackers accessed more personal information than the company previously disclosed,[35] such as tax identification numbers, e-mail addresses and driver's licence information beyond the licence numbers it originally disclosed.

Fallout

In October 2017, Equifax former CEO Richard Smith (together with former Yahoo Chief Executive) had to take the stand at a senate hearing and testify.[36] In January 2018, two senators proposed to introduce 'massive and mandatory' fines for data breaches at Equifax and other credit reporting companies, starting at US$100 for each consumer whose sensitive information is compromised.[37]

Lesson learned

The size of the Equifax breach (more than half of the US adult population affected), coupled with the sensitivity of the affected data and the 40 days it took in alerting the public is at the centre of public attention. The company blamed vulnerabilities in a 'web application', even though a software fix was available and the issue was presumably known to Equifax as it played a role in an earlier breach. Equifax response to the breach also left lots of consumers confused. Proper communication in the aftermath of a data breach is vital.

YAHOO! (2016)

Yahoo reported two major hacks compromising user account data in 2016. The first announced breach, reported in September 2016, had occurred sometime in late 2014, and affected over 500m Yahoo! user accounts.[38] A separate data breach, occurring earlier around August 2013, was reported in December 2016 and affected more than 1bn accounts.[39]

The hack exposed user account information, which includes name, e-mail address, hashed passwords, birthdays, phone numbers and, in some cases, 'encrypted or unencrypted security questions and answers', the company said back in 2016.[40] At the time, media reports described this as 'the biggest data breach in history'.[41] In October 2017, Yahoo stated that all 3bn of its user accounts were actually affected, breaking its own record for largest ever potential data breach.[42]

Fallout

The data breach affected Yahoo's purchase price; it was acquired by Verizon Communications for US$4.48bn, down US$350m from Verizon's initial offer due to the severity of the hacks.[43] The deal was delayed as the companies assessed the extent of the breach. The US Securities and Exchange Commission opened an investigation into whether Yahoo should have informed shareholders about the incident sooner.[44]

In October 2017, former Yahoo Chief Executive Marissa Mayer (together with Equifax's former CEO) testified before the US Senate.[45] In March 2018, Yahoo agreed to pay US$80m to settle a class action brought by investors who alleged that the company intentionally misled them about its cybersecurity practices.[46] On 24th April, 2018, the US Securities and Exchange Commission announced that Yahoo agreed to pay a US$35m penalty to settle charges that it misled investors by failing to disclose one of the world's largest data breaches.[47] On 12th June, 2018, the UK's ICO issued a fine of £250,000 against Yahoo's UK office.[48] The fine, which was levied against Yahoo's UK office rather than its global parent company, related specifically to the organisation's failure to protect the 515,000 UK-based accounts. The ICO warned that since the incident took place, the law had changed and is now stricter with the European GDPR in effect, thus future enforcement actions are likely to be stricter and bigger fines may be issued.

Lesson learned

According to reports, Yahoo's information security department was marginalised and even referred to internally as the 'Paranoids'.[49] The board's Special Cybersecurity Review Committee noted that 'it appeared certain senior executives did not properly comprehend or investigate, and therefore failed to act sufficiently upon the full extent of knowledge known internally by the …information security team.'[50] If the initial attack had been taken seriously, the company could have reacted to subsequent breaches and quickly reported them.

MORRISONS (2014)

An employee leaked payroll data of nearly 100,000 staff, including names, addresses, bank account details and salaries.[51] Earlier in the year he had been subject to disciplinary action, which led him to harbour a grudge against his employer. According to reports, the breach cost the company more than £2m in professional and legal fees.

Fallout

A group of former and current employees brought a suit against Morrisons in the English courts, alleging breaches of the Data Protection Act as well as breach of confidence and misuse of private information. On 1st December, 2017, the High Court of England and Wales ruled that while Morrisons was not directly liable for the data breaches and had taken appropriate technical and organisational measures, vicarious liability could be imposed on the employer in relation to the actions of the employee for actions 'committed in the conduct of his employment' since the data was entrusted to such employee during his employment.[52] It appears, however, that there was little Morrisons could have done differently to have prevented what happened in light of what the rogue employee was employed to do.

Lesson learned

An employer may be held vicariously liable for a deliberate data breach carried out by a rogue employee, out of working hours, at home on a personal computer. It is crucial for organisations to enforce the principle of least privilege to minimise the data that may be accessed by employees.

FEDEX (2018)

On 5th February, 2018, it was discovered that over 119,000 files relating to FedEx clients in the USA, Asia, Australia, Europe and the Middle East (such as passports, driving licences, security IDs, etc.) have been exposed after an unsecured Amazon Web Services (AWS) S3 storage server was found open to public access without a password.[53] The leaks came from a server associated with Bongo, a shipping calculation company purchased by FedEx back in 2014. The data appears to cover the period from 2009 to 2012, that is, before the FedEx acquisition took place.

Lesson learned

This illustrates the importance of auditing digital assets when an organisation acquires another and ensuring that customer data is secured and properly stored before, during and after a merger/acquisition.

WANNACRY AND PETYA RANSOMWARE (2017)

The global Petya cyberattack had a significant financial impact on victim companies; as the attack affected key IT systems, employees were forced to revert to paper and pen and use their own mobile phones.

Fallout

Maersk, the world's largest container ship and supply vessel operator, is said to have lost up to US$300m in lost revenues.[54] Falling victim to the Petya cyberattack cost FedEx around US$300m according to the company's earnings report.[55] Mondelez International, the world's second-largest confectionary company, said its second-quarter revenue growth would be reduced by 3 per cent, which some observers have estimated amount to about US$100m.[56] French car manufacturer Renault and German railway firm Deutsche Bahn were other high-profile victims in Europe. In the UK, the National Health Service was severely hit: at least 6,900 NHS appointments were cancelled as a result of the ransomware.[57] A report from the National Audit Office (NAO) found that the NHS could have prevented the attack had it followed recommendations:[58] the Department of Health was warned about the risks of cyberattacks on the NHS a year before WannaCry and that it was essential to patch or migrate from vulnerable older software. In addition, the report found that a cyberattack response plan was available, which included roles and responsibilities of national and local organisations for responding to an attack, but the plan was not tested at a local level. Due to the lack of rehearsal, it was not immediately clear who should lead the response and there was a breakdown in communications. The NHS determined that it needed to have an alternative communication channel for when systems are shut down; communications failures and the use of alternative channels should have been practiced previously.

The fallout from WannaCry is still far from over. In March 2018, aircraft manufacturing company Boeing was reportedly hit by the WannaCry ransomware, which affected its systems.[59] More recently, semiconductor manufacturer TSMC was the victim of a 'computer virus outbreak', which affected a number of computer systems and caused 'shipment delays and additional costs'. [60] According to media reports, the virus that brought down its semiconductor fabrication plants was a variant of WannaCry.[61] The company has announced that it expects that 'the impact to third quarter revenue to be about three percent, and impact to gross margin to be about one percentage point.'[62]

Lesson learned

It is crucial to migrate away from old software (such as Windows XP) and to consistently patch operating systems and applications in order to avoid known vulnerabilities.

CONCLUSION

As data breaches become increasingly sophisticated, it is becoming increasingly difficult, if not impossible, to ensure that a data breach does not occur. If recent data breaches have taught us anything, it is that any organisation is susceptible to a cyberattack; and organisations should be prepared to face such an event. The global outbreaks of WannaCry and NotPetya are powerful demonstrations of what can happen when organisations are not sufficiently prepared for an attack. Nevertheless, the future is not all gloom and doom. We have learned a number of important lessons from past incidents to help ensure that the same thing does not happen again. Rehearsals of incident response plans are essential to ensure everyone knows in advance what their role is and how to escalate and otherwise to communicate properly and respond. A company can have a seemingly perfect plan on paper, but if there are no clear and effective policies in place, then it may be rendered meaningless.

While the next victim of a cyber-attack may be unknown, it is increasingly clear that data breaches are inevitable.

References

1. '2017 BDO Cyber governance survey', available at: https://www.bdo.com/insights/assurance/corporate-governance/2017-bdo-board-survey/2017-bdo-cyber-governance-survey (accessed 20th August, 2018).
2. 'Cities held for ransom – Lessons from Atlanta's cyber extortion', *Forbes*, 2nd April, 2018, available at: https://www.forbes.com/sites/dantedisparte/2018/04/02/cities-held-for-ransom-lessons-from-atlantas-cyber-extortion/#16d018465996 (accessed 20th August, 2018).
3. GDPR, Article 32, 'Security of processing'.
4. 'Investigation into unauthorised data access', Dixons Carphone Press Release, 13th June, 2018, available at: https://www.dixonscarphone.com/~/media/Files/D/Dixons-Carphone/documents/pr-investigation-into-unauthorised-data-access.pdf (accessed 20th August, 2018).
5. 'Statement: Dixons Carphone data breach', National Cyber Security Centre, 13th June, 2018available at: https://www.ncsc.gov.uk/news/statement-dixons-carphone-data-breach (accessed 20th August, 2018).
6. 'Update on investigation into unauthorised data access', Dixons Carphone, 31st July, 2018, available at: http://www.dixonscarphone.com/~/media/Files/D/Dixons-Carphone/documents/dixons-carphone-update-on-unauthorised-data-access.pdf (accessed 20th August, 2018).
7. 'ICO statement in response to Dixons Carphone breach announcement', Information Commissioner's Office, Press Release, 13th June, 2018, last updated on 31st July, 2018, available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/07/ico-statement-in-response-to-dixons-carphone-breach-announcement/ (accessed 20th August, 2018).
8. Ibid.
9. 'Carphone Warehouse fined £400,000 after serious failures placed customer and employee data at risk', Information Commissioner's Office, Press Release, 10th January, 2018, available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/01/carphone-warehouse-fined-400-000-after-serious-failures-placed-customer-and-employee-data-at-risk/ (accessed 20th August, 2018).
10. See: Schedule 1 of the Data Protection Act 1998, available at: http://www.legislation.gov.uk/ukpga/1998/29/schedule/1/enacted (accessed 20th August, 2018).
11. 'TSB: How it all went so wrong for the bank', BBC News, 28th April, 2018, available at: https://www.bbc.com/news/business-43923561 (accessed 20th August, 2018).
12. 'TSB customers still unable to access accounts four weeks after "glitch"', *The Guardian*, 20th May, 2018, available at: https://www.theguardian.com/business/2018/may/20/tsb-customers-still-unable-to-access-accounts-four-weeks-after-glitch (accessed 20th August, 2018).
13. 'TSB crisis continues eight weeks on', BBC News, 12th June, 2018, available at: https://www.bbc.com/news/business-44454314 (accessed 20th August, 2018).
14. 'TSB chaos: "We are on our knees," says boss', BBC News, 26th April, 2018, available at: https://www.bbc.co.uk/news/business-43904267 (accessed 20th August, 2018).
15. 'TSB's testing of new IT platform was inadequate — IBM report', Reuters, 21st June, 2018, available at: https://uk.reuters.com/article/uk-britain-tsb-ibm/tsbs-testing-of-new-it-platform-was-inadequate-ibm-report-idUKKBN1JH12D (accessed 20th August, 2018).
16. 'TSB loses 12,500 customers in wake of IT failure', *The Independent*, 6th June, 2018, available at: https://www.independent.co.uk/news/business/news/tsb-it-failure-latest-fraud-attempts-thousands-online-banking-paul-pester-a8386271.html (accessed 20th August, 2018).
17. 'ICO and finance regulator assess TSB IT blunder', *Computer Weekly*, 24th April, 2018, available at: https://www.computerweekly.com/news/252439781/ICO-and-finance-regulator-assess-TSB-IT-blunder (accessed 20th August, 2018).
18. 'TSB investigated over IT meltdown', BBC News, 6th June, 2018, available at: https://www.bbc.co.uk/news/business-44370802 (accessed 20th August, 2018).
19. 'TSB chief executive Paul Pester grilled by MPs', BBC News, 2nd May, 2018, available at: https://www.bbc.com/news/av/business-43977692/tsb-chief-executive-paul-pester-grilled-by-mps (accessed 20th August, 2018).
20. 'MPs have "lost confidence" in TSB chief', BBC News, 7th June, 2018, available at: https://www.bbc.com/news/business-44404043 (accessed 20th August, 2018).
21. 'Nicky Morgan "deeply concerned by TSB's poor communications"', Parliament UK, 7th June, 2018, available at: https://www.parliament.uk/business/committees/committees-a-z/commons-select/treasury-committee/news-parliament-2017/tsb-sabadell-fca-letters-17-19/ (accessed 20th August, 2018).
22. 'Information about Orbitz data security incident', Orbitz, available at: https://orbitz.allclearid.com/additionalinformation.html (accessed 20th August, 2018).
23. 'Orbitz hack may have compromised 880,000 credit cards', Bloomberg, 20th March, 2018, available at: https://www.bloomberg.com/news/articles/2018-03-20/expedia-s-orbitz-hack-may-have-compromised-880-000-credit-cards (accessed 20th August, 2018).
24. 'Hack brief: Uber paid off hackers to hide a 57-million user data breach', Wired, 21st November, 2017, available at: https://www.wired.com/story/

uber-paid-off-hackers-to-hide-a-57-million-user-data-breach/ (accessed 20th August, 2018).

25. 'Uber paid hackers to delete stolen data on 57 million people', Bloomberg, 22nd November, 2017, available at: https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data (accessed 20th August, 2018).
26. 'Uber is sued over massive data breach after paying hackers to keep quiet', *Washington Post*, 24th November, 2017, available at: https://www.washingtonpost.com/news/the-switch/wp/2017/11/24/uber-is-sued-over-massive-data-breach-after-paying-hackers-to-keep-quiet/?noredirect=on&utm_term=.8d84a2fce7f6 (accessed 20th August, 2018).
27. 'Uber "surprised" by totally unsurprising Pennsylvania data breach lawsuit', Wired, 3rd May, 2018, available at: https://www.wired.com/story/uber-pennsylvania-data-breach-lawsuit/ (accessed 20th August, 2018).
28. 'Uber breach, cover up trigger government probes around the globe', Reuters, 23rd November, 2017, available at: https://www.reuters.com/article/uber-cyberattack/uber-breach-cover-up-trigger-government-probes-around-the-globe-idUSL1N1NS189 (accessed 20th August, 2018).
29. 'Uber settles FTC allegations that it made deceptive privacy and data security claims', Federal Trade Commission, Press Release, 15th August, 2017, available at: https://www.ftc.gov/news-events/press-releases/2017/08/uber-settles-ftc-allegations-it-made-deceptive-privacy-data (accessed 20th August, 2018).
30. 'Uber agrees to expanded settlement with FTC related to privacy, security claims', Federal Trade Commission, Press Release, 12th April, 2018, available at: https://www.ftc.gov/news-events/press-releases/2018/04/uber-agrees-expanded-settlement-ftc-related-privacy-security (accessed 20th August, 2018).
31. 'Uber answers for data breach, alleged cover up in Senate probe', Bloomberg Law, 6th February, 2018, available at: https://www.bna.com/uber-answers-data-n57982088428/ (accessed 20th August, 2018).
32. 'Deloitte hacked, says "very few" clients affected', Reuters, 25th September, 2017, available at: https://www.reuters.com/article/us-deloitte-cyber/deloitte-hacked-says-very-few-clients-affected-idUSKCN1C01PB (accessed 20th August, 2018).
33. 'Deloitte hack hit server containing emails from across US government', *The Guardian*, 10th October, 2017, available at: https://www.theguardian.com/business/2017/oct/10/deloitte-hack-hit-server-containing-emails-from-across-us-government (accessed 20th August, 2018).
34. 'Equifax announces cybersecurity firm has concluded forensic investigation of cybersecurity incident', Equifax News, 2nd October, 2017, available at: https://investor.equifax.com/news-and-events/news/2017/10-02-2017-213238821 (accessed 20th August, 2018).
35. 'Equifax hack might be worse than you think', *Wall Street Journal*, 9th February, 2018, available at: https://www.wsj.com/articles/equifax-hack-might-be-worse-than-you-think-1518191370 (accessed 20th August, 2018).
36. 'Former Equifax CEO Richard Smith: "I am deeply sorry"', *CNN Money*, 2nd October, 2017, available at: http://money.cnn.com/2017/10/02/news/companies/equifax-smith-cyber-breach-apology/index.html (accessed 20th August, 2018).
37. See: https://www.sfgate.com/business/article/Senators-want-massive-fines-for-data-12488940.php or https://compliancex.com/senators-want-massive-fines-data-breaches-equifax-credit-reporting-firms/ (accessed 20th August, 2018).
38. 'Yahoo says hackers stole data on 500 million users in 2014', *The New York Times*, 22nd September, 2016, available at: https://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html (accessed 20th August, 2018).
39. Yahoo says 1 billion user accounts were hacked, *The New York Times*, 14th December, 2016, available at: https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html (accessed 20th August, 2018).
40. After massive Yahoo hack, a new way to think about security questions, *The Daily Dot*, 24th September, 2016, available at: https://www.dailydot.com/layer8/security-questions-yahoo-hack/ (accessed 20th August, 2018).
41. 'Yahoo experiences biggest data breach in history: 1 billion affected', WeLiveSecurity, 15th December, 2016, available at: https://www.welivesecurity.com/2016/12/15/yahoo-experiences-biggest-data-breach-history-1-billion-affected/ (accessed 20th August, 2018).
42. 'Yahoo tops the list of largest ever data breaches', *CNN Money*, 4th October, 2017, available at: http://money.cnn.com/2017/10/04/technology/yahoo-biggest-data-breaches-ever/index.html (accessed 20th August, 2018).
43. 'After data breaches, Verizon knocks $350M off Yahoo sale, now valued at $4.48B', Techcrunch, 21st February, 2017, available at: https://techcrunch.com/2017/02/21/verizon-knocks-350m-off-yahoo-sale-after-data-breaches-now-valued-at-4-48b/ (accessed 20th August, 2018).
44. 'Yahoo says the SEC is investigating its recent data breaches', *Fortune*, 23rd January, 2017, available at: http://fortune.com/2017/01/23/yahoo-sec-data-breaches/ (accessed 20th August, 2018).
45. 'Former Yahoo CEO, Equifax CEO to testify at Senate hearing', Reuters, 2nd November, 2017, available at: https://www.reuters.com/article/us-usa-databreaches/former-yahoo-ceo-equifax-ceo-to-testify-at-senate-hearing-idUSKBN1D15X5 (accessed 20th August, 2018).
46. 'Yahoo agrees to pay $80m to settle securities fraud suit', Bloomberg Law, 6th March, 2018, available at: https://biglawbusiness.com/yahoo-agrees-to-pay-80m-to-settle-securities-fraud-suit/ (accessed 20th August, 2018).

47. 'Altaba, formerly known as Yahoo!, charged with failing to disclose massive cybersecurity breach; Agrees to pay $35 million', US Securities and Exchange Commission, Press Release, 24th April, 2018, available at: https://www.sec.gov/news/press-release/2018-71 (accessed 20th August, 2018).
48. 'Blog: Standing up for the data rights of our citizens - ICO fines Yahoo! UK Services Limited £250,000 after it failed to protect customers' personal data', Information Commissioner's Office, 12th June, 2018, available at: https://ico.org.uk/about-the-ico/news-and-events/standing-up-for-the-data-rights-of-our-citizens/ (accessed 20th August, 2018).
49. 'Marissa Mayer declined to reset Yahoo users' passwords 2 years ago', Naked Security, 28th September, 2016, available at: https://nakedsecurity.sophos.com/2016/09/28/marissa-mayer-declined-to-reset-yahoo-users-passwords-2-years-ago/ (accessed 20th August, 2018).
50. 'Yahoo hackers accessed 32 million accounts with forged cookies', Engadget, 3rd January, 2017, available at: https://www.engadget.com/2017/03/01/yahoo-hackers-accessed-32-million-accounts-with-forged-cookies/ (accessed 20th August, 2018).
51. 'Morrisons found liable for staff data leak in landmark ruling', *The Guardian*, 1st December, 2017, available at: https://www.theguardian.com/business/2017/dec/01/morrisons-liable-staff-data-leak-landmark-decision (accessed 20th August, 2018).
52. 'Vicarious liability in UK data breach-related litigation — is Morrisons a game-changer?', Data Protection Report, 4th December, 2017, available at: https://www.dataprotectionreport.com/2017/12/vicarious-liability-in-uk-data-breach-related-litigation-is-morrisons-a-game-changer/ (accessed 20th August, 2018).
53. 'What you need to know about the major FedEx data leak', Silicon Republic, 16th February, 2018, available at: https://www.siliconrepublic.com/enterprise/fedex-data-leak-amazon (accessed 20th August, 2018).
54. 'Petya ransomware: Cyberattack costs could hit $300m for shipping giant Maersk', ZD Net, 16th August, 2017, available at: https://www.zdnet.com/article/petya-ransomware-cyber-attack-costs-could-hit-300m-for-shipping-giant-maersk/ (accessed 20th August, 2018).
55. 'NotPetya cyber attack on TNT Express cost FedEx $300m', ZD Net, 20th September, 2017, available at: https://www.zdnet.com/article/notpetya-cyber-attack-on-tnt-express-cost-fedex-300m/ (accessed 20th August, 2018).
56. Malware may have cost Mondelez $100 million, *Food Processing*, 6th November, 2017, available at: https://www.foodprocessing.com/articles/2017/malware-may-have-cost-mondelez-millions/ (accessed 20th August, 2018).
57. 'NHS was crippled by "unsophisticated" cyber attack', Pharmafile, 27th October, 2017, available at: http://www.pharmafile.com/news/515500/nhs-was-crippled-unsophisticated-cyber-attack (accessed 20th August, 2018).
58. 'Investigation: WannaCry cyber attack and the NHS', National Audit Office, 27th October, 2017, available at: https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/ (accessed 20th August, 2018).
59. 'Boeing reportedly hit by Wannacry ransomware', Techcrunch, 29th March, 2018, available at: https://techcrunch.com/2018/03/28/boeing-reportedly-hit-by-wannacry-ransomware/ (accessed 20th August, 2018).
60. 'TSMC details impact of computer virus incident', TSMC, Press Release, 5th August, 2018, available at: http://www.tsmc.com/tsmcdotcom/PRListingNewsAction.do?action=detail&newsid=THHIANTHTH&language=E (accessed 20th August, 2018).
61. 'TSMC says variant of WannaCry virus brought down its plants', ZDNet, 6th August, 2018, available at: https://www.zdnet.com/article/tsmc-says-variant-of-wannacry-virus-brought-down-its-plants/ (accessed 20th August, 2018).
62. TSMC, ref. 61 above.