14 July 2023

Data breach incidents and response plans

Chartered Institute of Internal Auditors

Don't be caught out by the GDPR requirements

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. This must be done within 72 hours of becoming aware of the breach, where feasible.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the organisation must also inform those individuals without undue delay.

Robust breach detection, investigation and internal reporting procedures should be in place. This will facilitate decision-making about whether or not the organisation needs to notify the relevant supervisory authority and the affected individuals.

A record of any personal data breaches must be kept, regardless of whether you are required to notify.

Internal audit's role should be to support the business in preparing for a breach and understanding the lessons learned where one occurs but not managing or generally being involved in a breach, unless absolutely necessary.

What is a personal data breach?

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Examples of personal data breaches provided by the Information Commissioner's Office (ICO) can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

Recital 87 of the GDPR makes clear that when a security incident takes place, you should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required.

The ICO defines a personal data breach as:

A security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

How are data breaches discovered?

Data breaches are discovered through a number of different channels, for instance:

1. Automated system monitoring - detecting a potential data breach; this is usually reviewed manually prior to action being taken.

2. Whistleblowing facilities for groups such as staff, customers and suppliers to report concerns anonymously. End users may report breaches to the IT helpdesk, however be aware that issues reported in this way may not be logged as breaches. To report incidents, staff need to be aware of the process; this should be included in both initial staff training and refresher training.

3. After details are published by the hackers, or when members of the public find IT equipment and report it to news outlets. On occasions it may be that the breach is in the public domain before the organisation learns of it. It is then harder to control the flow of information and control the incident.

4. When an incident comes to light, the actual report of the breach itself may contain sensitive and/or personal data which should be subject the organisation's information classification policy and protected appropriately.

Information security policy

The organisation should have an information security policy that reflects the organisation's objectives for security which is formally agreed by executive management.

The information security policy should include:

- an acceptable use policy
- details of how employees will be educated about protecting the organisation's assets
- how security measurements will be carried out and enforced
- procedures for evaluating the effectiveness of the security policy

The policy should also include how to record near-misses and how these are monitored. Any incident may need a manual back-up and some way to invoke it without the use of IT systems, including communication with others.

Response

Preparing for an incident

It is important to create an incident response plan in advance, before a breach occurs. It cannot be an afterthought. Where internal audit reviews readiness, the following points could be considered:

1. Responsibilities and authorities should be defined to key individuals (the response team) along with contact details.

2. The response team may include the head of IT, information security, head of corporate communications and senior executives.

3. Training should be conducted; to ensure that all staff know how to recognise a personal data breach. Exercises and scenarios should be practiced to ensure that people are aware of their roles in an incident and the plan updated if need be.

4. The internal escalation process for incident responses should be documented and tested periodically. It may be that other bodies need to be notified depending on the industry in which the organisation operates.

   Examples of bodies which may need to be notified include the Information Commissioner's Office (ICO), Financial Conduct Authority (FCA), Prudential Regulation Authority (PRA), Care Quality Commission (CQC). Organisations may already have a documented process for approaching regulators, and these principals will need to be incorporated and the necessary individuals involved in planning.

5. The breach may affect more than one physical or virtual site and the people on the response team need to have the relevant permissions to make decisions or enforce actions on these sites. This could include issues such as ensuring that response team members have passes which allow them access to all relevant sites, or ensuring that passwords are in place to allow them access to the relevant IT equipment.

6. The response team may need to secure the site(s) physically to ensure people's safety. This may involve facilities management or using contractors. Again, ensuring that the response team have access to critical contacts and the ability to place order during an incident is critical.

7. In responding to an incident, management need to be aware that while ensuring the integrity of critical systems, they should also consider any investigation and how this might be affected by the focus and actions of returning to business as usual as quickly as possible. A decision like this, and which takes priority if they cannot be done together, should be agreed by the board or sub-committee prior to the event.

8. Prior to any incident, the policy should define system response times and the relative priority they have over business as usual processes.

9. It may be that damage limitation is needed both physically on-site and with customers and the corporate communications team will be invaluable in assisting with this. Pre-agreed scripts for certain scenarios along with when and to who may save time in the event of an incident as well as communication method if normal tools (email, network, etc.) were compromised or unavailable

because of the incident.

10. A key point is that the organisation should test various scenarios periodically to ensure that the response is rehearsed and roles are known.

Responding/reacting to an incident

The predefined response should only allow defined and authorised staff to be involved in the response. Bear in mind that any continuing response could be time-consuming and potentially last for months.

The response team need to be called together as soon as the data breach is known. (If the organisation employs media monitoring, this notification may happen at any time and the key individuals would have to be available out of hours.) Initially the meeting may be virtual; however getting the team together in person is an important step. An initial meeting should be held with the response team to establish the next steps and who to involve at that stage along with:

1. The value of the data which has been breached needs to be understood so that the recovery can be prioritised. The organisation may have an incident categorisation model, such as minor, moderate, severe, crisis. This may depend not only on the volume of data but the nature of data (for example personal sensitive data as defined by the general data protection regulation).

2. A decision on record keeping – both relating to organisational logs and records that the team create during the response. It is good practice to note down the timing of events, such as when individuals were informed, when decisions were made and who was involved in making them.

3. A review of whether affected individuals need to be informed. The information that needs to be provided to them and advice to help them protect themselves from its effects.

4. A review of whether external bodies, including regulators need to be involved and initiate this, using the appropriate process and within laid down timescales (ie ICO within 72 hours of becoming aware of it).

5. Whether a forensic expert is needed to understand what needs to be searched for, collect any/all items related to the incident as well as deciding whether the police, etc. need to be informed. The procedure should detail who can be contacted and who authorises the appointment.

6. Ensuring any internal investigation is kept as confidential as possible; not only to protect the data but also because the source of the breach may be an insider who subsequently has a role in the response.

7. Work to prevent any further breach and stop the current breach (if it’s ongoing) and mitigate the damage that the breach, and any leaked data, can cause. This might include the public relations team and the issuing of press releases. Ensure that the response team contains people with the authority to initiate this.

8. Giving instructions to isolate the affected systems and equipment. These may be needed for any subsequent investigation. Ensure the chain of custody remains intact. Bear in mind that closing down or isolating a system could have a huge impact on the organisation.

9. Beginning to investigate the cause of the incident. This may take a lower priority whilst the team

firefight initially, but establishing how it happened may assist with stopping the current breach.

10. How to recover systems in line with contracts/SLAs. This may involve invoking the business continuity or disaster recovery plans if key systems are unusable. IT should ensure that any secondary sites/systems are not also affected by the breach prior to rerouting critical systems. (There may be conflicts between the investigation and the recovery plans; the business tries to recover but the investigation is ongoing.)

11. Establish who should be informed, both internally and externally; this could include the information security officer, IT, HR, facilities management, legal team, compliance team, internal audit, public relations/press office, security, regulators, police, insurers, alarm company and so on.

12. Advising the information owner that data they are responsible for has been breached.

13. It is likely that the proper investigation of an incident will delay the recovery to business as usual.

14. Being aware of false alerts – these could potentially close down parts of the business.

15. The temptation to launch a counter-offensive if the source is identified, but this is likely to be illegal.

Lessons learned (after the incident)

1. Once the incident is brought under control the organisation has to consider how to learn from it and how to prevent further breaches going forward. As independent and objective providers of assurance internal audit is placed to be involved in this process as part of a team that has the overall expertise to perform this function. Internal audit should not accept involvement where it does not have the skills or experience. This also applies to the provision of assurance set out in the next section.

2. This may also involve monitoring near misses at an appropriate committee or board (which should already be clarified as part of the organisation's information security policies and procedures).

3. The organisation may find there are later repercussions from the initial incident and may find further leaked data in the public domain which requires an additional response. It may be that the attack ‘repeats’ and the cycle of responding to an incident continues. If this happens, the organisation’s resources can be heavily depleted and in extreme circumstances could cause the business to close down.

What can internal audit do?

Include the incident plan in the audit universe

Internal audit should incorporate the incident/breach response plan within the audit universe and periodically review the incident/breach response plan as part of the annual audit plan process. This will help ensure that the incident/breach response plan:

- contains accurate and current information
- is assessed and fine tuned

- identifies potential issues in advance – before the breach occurs
- allows the process to operate more efficiently – if a breach subsequently occurs
- provide assurance that risks are addressed

Monitor and review activity

As part of the testing of the incident/breach response plan, internal audit can monitor and review the activity undertaken and confirm whether any lessons learned have been reflected in the plan.

Assess whether risk management is effective

Internal audit has an important role to play in evaluating whether risk management processes in this area is working effectively, that the reporting of risks is complete and accurate and that risk mitigation has been applied and is working in line with industry standards.

Review risk registers

To begin with, internal auditors can review risk registers to ensure that risks in relation to data security and privacy have been adequately identified and assessed, according to the risk management process within the organisation, and that managers are working to and within risk tolerances.

Participate in internal/external forums

This is to ensure awareness of emerging security threats and practices for protecting against them.

Consider data security

Ensure that data security is considered and included generally during all types of audit work.

Further reading

Blog post GDPR – Data breaches

ICO's Personal data breaches