

Data breaches and cyber incidents in law firms

What to do in the first 72 hours

Practical breach-response guidance
for law firms

Kristy Gouldsmith
Spencer West LLP



SPEAKER

Kristy Gouldsmith

kristy.gouldsmith@spencer-west.com



Data protection law specialist

- 1 Advises organisations across multiple sectors on data protection, privacy and compliance.
- 2 Works with clients ranging from smaller businesses to large international companies.
- 3 Practical focus: helping firms balance innovation, client trust and regulatory risk.

Sector experience includes

SaaS platforms

Retailers

Manufacturers

Schools

Care homes

Financial services

Law firms

Today's focus: data breach reporting.

Agenda

- **Set the scene** Why law firms are attractive targets and why breach response is different in legal practice.
- **Recognise and stabilise** Data breaches; containment; roles; first facts.
- **Reportability decisions** ICO threshold, high-risk individual notification and phased reporting.
- **Communications and regulators** Clients, employees, SRA, insurers, NCSC, police and suppliers.
- **Investigation and readiness** Evidence, decision records, common mistakes and the response plan.

The Q&A is deliberately left for the end: most questions are usually about timing, wording and what to report.

Why breach response is different in law firms

The same incident can trigger data protection, professional and client relationship issues

1

Dense confidential material

Matter files can include privileged advice, litigation strategy, special category data and financial details.

2

Client trust and duties

The issue is not only data loss; it can affect confidentiality, undertakings, deadlines and client confidence.

3

Multiple notification routes

ICO, clients, SRA, insurers, NCSC or police may all need to be considered, but not always notified.

The practical problem

The firm needs to move quickly without over-reporting, under-reporting, alarming clients unnecessarily or destroying evidence.

Definition of a data breach:

A data breach is a breach of security leading to the accidental or unlawful:

- destruction
- loss
- alteration
- unauthorised disclosure of
- unauthorised access to

Personal Data

Definition of personal data:

- any **information** relating to an identified or **identifiable natural person** ('data subject')
- an identifiable natural person is one who can be identified, **directly** or **indirectly**, by:
 - name
 - identification number
 - location data
 - online identifier
 - physical, physiological, genetic, mental, economic, cultural or social identity

The 72-hour clock starts when the firm is aware

Do not wait for a perfect forensic report before starting the log

72 hours

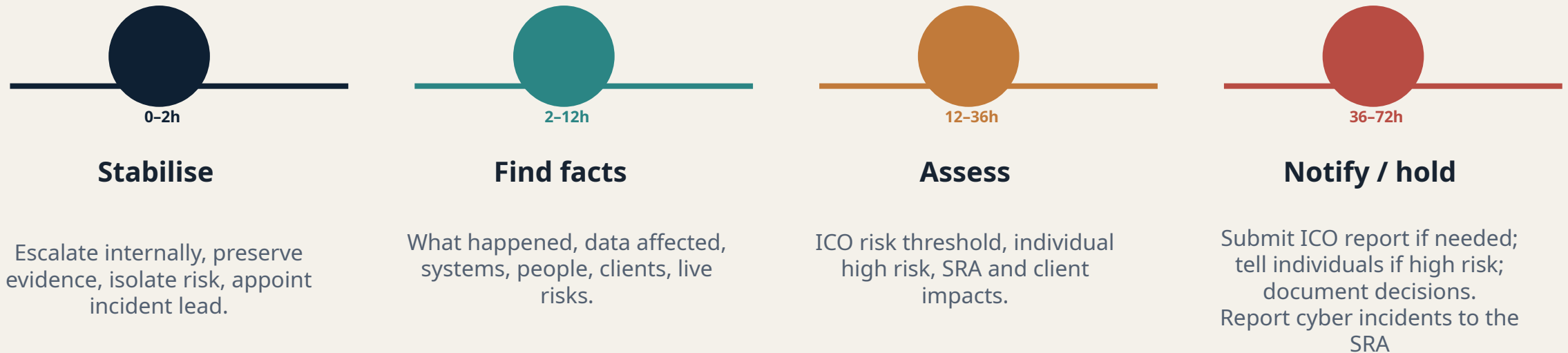
Notifiable breaches must be reported without undue delay and, where feasible, not later than 72 hours after becoming aware. If the firm cannot provide all details, information can be provided in phases.

Practical rule: start the timer and the incident log immediately, even if you later decide it is not reportable.



A practical first 72-hour structure

The plan is not linear — containment, facts and decisions run together



Do not treat “report to the ICO” as the only task. The wider response is usually where mistakes happen.

Immediate triage: what to establish first

Enough facts to contain the risk and make a defensible notification decision

1 What happened?

When detected, by whom, how, and whether it is ongoing.

2 What data?

Client matter files, emails, HR records, AML/KYC, bank details, special category data.

3 Whose data?

Clients, counterparties, employees, witnesses, children, vulnerable individuals.

4 What systems?

M365, case management, email gateway, cloud supplier, personal device.

5 What exposure?

Access only, exfiltration, publication, encryption, loss, alteration or unavailability.

6 What immediate harm?

Fraud risk, safeguarding, litigation prejudice, confidentiality, distress or service disruption.

Capture “known / unknown / next action” for each point — do not leave uncertainty invisible.

Containment: act quickly, but do not destroy evidence

The right response depends on the incident type



- Disable compromised accounts and revoke sessions.
- Reset credentials, especially privileged accounts.
- Preserve logs, headers, audit trails and suspicious emails.
- Isolate affected machines before wiping or rebuilding.
- Secure backups and test restoration routes.
- Stop further disclosure: recall emails, request deletion, suspend links.

Good containment reduces harm. Poor containment can make the investigation harder.

Allocate roles before the room gets crowded

A breach response needs ownership, not a long email chain



Incident lead

Owens timeline, actions, meetings and escalation.



IT / forensic lead

Contains, preserves logs and explains technical facts.



DPO / privacy

Assessment and records.



COLP / risk

Assesses SRA, professional and client obligations.



Comms / client lead

Controls wording, audiences and approval route.



Board / managing partner

Makes strategic decisions and authorises spend.

Decide who can approve: ICO report, individual notice, client notice, public statement, regulator report, ransom position.

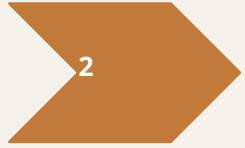
The UK GDPR breach framework

Three separate questions — often confused under pressure



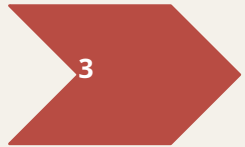
Has there been a personal data breach?

Review definitions



Is it reportable to the ICO?

Report unless it is unlikely to result in a risk to rights and freedoms.



Do individuals need to be told?

Tell individuals without undue delay if it is likely to result in a high risk.

Keep the thresholds separate in the breach record.

Assess risk from the individual's perspective

The ICO focus is potential adverse consequences for people

Data sensitivity

Special category, criminal offence, financial, children, safeguarding, litigation material.

Volume and identifiability

How many people, how easy to identify, whether data was encrypted or pseudonymised.

Recipient / attacker

Trusted recipient, unknown person, hostile party, dark web, opponent, disgruntled employee.

Likely consequences

Fraud, distress, loss of confidentiality, reputational damage, prejudice, safeguarding risk.

Containment and mitigation

Deletion confirmed, access closed, publication removed, password resets, monitoring offered.

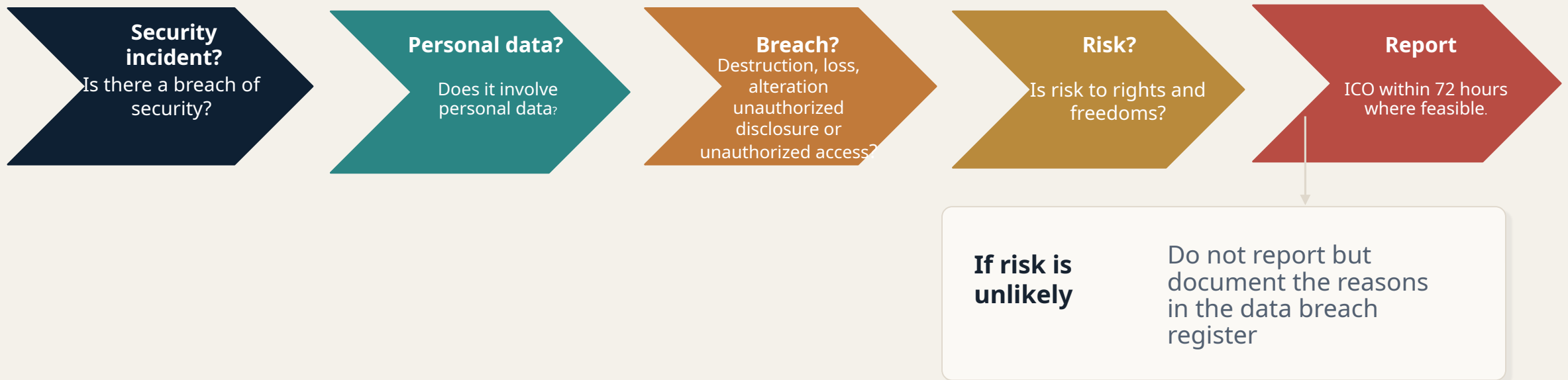
Characteristics of people

Vulnerability, children, protected characteristics, sensitive disputes or high-profile clients.

Ask: "What could happen to the people whose data is involved?"

ICO reportability: a simple decision tree

A structured decision reduces panic and inconsistency



A “borderline” reportability decision should be supported by facts, not instinct.

What goes into an ICO report?

The initial report can be phased

Nature of breach

What happened, incident type, dates, systems and whether it is ongoing.

People and records

Categories and approximate numbers of individuals and records affected.

Contact point

DPO or other person the ICO can contact for more information.

Consequences

Likely harm or adverse effects on affected individuals.

Measures

Containment, remediation and mitigation already taken or proposed.

Do not delay notification just because the root cause is still under investigation.

When do affected individuals need to be told?

The threshold is “likely high risk” not every reportable breach

Tell individuals without undue delay if:

- the breach is likely to result in high risk;
- they need to take steps to protect themselves;
- clear advice will reduce harm or distress.

The message must include:

- what happened in clear, plain language;
- likely consequences;
- mitigation and contact point.

Do not turn a notification into a legal admission. Do make it useful enough for people to protect themselves.

Communications: say enough, not too much

Poor wording can increase complaint, claim and reputational risk

Do

Use approved wording and one source of truth.

Do

Separate facts, assumptions and action being taken.

Do

Give practical steps: password reset, fraud alert, contact point.

Avoid

Speculating on blame, motive, scope or root cause.

Avoid

Over-promising that all risk has been eliminated.

Avoid

Uncoordinated calls from multiple partners to clients.



Every external message should match the breach record and the actual controls deployed.

Other reporting routes: do not treat the ICO as the whole answer

Ask who else needs to know — and why

SRA	Prompt report where firm or clients are directly affected by a cyberattack, or where there is client impact/potential impact.
Insurers / brokers	Check cyber and PII notification conditions early; late notice can create coverage problems.
NCSC / Report Fraud	Consider NCSC and police routes for significant cyber incidents, live attacks, fraud and extortion.
Banks / payment partners	Act fast where client money, bank details, mandate fraud or payment instructions are involved.
Clients / counterparties	Separate legal duties from practical client-service expectations and contractual duties.

Record each route considered: notified / not notified / not yet / owner / reason.

What and when to inform the SRA

Law firms have an extra layer beyond UK GDPR



No duty to report every cyber attack

The duty arises where the incident is sufficiently serious, or the facts ought to be brought to the SRA's attention so that it can decide whether regulatory action is required.



Report promptly where:

- the facts are capable of amounting to a serious breach of the SRA's regulatory arrangements; or
- the matter should be brought to the SRA's attention so that it can investigate whether a serious breach occurred or exercise its regulatory powers



COLP

The COLP has a corresponding duty under paragraph 9.1(d) and (e) to ensure that the report is made. [SRA Code of Conduct for Firms](#)

Practical control: decide who will inform the SRA, if required.

Supplier incidents: get control of the facts fast

A processor's breach can become the firm's 72-hour problem

- 1 Notice trigger**
When did the supplier become aware and when did it notify you?
- 2 Data scope**
Which firm data, clients, matters, systems and countries are affected?
- 3 Access/exfiltration**
Was there access, copying, encryption, publication or only attempted intrusion?
- 4 Sub-processors**
Were hosting, support or security vendors involved?
- 5 Mitigation**
What steps have been taken and what do they need from the firm?



Check the contract: breach notice, cooperation, audit, logs, forensic reports, confidentiality and communications control.

Internal investigation: preserve evidence and learn the root cause

You need a defensible story of what happened and what changed

1

Technical evidence

Logs, alerts, audit trail, email headers, endpoint image, access logs, backups.

2

Timeline

Detection, escalation, containment, decisions, notifications, remediation.

3

People evidence

Witness accounts, screenshots, call notes, training records, approvals.

4

Decision evidence

Risk assessment, reportability decision, individual notification decision, regulator/client comms.

The final incident report should be useful to the firm, not just written for the ICO.

The breach register: your best defence months later

Record all breaches, whether or not they are reported

Field	Why it matters
Facts and timeline	Shows when the firm became aware and what happened next.
Data and people affected	Supports ICO and individual notification thresholds.
Risk assessment	Explains the likely consequences and mitigations.
Notifications considered	Shows why ICO, individuals, SRA, clients or insurers were or were not notified.
Remedial action	Connects root cause to changes in controls, training and supervision.

Document the facts, effects and remedial action.

Common mistakes that make incidents worse

Most failures are governance failures, not only technical failures

1

Waiting for certainty

The 72-hour deadline is missed while the firm seeks perfect facts.

2

No single owner

Multiple partners, IT and suppliers act without one decision record.

3

Destroying evidence

Systems are wiped or rebuilt before logs and images are preserved.

4

Wrong audience

Clients, individuals and regulators receive inconsistent explanations.

5

Over-notifying or under-notifying

The threshold is not applied or the rationale is not recorded.

6

No lessons learned

The final report identifies changes but no one owns implementation.

Keep calm!

Build the breach-response plan before you need it

The plan should be short enough to use under pressure

Escalation

Who must be told, how fast, and how staff report breaches.

Incident team

Named roles, deputies, contact numbers and authority to spend.

Playbooks

Misdirected email, mailbox compromise, ransomware, supplier breach, lost device.

Templates

Breach log, ICO assessment, individual notice, client note, SRA note.

Supplier pack

Critical suppliers, incident contacts, DPAs, security contacts, sub-processors.

Testing

Tabletop exercise, lessons learned and board/practice group reporting.

Keep the plan practical.

Testing the plan: a tabletop scenario for law firms

A good test forces real decisions within a realistic timeline

09:10



Partner reports suspicious mailbox rule and missing sent emails.

10:30



IT finds external forwarding and suspicious logins.

13:00



Three client matter folders may have been accessed.

16:30



A client asks whether confidential deal documents are safe.

Day 2



Supplier confirms incomplete logs and possible exfiltration.

Test decisions: containment, ICO, individuals, client notice, SRA, public line, task owners.

The safe response checklist

The takeaway: stabilise, assess, record and communicate with discipline

- Start the incident log and 72-hour clock immediately.
- Contain the incident while preserving evidence.
- Identify data, people, systems, clients and live harm.
- Apply the duty to inform the ICO and the data subjects as separate thresholds.
- Consider SRA, insurer, client, NCSC, police and supplier routes.
- Use one approved communication line and avoid speculation.
- Record decisions, owners, timing, reasons and remedial actions.

Responsible incident response is about calm, accurate decisions made quickly — not perfect certainty.

QUESTIONS

Questions

15 minutes