Global FINEX - Professional Indemnity Insurance

The impact of the pandemic on data breaches reported by the Legal Sector

November 2021

Introduction

The last 18 months saw law firms quickly adapting their IT infrastructures in response to the coronavirus (COVID-19). The Government imposed lockdown restrictions expedited any IT investment programmes to ensure businesses could support their entire workforce and their clients. With many of these changes expected to remain post pandemic and it is envisaged that the use of artificial intelligence (AI) and emerging technologies are increasingly being used by all businesses, not just the legal sector[1] it is inevitable that the security of data will be vulnerable to the threats from cyber criminals but also as a result of human error.

With the increase in reliance on IT and data breaches occurring frequently[2] the need to protect businesses, their staff and their clients from data breaches becomes of paramount importance. The latest report published by IBM suggests that during the pandemic the cost of a data breach hit record levels[3]. This article will examine the data breaches reported by the legal sector to the Information Commissioner's Office (ICO) during the pandemic.

Law firms handle financial transactions daily often involving large amounts of money and containing valuable sensitive client information and must satisfy both regulatory and legislative obligations in order to protect client monies, and to keep client affairs confidential[4]. They must report certain personal data breaches to the ICO within 72 hours of becoming aware of such breaches where feasible. The ICO publishes quarterly reports on data breaches that have been reported to them and this includes specific reports from the legal sector.

For the purpose of this article we will analyse the data breaches reported to the ICO from 1 March 2020 to 30 June 2021[5] which will cover the periods of the first lockdown in March 2020 through to the start of restrictions being eased this summer. The ICO publish reports on a quarterly basis and are as follows:-

1. The Law Society. (2021). Future Worlds 2050: images of the future worlds facing the legal profession 2020-2030. Retrieved from: https://www.lawsociety.org.uk/topics/research/future-worlds-2050-images-of-the-future-worlds-facing-the-legal-profession-2020-2030?sc_camp=5C0FE0D28B474F6BA2EE374CB3EE601B
2. National Cyber Security Centre. (2021). Introducing data breach guidance for individuals and families. Retrieved from: https://www.ncsc.gov.uk/blog-post/introducing-data-breach-guidance-for-individuals-and-families and Department for Digital, Culture, Media & Sport (2021). Cyber Security Breaches Survey 2021. Retrieved from the Gov.UK's website: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/972399/Cyber_Security_Breaches_Survey_2021_Statistical_Release.pdf
3. IBM. (2021). How much does a data breach cost?. Retrieved from: https://www.ibm.com/uk-en/security/data-breach
4. Paragraphs 4.2 and 6.3 of the SRA Code of Conduct for Solicitors. Retrieved from: https://www.sra.org.uk/solicitors/standards-regulations/code-conduct-solicitors/ and paragraphs 5.2 and 6.3 of the SRA Code of Conduct for Firms. Retrieved from https://www.sra.org.uk/solicitors/standards-regulations/code-conduct-firms/
5. Information Commissioner's Office (n.d). Previous reports. Retrieved from: https://ico.org.uk/action-weve-taken/data-security-incident-trends/previous-reports/

Legal Sector Breaches reported during 1 March 2020 to 30 June 2021

The types of breaches reported to the ICO are categorised as:-

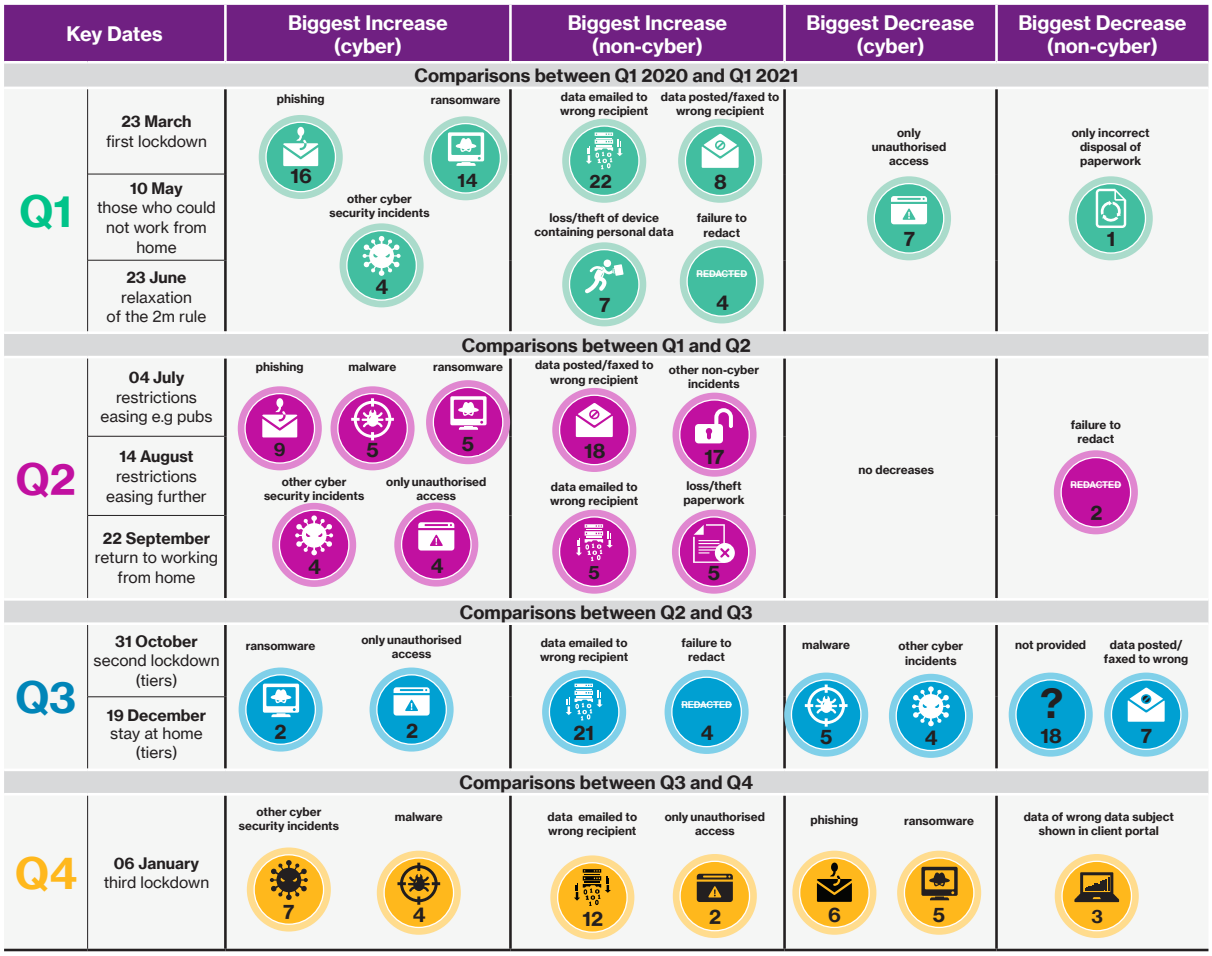
- **Cyber security incidents:** which mainly occur as a result of a cyber attack and include ransomware, phishing, malware attacks and unauthorised access. A total of 181 cyber security incidents were reported during this period.
- **Non cyber security incidents:** which mainly occur as a result of human error and includes data being emailed, posted or faxed to the wrong recipient, failure to redact and the loss or theft of paperwork or data left in an insecure location. A total of 472 non cyber security incidents were reported during this period.

The below diagram summarises the analysis of the types of breaches reported to the ICO during the periods from Q1 2020 through to Q1 2021 and the volume looking first at breaches as a result of cyber attacks followed by the breaches resulting from non cyber related incidents.

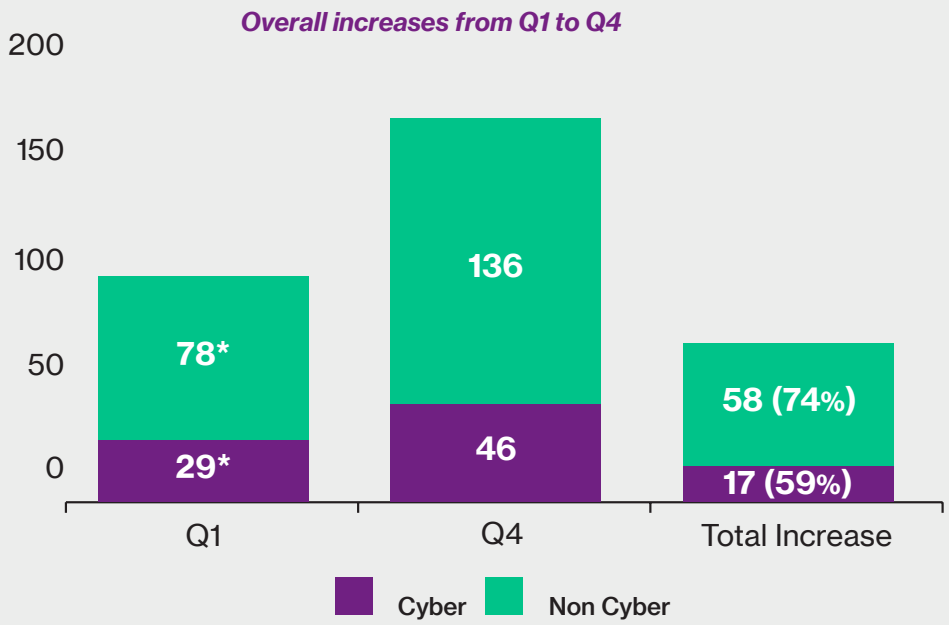
An analysis of reported data breaches 2020-2021

This data covers the data breaches reported to the ICO from 01 March 2020 to 30 June 2021 which includes the first lockdown in March 2020 through to the start of restrictions being eased during June and July 2021.

The diagram identifies both the areas of biggest difference and the size of the difference. The highlighted numbers compare the difference in the volume of cases from 2020-2021 for the relevant quarter.



Key: Q1: 01 April - 30 June Q2: 01 July - 30 September Q3: 01 October - 31 December Q4: 01 January - 31 March



* These figures are based on the registered completion date of incidents rather than when they were notified to the ICO the source for this is https://ico.org.uk/action-weve-taken/data-security-incident-trends/previous-reports/

Cyber security incidents

During the pandemic the number of cyber security breaches increased by 117% with phishing attacks and ransomware attacks being the most common.

The biggest increase arose during Q1 2020 and Q2 2020 which could arguably be as a result of people transitioning from physically working in the office to working remotely following the lockdown restrictions imposed by the UK Government on 23 March 2020.

Ransomware attacks increased fivefold during 1 July 2020 and 30 September 2020 (Q2 2020). This was unsurprising as law enforcement agencies had predicted an increased threat of COVID-19 cyber activity involving ransomware attacks as cyber criminals took advantage of the pandemic. In recognition of such threats the Ransomware Task Force was introduced to develop a comprehensive framework for tackling the global ransomware threat[6].

Phishing attacks increased overall by 76% with the largest rise occurring during 1 July 2020 and 30 September 2020 (42%).

The increase in cyber related incidents was reflective of the warnings about cyber criminals taking advantage of all businesses who were increasingly working under extreme pressure and were doing so remotely, which for many was a new concept. Interestingly during the last two quarters of the 2020 reporting period the numbers of incidents reported from these threats decreased, which may suggest that people were adapting to new working practices and a greater cyber risk awareness.

Phishing attacks increased overall by 76% with the largest rise occurring during 1 July 2020 and 30 September 2020 (42%).

6. National Cyber Security Centre. (2021). Ransomware Taskforce (RTF) announce framework to combat ransomware. Retrieved from: https://www.ncsc.gov.uk/blog-post/ransomware-taskforce-rtf-announce-framework-to-combat-ransomware

Non cyber security incidents

Looking at the non cyber security incidents reported to the ICO during Q1 2020 to Q1 2021 the numbers of such breaches reported by the legal sector during the pandemic rose by 73%. The largest increase arising out of incidents from the loss or theft of devices containing personal data, which increased by 350% (increased from 2 incidents to 9). This was followed by data incidents arising from emails being sent to the wrong recipient which increased by 81%. Failure to redact also saw a significant increase in reported incidents (50%), followed by data posted or faxed to incorrect recipient breaches which rose by 40%. It was noted that there was a sharp increase in 'other non cyber related breaches' of 55%.

The largest increase for the above incidents arose during Q2 apart from breaches arising from emails being sent to the wrong recipient. These breaches increased by 66% in Q3 which was when the UK was moving in and out the three-tier system of COVID-19 restrictions, a second national lockdown being imposed and further tiered restrictions covering the Christmas period. It is arguable that focus during this time was more on trying to adjust to the various changes in restrictions and the disappointment of not seeing friends and family over the festive period rather than cyber security awareness which may have been the cause for the rise in such incidents occurring.

Summary

Despite the warnings from law enforcement and regulators around increased activity from cyber criminals the statistics indicate that there was an increase in cyber attacks during the pandemic. However, having analysed the data published by the ICO the majority of data breach reports made by the legal sector occurred as a result non cyber security incidents suggesting they arose due to human error.

As businesses and employees are returning to the office and starting to adapt to the 'new normal' in whatever form that may take, what is vitally important is that cyber criminals will be monitoring such activity. Cyber attacks are likely to continue, and people will make mistakes, especially as they are trying to deal with the impact the pandemic has had on both their working and personal lives.

However, there is no room for complacency and any poor practices that may have gone previously unnoticed over the last 18 months are likely to come to the fore. Now is a good time to ensure that everyone is reminded of their regulatory and legislative obligations around keeping client affairs confidential and provide everyone with regular and tailored training including senior management as this will reinforce the message about the seriousness of data breaches and businesses ability to react accordingly in the event of such incidents arising.

For further information please contact:

Joanne Cracknell MSc LLB (Hons)
Associate Director, FINEX Global
+44 117 976 9376
+44 7584 683 012
Joanne.Cracknell@WillisTowersWatson.com

Disclaimer

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 45,000 employees serving more than 140 countries and markets. We design and deliver solutions that manage risk, optimise benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas – the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

willistowerswatson.com/social-media

FPS2180189 WTW-FINEX 487402/11/21

willistowerswatson.com

Willis Towers Watson