

PwC's In-house Legal Academy: Managing Data Breaches

May 2024

Data Protection (part of Legal Business Solutions)



PwC Data Protection (Legal Business Solutions)

Our team advises clients on the laws and regulations in relation to personal data. Much of our work originates outside the UK, advising clients with global operations in connection with issues such as **GDPR compliance, international data flows and cross-border transfers**. We also advise in the case of serious **data breaches & other crisis management** situations, provide **thought leadership on emerging issues**, such as the **use of AI**, and how to incorporate **privacy by design** into new services & business models.

With you today



Shivani Shenoy
Senior Associate
shivani.x.shenoy@pwc.com



Karmen Yee
Senior Associate
karmen.yee@pwc.com

Agenda

- 01 **Introduction to Data Breaches**
- 02 **What Should I do in a Data Breach?**
- 03 **Case Study**
- 04 **Key Takeaways**

Slido Code: 5754482

<https://www.slido.com/>



1

Introduction to Data Breaches

Why breach readiness is important

70 - 74%

Medium - Large businesses have experienced a cyber security breach or attack in the last 12 months *

32%

Large businesses have experienced a negative outcome (i.e. systems compromised, assets stolen) *

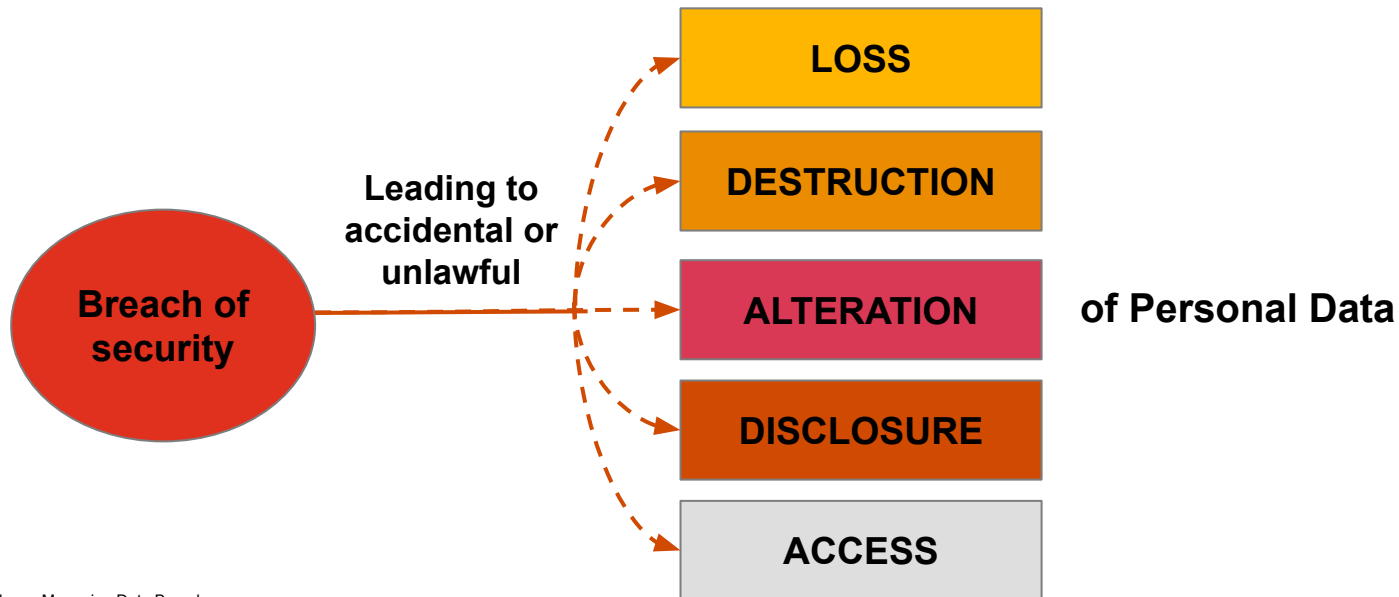
£8.7 million OR 2% of global annual turnover

Organisations have to ensure that sufficient measures are in place to keep the data secure. Failure to do so can lead to fines being imposed.

*** Source:** *Cyber security breaches survey 2024 (Gov.UK)*

What is a personal data breach?

Personal data is any information relating to an identified or identifiable natural person, in particular by reference to an identifier such as a name, an identification number, location data.



Quiz: Which of the following are data breaches?

A

Annie receives a link via her work email to enter a prize draw for a lifetime supply of coffee. She clicks on this link and enters her log in details. As a result of this, there is evidence of unauthorised access to her mailbox.

B

Sean is working in a café and leaves his password manager opened on his unlocked work laptop whilst he goes to order a cup of tea. During this period, Jon walks past and copies several of his passwords.

C

There is a system outage at the office which leads to customer calls being unanswered for a short period of time.

D

Doug sends an email containing sensitive documents to the wrong client.

E

James spills water on his laptop and it can no longer be used.

Answer: Which of the following are data breaches?

A

Annie receives a link via her work email to enter a prize draw for a lifetime supply of coffee. She clicks on this link and enters her log in details. As a result of this, there is evidence of unauthorised access to her mailbox.

B

Sean is working in a café and leaves his password manager opened on his unlocked work laptop whilst he goes to order a cup of tea. During this period, Jon walks past and copies several of his passwords.

D

Doug sends an email containing sensitive documents to the wrong client.

C

There is a system outage at in the office which leads to customer calls being unanswered for a short period of time.

E

James spills water on his laptop and it can no longer be used.

Quiz: What was the leading cause of data breaches in the UK?

1

Phishing

2

Emailing the wrong recipient

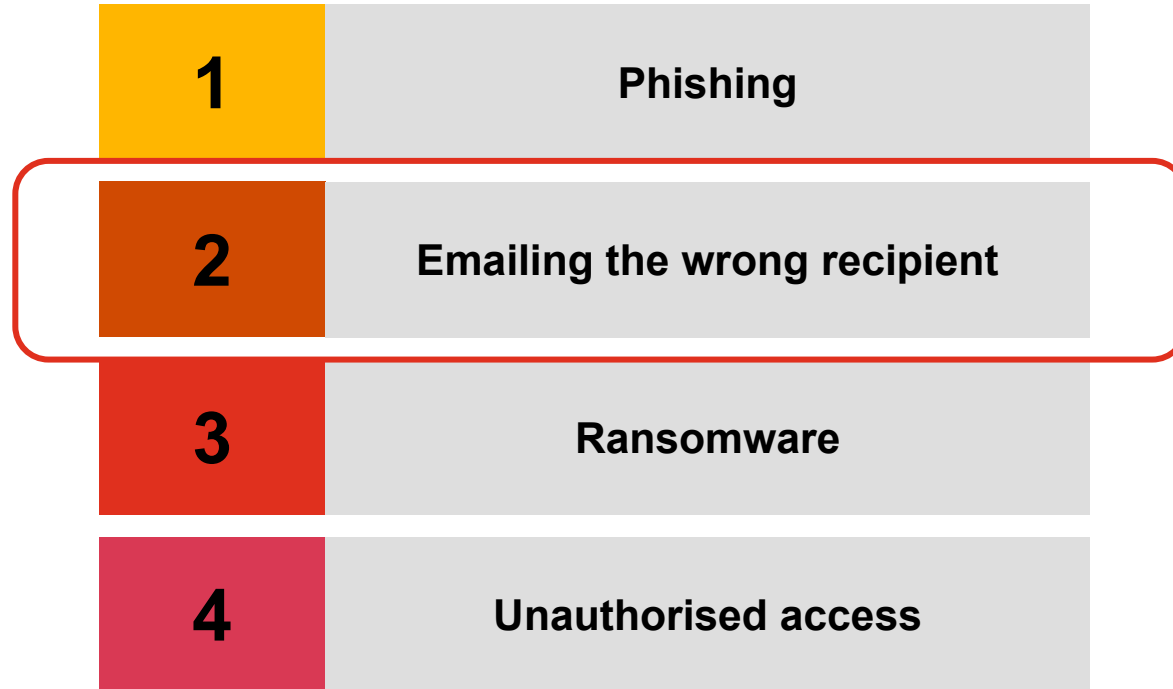
3

Ransomware

4

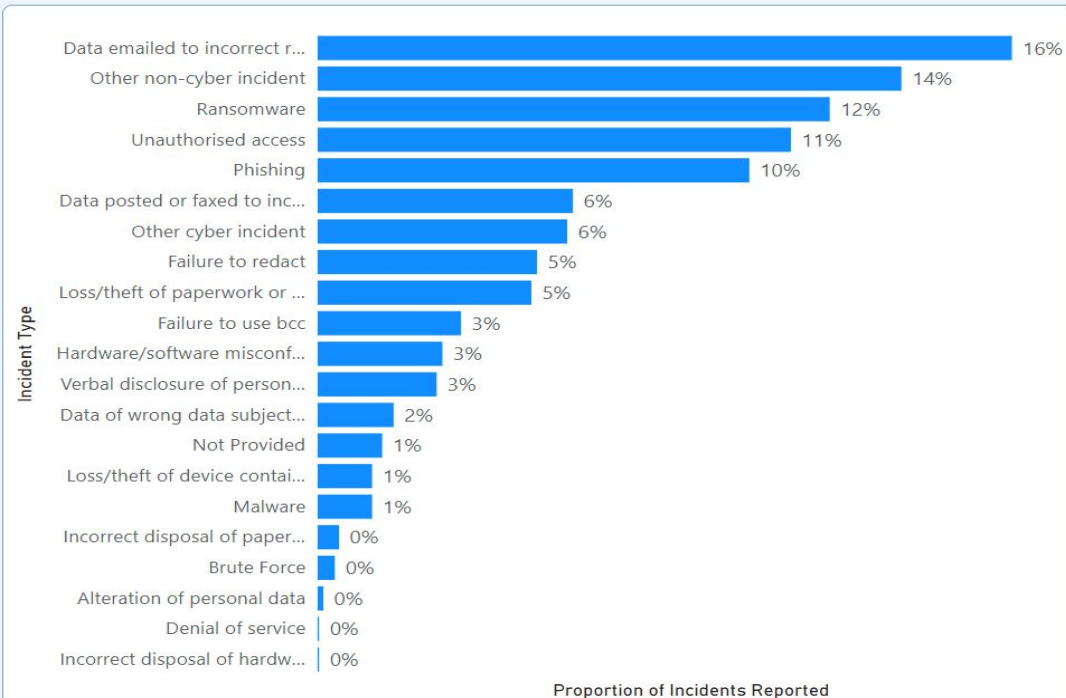
Unauthorised access

Answer: What was the leading cause of data breaches in the UK?



Data Breaches Reported

Proportion of Incidents Reported

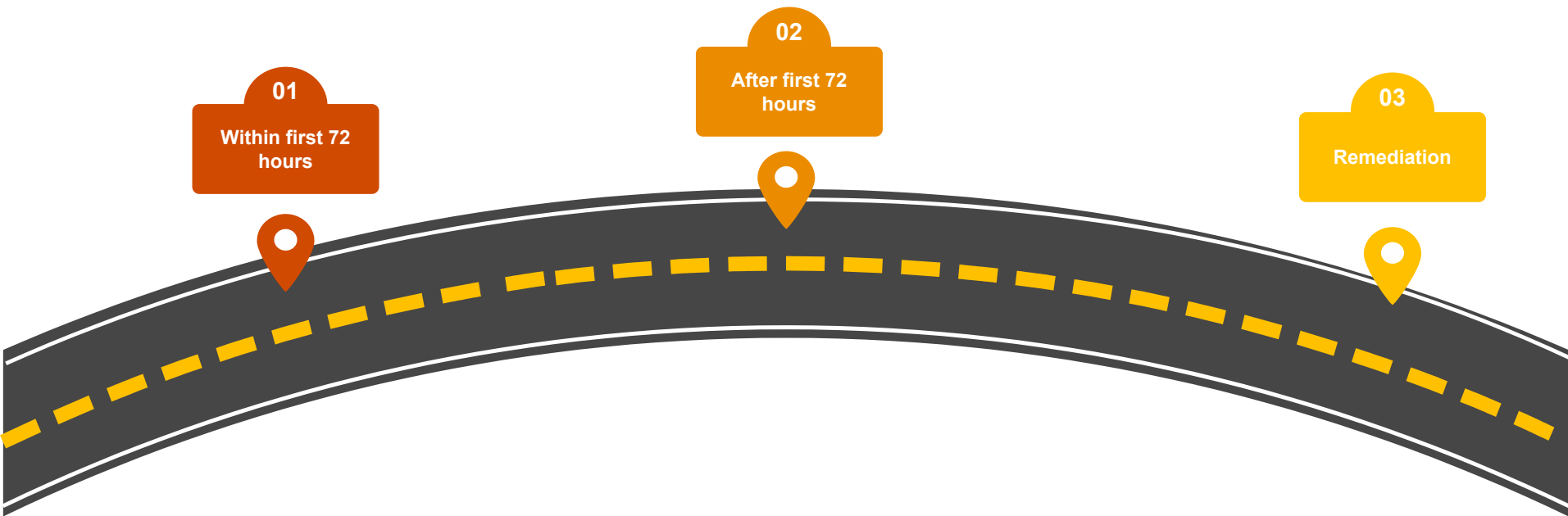


Source: ICO data security incidents trends dashboard (2023)

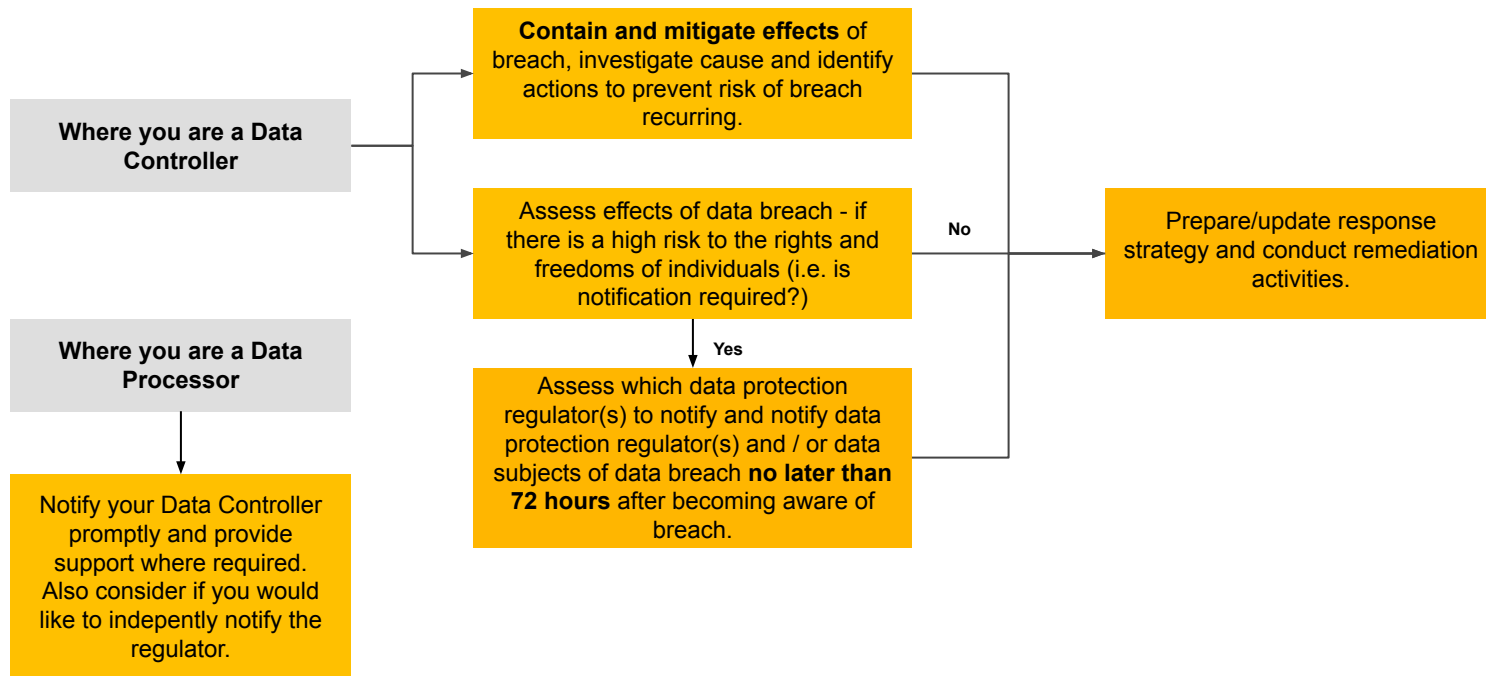
2

What Should I Do in a Data Breach?

Data breach response timeline (under the GDPR)



What do I need to do in a data breach?



Quiz: To notify or not to notify?

A

A medical professional sends incorrect medical records to another professional. The recipient informs the sender immediately and deletes the records securely.

B

A customer database is stolen.

C

A member of staff at a university accidentally deletes records of alumni contact details. The details are recreated from a backup.

D

A company uses a third party platform to provide health insurance for its employees. The platform notifies the company that a number of their databases containing employee data have been compromised due to a phishing attempt.

Answer: To notify or not to notify?

D

A company uses a third party platform to provide health insurance for its employees. The platform notifies the company that a number of their databases containing employee data have been compromised due to a phishing attempt.

B

A customer database is stolen.

C

A member of staff at a university accidentally deletes records of alumni contact details. The details are recreated from a backup.

A

A medical professional sends incorrect medical records to another professional. The recipient informs the sender immediately and deletes the records securely.

3

Case Study

Incident background

Background



Chill Breaks Limited provides holiday packages



Jay (an employee based in the UK office) liaises with independent tour providers, including Icelandic Snow Ventures.



Incident



Jay receives an email from "HR" asking him to verify his employment details for an internal system update.



Two days later...



Chill Breaks Limited receives complaints from customers that they did not receive payment confirmation from Icelandic Snow Ventures despite making a payment.

Incident outcome



Phishing - Employee (Jay)



Phishing - Customers




Jay's account is closed. Activity suspended on compromised systems.

Impacted customers are sent an initial message to make no further payments and to contact their banks.

What should happen next?



**Notify the ICO
and customers?**



**Do not notify the
ICO and
customers?**

First 72 hours: Key actions for internal legal teams

01

Risk Assessment

- **Assess risks to data subjects** (i.e. customers)
- Determine whether there is a need to **notify ICO / other regulators and data subjects**.

02

Notifications

- **Prepare notification** to ICO (& other regulators)
- **Notify data subjects** and steps they can take to mitigate harm

03

Comms

- Communications to customer facing employees - **guidance on handling complaints**
- Work with comms team to prepare **public facing notifications** in line with **liability response strategy**
- General communications to employees - **stay vigilant**

04

Wider Response Strategy

- Review strategy for response to **internal stakeholders and external parties** (e.g. insurer / Icelandic Snow Ventures)
- **Review contracts** (including insurance contract)
- Consider **risk of litigation** being launched

Post 72 hours: Key actions and remediation

Scenario:
ICO raises
questions on
notification
sent



POST 72 HOURS



- Respond to queries received from ICO
- Document findings from investigation
- Report internally and determine plan for remediation



REMEDATION



- Complete internal data breach report
- Revisit and refresh employee training
- Review and update internal breach reporting framework
- Update relevant policies
- Review DSAR / complaints management process

4

Key Takeaways

Key takeaways



Arrange regular security training and breach simulations



Ensure you have clear process for incident response



Cyber response strategy and governance



Keep up to date with changes

