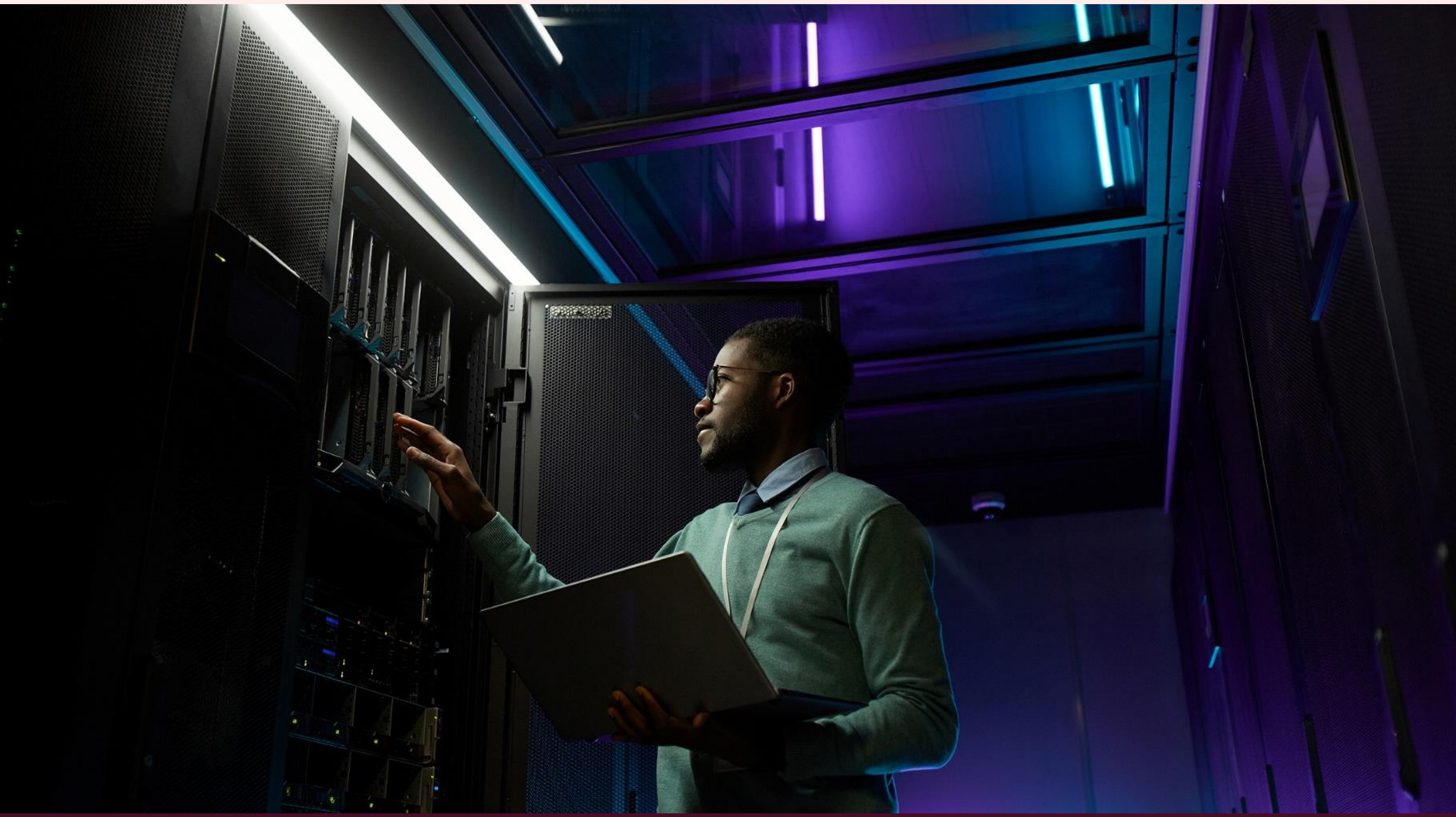
13 June 2024

Shared Insights

Handling data breaches in the health and care sector

Panel of speakers

Charlotte Harpin, Partner (Chair)
Matthew Alderton, Partner
Heather McKay, Senior Associate



Introduction

The recent cyber attack on two prominent London Hospitals this month has brought to light the importance of understanding the potential consequences of data breaches and what can be done to prevent them.

This Shared Insights session enabled a timely exploration of three scenarios that many organisations face and what can be done to mitigate the adverse effect of data breaches in the health and care sector.

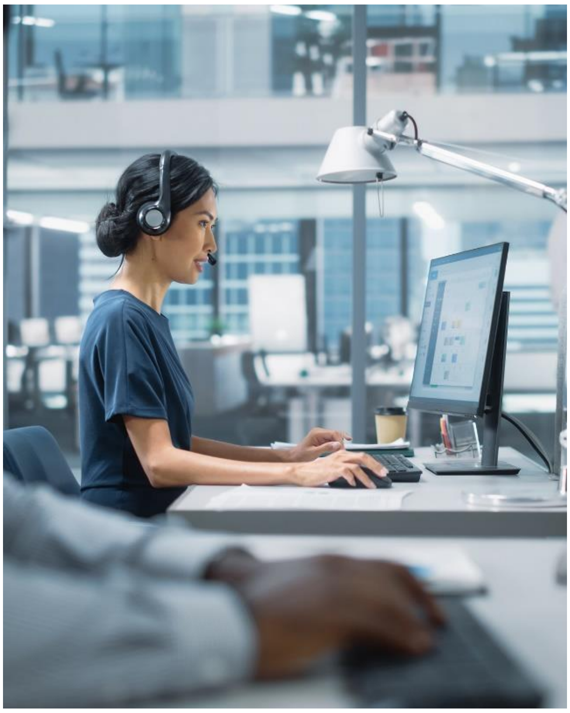
Charlotte Harpin
Partner

+44 (0)330 045 2405
charlotte.harpin
@brownejacobson.com

Contents

How we can help

With our comprehensive suite of services, Browne Jacobson can help you fortify your data protection practices by providing timely insights, expert guidance, bespoke training and tailored solutions to navigate the evolving landscape of data breach and cyber threat.



Cyber Attacks

Matthew Alderton
Browne Jacobson

As cyber-attacks continue to increase in frequency and sophistication, organisations in the health and care sector are facing growing threats to their data security. From subtle system access loss to outright ransom demands, the consequences of a cyber-attack can be devastating.

As cyber-attacks become increasingly complex, it is important to be aware of common indicators of an attack. These can range from subtle system access loss to outright ransom demands. Threat actors are becoming more sophisticated, making it essential to establish a response protocol in advance. Testing and communicating this protocol to staff is crucial to achieving the best outcome in the event of an attack.

Identifying a cyber response team, having cyber insurance, and knowing who to contact in the event of an attack are all important steps. Having a team of experts on hand to manage the process of containing the attack, notifying regulators and those affected, and helping the organisation return to business as usual in a timely and responsive way is essential. Key people to contact include the IT leads, legal and PR teams and head of risk. It is important to have a multifaceted response to the attack, including senior clinicians in the health and care sector.

If you have cyber insurance in place, it is important to notify your insurers immediately. They may need to take systems completely offline and have someone go physically into your building to collect data. They may instruct panel solicitors on how to act and how to deal with a ransom demand if you receive one.

Understanding the attack is crucial. Identifying what type of data is at risk and conducting an initial risk assessment. Your technical lead may remove any links to other systems and talk to other organisations through the cloud across the region or internationally. It is also important to notify suppliers and business partners who may be impacted if your systems go down (or vice versa).

Good policy and procedures should be in place, including a coordinated response team that can bring in different areas of the organisation as soon as possible. Staff should be trained through awareness campaigns and training to identify problems. Systems should be monitored, and findings escalated.

Matthew Alderton
Partner

+44 (0)330 045 2747
matthew.alderton
@brownejacobson.com

Mitigating the risk of data breaches caused by human error

Heather McKay
Browne Jacobson

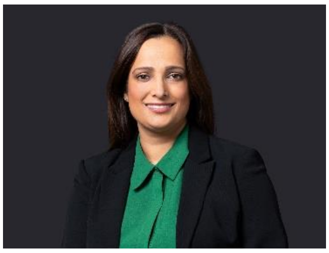
Data breaches are a growing concern in the health and care sector, often caused by human error such as sending an email containing personal data to the wrong recipient.

Reassuring the person who made the mistake, determining the cause, and being transparent about the breach can help build trust and maintain positive relationships with those affected.

Human error is a common cause of data breaches in many organisations, and it can be particularly concerning in a health and care setting where the data may concern patients or vulnerable individuals. When an email containing personal data is sent to the wrong recipient, it's important to reassure the person who made the mistake and foster trust to encourage them to report their mistake. This enables a suitable response and facilitates the investigation of the incident and any required remediation. Executive leadership teams, the board, and Caldicott guardians can make decisions based on the outcome of the investigation.

It's also important to look at the person who made the mistake to determine whether they had sufficient training or if the mistake was due to other factors. Employing technical alternatives such as OneDrive to share files with a link instead of email can help prevent such errors. Building relationships internally and creating an open dialogue is fundamental in handling the situation.

It can be difficult to determine when and how to notify individuals of a data breach due to the potential consequences. In such cases, it's important to be guided by clinicians working with the affected individuals to ensure that the right choice is made. In our experience, being open and transparent about what happened is beneficial, both with the Information Commissioner's Office (ICO) and with the individuals affected by the breach. This can help to build trust and maintain a positive relationship with those affected.



Heather McKay
Senior Associate

+44 (0)3300452232
heather.mckay
@brownejacobson.com

Unauthorised use of data

Matthew Alderton
Browne Jacobson

Data breaches caused by unauthorised access to data are a growing concern in the health and care sector, where the data may concern patients or vulnerable individuals.

Investigating the background to determine what information has been accessed and why and taking steps to minimise the risk of unauthorised access, is crucial in preventing such breaches.

Data breaches caused by unauthorised access to data can occur in various ways, from employees misusing their access rights to obtain information about friends or family to disgruntled employees taking data to get back at their employer. Unfortunately, this is more common than most people think, and it's crucial to take appropriate action to prevent such breaches.

In such cases, it's important to investigate the background to determine what information has been accessed, HR or line managers can often provide useful context to determine the reason for the unauthorised access.

Annual training and randomised spot checks can help prevent such breaches. However, these checks can be challenging in a clinical context where many people need to access records. Nonetheless, it's important to take steps to minimise the risk of unauthorised access.

If an individual doesn't engage, contacting the ICO or obtaining a civil injunction can be effective in minimising payment and risk stemming from the individual's actions. It's important to gain advice from the ICO where there is a whistle-blower, as this can complicate legal cases greatly. Taking appropriate action can help prevent future breaches and minimise the risk of liability.

Matthew Alderton
Partner

+44 (0)330 045 2747
matthew.alderton
@brownejacobson.com

Discussion

We had a lively and interesting discussion where attendees shared valuable tips and insights.

Common themes that emerged from the discussion in relation to the three case studies included the importance of:

- Preparing for a breach by engaging with stakeholders across the organisation to ensure that people know who to contact when something goes wrong.
- Having effective, proportionate, and tested policies and procedures in place for when a breach is discovered to ensure it can be dealt with smoothly and without panic.
- Fostering a culture of compliance where everyone feels comfortable speaking up when things inevitably go wrong.

Key takeaways and reflections

As data breaches and cyber threats become more prevalent, it is crucial to invest in preparation for such events. This can be the deciding factor in achieving a positive outcome. The establishment of frameworks that prioritise preparedness is essential.

Early detection, a coordinated response, and awareness of proper procedures are key to effectively managing this increasing threat.

Conclusion

In conclusion, data breaches are a serious threat. As we have seen, such breaches can occur in various ways, from human error to unauthorised access. It's crucial to take appropriate action to prevent such breaches, including preparing for a breach, having effective policies and procedures in place, and fostering a culture of compliance. By doing so, we can minimise the risk of data breaches and protect the privacy and security of sensitive information. It's important to remain vigilant and take proactive steps to prevent data breaches from occurring, and to respond quickly and effectively when they do.

Contact us

Lorna Hardman
Partner

+44 (0)115 976 6228
lorna.hardman
@brownejacobson.com

Simon Tait
Partner

+44 (0)115 976 6559
simon.tait
@brownejacobson.com

Nicola Evans
Partner

+44 (0)330 045 2962
nicola.evans
@brownejacobson.com

Charlotte Harpin
Partner

+44 (0)330 045 2405
charlotte.harpin
@brownejacobson.com

Matthew Alderton
Partner

+44 (0)330 045 2747
matthew.alderton
@brownejacobson.com

Heather McKay
Senior Associate

+44 (0)3300452232
heather.mckay
@brownejacobson.com

For further information about any of our services, please visit **brownejacobson.com**