

LEGAL 150 DATA BREACH REPORT



2022

Data Breaches reported to the ICO by the top 150 UK law firms

Three years on from GDPR coming into force we look at how many law firms have reported data breaches to the ICO, the nature of those breaches and any trends that are emerging.

Headline Numbers

28%

OF THE TOP 150 HAVE
REPORTED DATA
BREACHES

2020 Figure = 47%

84

DATA BREACHES
REPORTED

2020 Figure = 155

9%

BREACHES REPORTED
DUE TO FAILURE TO
REDACT

2020 Figure = 3%

40%

OF DATA BREACHES ARE
DUE TO EMAILING
WRONG RECIPIENT

2020 Figure = 23%

3

LAW FIRMS HAVE
REPORTED 5 OR MORE
BREACHES

2020 Figure = 4

8

HIGHEST NUMBER OF
BREACHES REPORTED
BY ONE LAW FIRM

2020 Figure = 13

Introduction

3 years on from the introduction of GDPR and there is yet to be a significant penalty awarded to a law firm. This may be because law firms have well organised Information Security practices and well-trained employees, or it could be blind luck and just a matter of time before a significant breach occurs. Either way, with client trust essential, the prospect of reputation damage is likely to be of greater concern to many than a financial penalty.

This report looks at data breaches reported to the ICO covering the period of January 2021 to January 2022 and using the statistics provided attempts to identify any clear trends or patterns by focussing on:

Law firm reporting statistics

Breach type statistics

We conclude the report with a reminder of the ICO's data breach preparation guidance.

THIS REPORT IS PROVIDED FREE OF CHARGE AND YOU ARE WELCOME TO USE ANY OF THE CONTENT - BUT IF YOU FIND IT USEFUL, WE ENCOURAGE MAKING A SMALL DONATION TO OUR LOCAL SHELTER CHARITY - <https://www.snowflake-nightshelter.org.uk/>

Data Considerations

Law Firm Information

Although the information sourced is publicly available, we have not included the names of the law firms as the purpose of this report is not to 'name and shame' but rather to act as a useful resource for firms highlighting vulnerable areas to keep a focus on.

We will however be happy to let you know the stats for your own firm if you contact us from an official email address.

Data Breach Information

It should be noted that the statistics provided by the ICO are for those firms that have **reported** data breaches which may not reflect **actual** data breaches.

There are a number of reasons that there could be a difference between the number of reported breaches and actual breaches including:

- **A Data Breach was known of and was correctly identified as not meeting ICO reportable criteria**
- **A Data Breach was known of but was incorrectly identified as not meeting ICO reportable criteria**
- **A Data Breach was known of but was deliberately not reported even though meeting ICO reportable criteria (unlikely to be the case for most professional organisations)**
- **A Data Breach occurred but was not known of**

It should also be remembered that the ICO figures may include Data Breaches that were not necessary to report.

Data Source

The data was provided by the Information Commissioner's Office (ICO) following a Freedom of Information (FOI) submission by 2twenty4 Consulting on 14 January 2022.

We asked for the following information:

details of all data breaches reported by the top 150 law firms from January 2021 to January 2022

- **the type of breach reported**
- **details of any action taken or advice given by the ICO**

The ICO responded within the allocated time allowed and provided all the statistical information included in this report.

The ICO declined to provide information as to the remedial advice it returned.



What is a Data Breach?

The term ‘Data Breach’ is often associated with the **loss of data** due to human error such as an email sent to the wrong person or a laptop left on public transport or possibly some form of hacker activity. This is however only one form of data breach known as a ‘**Confidentiality Breach**’. Two other less publicised but equally important forms of data breach are the ‘**Integrity Breach**’ and the ‘**Availability Breach**’.



An Integrity Breach occurs where the client’s personal data has not been lost or exposed and is readily available but has corrupted for some reason.

An Availability Breach occurs when data is not readily available, and a client suffers harm as a consequence. An increasingly common example of this is ransomware.

TYPE OF BREACH	EXAMPLE
Confidentiality Breach	The Document Store has been hacked by an external entity and data has been taken. An email containing medical records has been sent to the wrong client.
Integrity Breach	The data has been corrupted due to a failed restore process from backup.
Availability Breach	The Document Management System is down and a key date for document submission or court appearance is missed as a consequence.

NOTE – Any potential fine or sanction is equally applicable to all forms of breach.

For the third year running it appears that mainly data breaches of the ‘confidentiality breach’ type have been reported although 2021 sees Ransomware reports increasing which are likely to be ‘availability’ breaches.

Data Breach by Law firm

A few key statistics



	2019	2020	2021	% change
Number of law firms reporting breaches	74	71	42	- 40% ↓
Highest number of breaches by one firm	15	13	8	- 38% ↓
Law firms reporting 5 or more breaches	12	4	3	- 25% ↓
Law firms reporting 3 or more breaches	24	16	8	- 50% ↓

Top Reporters







RANK	LAST YEAR	FIRM	REPORTED BREACHES
=1	NE ↑	(firm name available on request)	8
=1	2 ↑	(firm name available on request)	8
=2	NE ↑	(firm name available on request)	7
=2	NE ↑	(firm name available on request)	7
=3	NE ↑	(firm name available on request)	4
=3	4 ↓	(firm name available on request)	4
=4	NE ↑	(firm name available on request)	3
=4	10 ↑	(firm name available on request)	3
=4	3 ↓	(firm name available on request)	3

Note – In all above cases of reported breaches no further action was required by the ICO.








It is a common assumption that the higher number of breaches reported the weaker the security is at the firm. This should be balanced however with the question as to whether reporting lower numbers (or none at all) means that no breaches occurred or that they have occurred, and the firm is simply unaware due to a lack of security monitoring functionality. As no law firm reported breaches have incurred any follow up action from the ICO (presumably because they were not serious or already handled appropriately) it may also be the case that the higher reporters simply have stronger or keener compliance cultures.

TRENDS

Top Breach Types Reported

RANK	LAST YEAR	BREACH TYPE
1	1 	Emailed to wrong recipient
2	2 	Mailed or Faxed to wrong recipient
3	NE 	Failure to Redact
4	6 	Ransomware
5	2 	Other Non-Cyber Incident
6	NE 	Unauthorised Access

Biggest changes

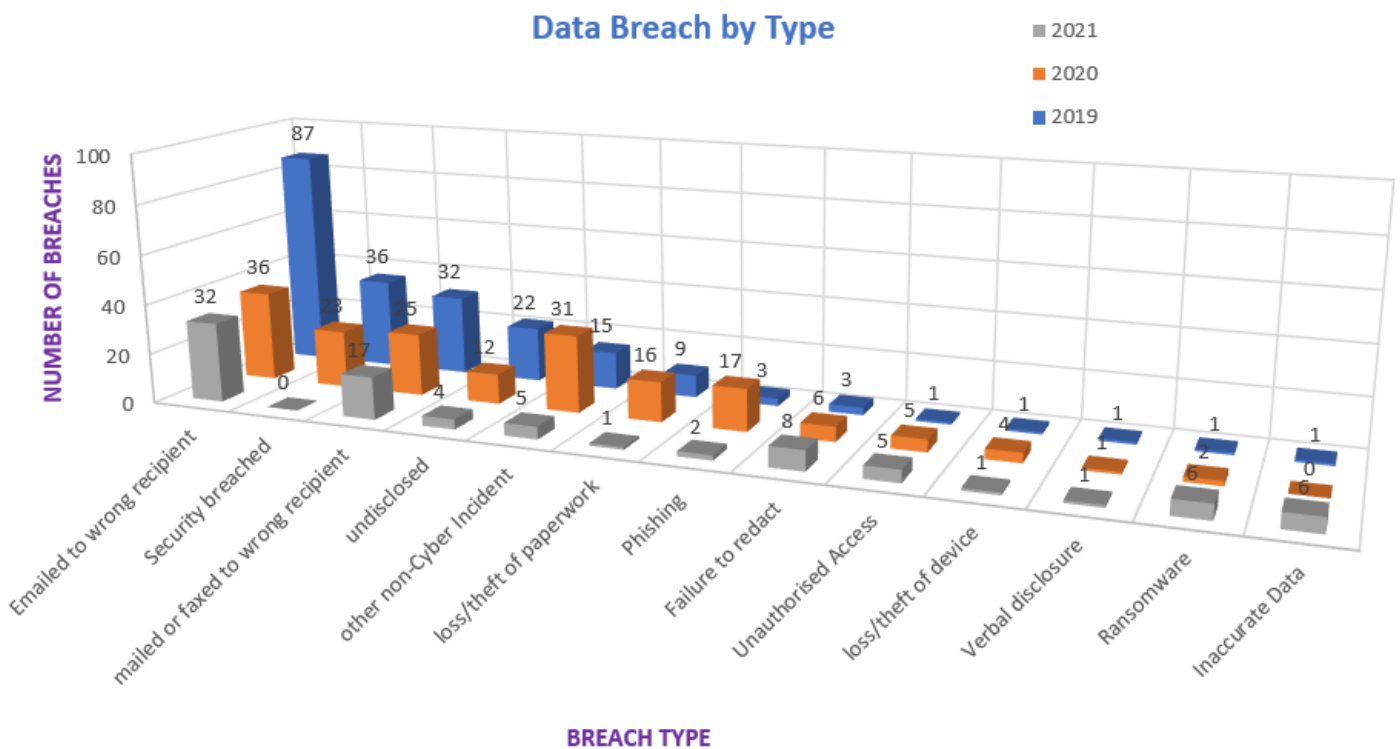
	2019	2020	% change
Ransomware	2	6	+200% 
Failure to Redact	6	8	+33% 
Security Breached	23	0	- 95% 
Loss or theft of paperwork	16	1	- 93% 
Phishing	17	2	- 88% 
Other Non-cyber incident	31	5	- 84% 
Loss or theft of device	4	1	- 75% 

Data Breach by Type

The analysis of data breaches by type is useful in that it may help determine which areas to focus attention on.

For the third year running 'Emailed to the wrong recipient' is the highest reported instance of a data breach.

A more interesting trend is the rise in those caused by 'ransomware' and 'failure to redact'.





Does the relatively consistent breach of ‘emailed to the wrong recipient’ mean that preventative technology is a must in this area or that employees simply need to be more diligent?



Does the increase in ransomware breaches indicate more sophisticated phishing scams?



Does the increase in ‘failure to redact’ breaches indicate an increase in Subject Access requests?



Is the decrease in ‘loss or theft of paperwork’ breaches related to the significant increase in home working?



Is the elimination of ‘security breached’ an indication that the general law firm information security standards have significantly improved or are the ICO categorising these differently?



Data Breach Preparation

The ICO have produced the following guidance:


Preparing for a personal data breach

Preparing for a personal data breach

- We know how to recognise a personal data breach.
- We understand that a personal data breach isn't only about loss or theft of personal data.
- We have prepared a response plan for addressing any personal data breaches that occur.
- We have allocated responsibility for managing breaches to a dedicated person or team.
- Our staff know how to escalate a security incident to the appropriate person or team in our organisation to determine whether a breach has occurred.

Responding to a personal data breach

- We have in place a process to assess the likely risk to individuals as a result of a breach.
- We know who is the relevant supervisory authority for our processing activities.
- We have a process to notify the ICO of a breach within 72 hours of becoming aware of it, even if we do not have all the details yet.
- We know what information we must give the ICO about a breach.
- We have a process to inform affected individuals about a breach when it is likely to result in a high risk to their rights and freedoms.
- We know we must inform affected individuals without undue delay.
- We know what information about a breach we must provide to individuals, and that we should provide advice to help them protect themselves from its effects.
- We document all breaches, even if they don't all need to be reported.



Data Breach Register

The following is the detail to be recorded for all data breaches regardless of whether they are reported to the ICO.

Breach Description	Date of breach	Breach Effect	Remedial Action Taken	Date of remediation	Personal Data Affected	Number of data subjects affected	Number of personal data records affected	Name and contact of the [Relationship Owner]	Likely consequences of the Breach

Conclusions

This is the third year of statistics representing the enhanced data breach reporting requirements brought in by GDPR (and now the UK GDPR) and we are seeing trends demonstrating that overall law firms are reporting less breaches. It should be remembered that these statistics are for 'breaches reported' and whilst it could mean there are less data breaches occurring it could also mean that firms have matured their data protection understanding as to what needs to be reported. It could also mean that less breaches are being detected.

Statistics are of course open to interpretation and reason. It is likely that larger firms have higher security budgets and therefore stronger protections and the type of legal work processed could also be significant. Private client and medical negligence firms tend to be smaller and at the same time likely to process considerably more personal data. There will no doubt be other factors that also affect the numbers.

The analysis of types of breach presents no surprises with human error being the single significant cause and in particular emails to the wrong recipient although this does have a declining trend. The rise in ransomware is a likely indicator that law firms are being increasingly targeted which mirrors commentary from many InfoSec teams.

Another interesting question is whether working from home has had an impact. It is possible that less travel has helped reduce the 'lost paperwork/devices' stats over this period and many firms have used the opportunity to catch up on employee training. Conversely could the rise in ransomware attacks relate to lesser protected home devices and wifi?

As with all statistical analysis there are as many questions generated as answers but in our view the following are the key lessons learnt from the information provided:

Ensure you have a robust, effective and measured data protection training programme.

Your email activity is the most likely process to result in a data breach.

Keep Data Protection policies and employee guidance up to date and communicated.

Make it easy for employees to protect data.

Log all data breaches in a breach register.

DON'T FORGET PAPER

YOU DECIDE

Is 28% of firms reporting breaches too high?

Is 84 reportable breaches in a year too many?

Should the legal profession be doing better?

Does law firm size make a difference to how well data is protected?

Should law firms prioritise IT Security spend on email data leakage and ransomware protection?

Is the current approach to data protection training effective?

Has working from home impacted the likelihood of a data breach?



FOR MORE INFORMATION ON OUR DPO SERVICES CONTACT US AT info@twenty4consulting.com