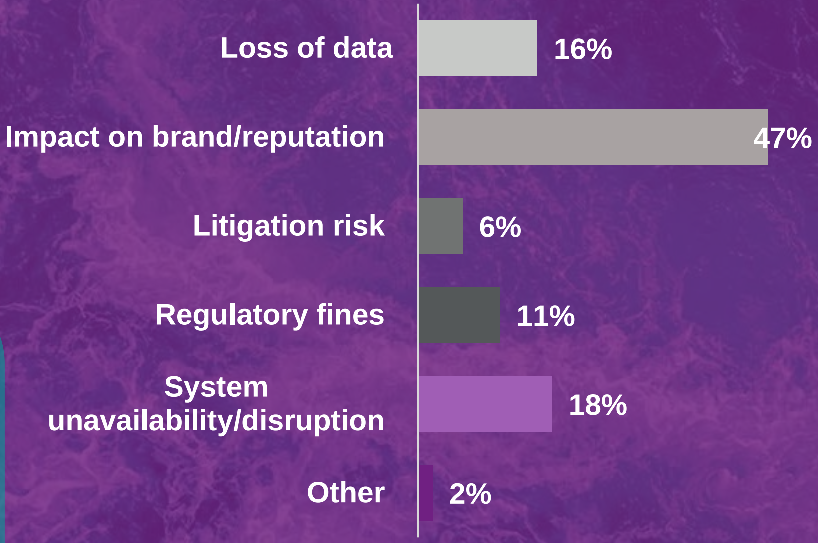
CX program: managing data and cyber breaches – lessons learned

What concerns in-house legal teams most about cybersecurity and the risk of breaches? At our CX program webinar in March 2023, members of our Global Privacy and Cybersecurity group, Antonis Patrikios (UK), Robyn Chatwood (Australia), Allison Jetton Bender (US) and Ken Dai (China), provided their expertise and actionable insights from our practice about how in-house legal teams can approach incident response, and discussed what should be done in advance to optimise incident response efforts. View the recording from the session **here.**

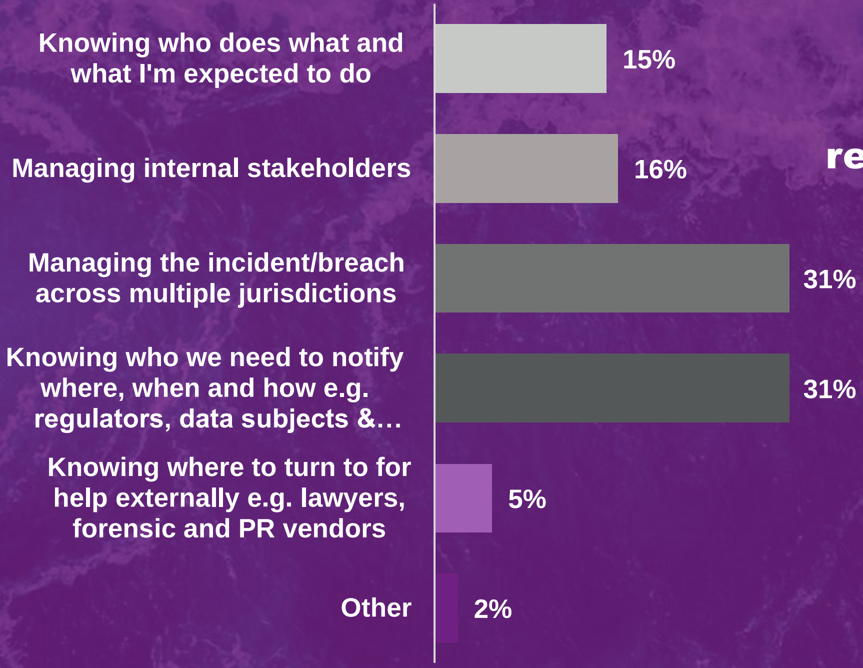
We asked our audience, comprising more than 100 general counsel and in-house legal teams from around the world, a number of questions on what their key challenges are.

What is your most significant concern regarding cybersecurity and the risk of breaches? What keeps you up at night?



Almost half (47%) of participants said that the impact on brand/reputation is their biggest cybersecurity concern, with system unavailability and loss of data coming in at second and third, respectively. In turn, the impact on brand/reputation has a significant impact on both public sentiment and the company's value. There have been a number of studies which indicate that, on average, share prices of breached companies decrease following a reported data breach.

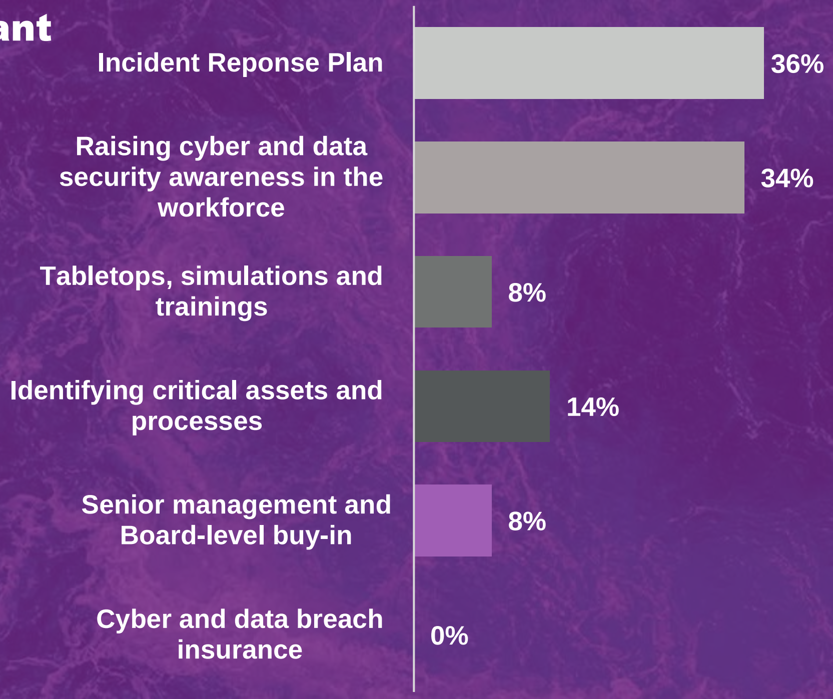
What do you feel is the most difficult and complex aspect of responding to an incident or data breach?



31% of participants said that it is knowing who to notify where, when and how, and another 31% said managing incident response across multiple jurisdictions. With both of these aspects highlighting the global complexity of data breaches, it is important to understand how a data breach could impact you on a global scale.

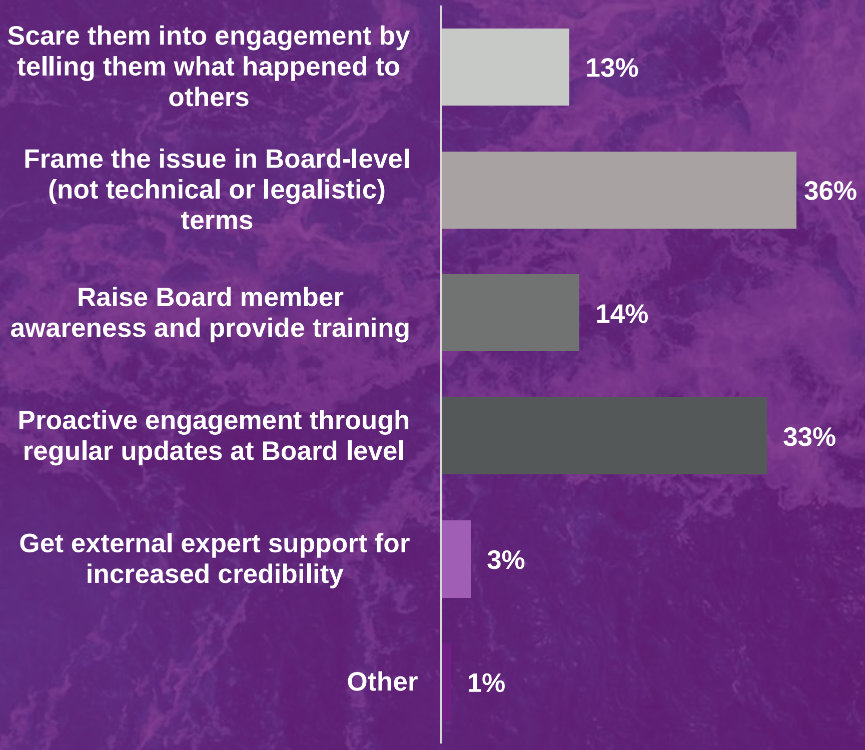
CX program: managing data and cyber breaches – lessons learned

What is the most important aspect of incident preparedness?



36% of participants shared that having an incident response plan is the most important aspect to their company's incident preparedness with "raising cyber and data security awareness in the workforce" coming in a close second at 34%. Both aspects are imperative to minimise risk and help you deal with incidents swiftly when they occur. They are also two of the key controls regulators expect to see in place, alongside tabletops, simulations and training.

In your experience, what is the best way to get Board-level engagement?



36% of participants said framing the issue at Board-level is the best way to gain Board-level engagement. This means that Board briefings should avoid technical and legal jargon and focus on key assets, risks, accountability, compliance controls and required investment.

33% said proactive and regular engagement. Board-level buy-in increases the chances of company-wide adoption and knowledge retention, and helps minimise risk when breaches occur.

Key takeaways – how to effectively get ready for managing cyber incidents and data breaches

1 Risk

Sooner or later, you will be breached.

How you deal with a cyber incident or data breach makes all the difference, so how we respond to incidents and manage breaches is essential.

2 Response

Responding to incidents can be challenging and complicated, especially across borders.

Preparation is key. Check your response plans and test them through tabletops and simulations. Review them regularly and after serious incidents. Define the composition of your incident response team (internal and key external vendors). Document your notification requirements matrix and prepare your key positions.

3 Preparedness

Everyone in the organisation has a role to play to prevent breaches and ensure appropriate incident response.

Continuous diagnostics, monitoring and mitigation, a defined plan reviewed regularly and after serious incidents, role-based training, workforce awareness and Board buy-in **will help minimise the risks** and get you ready to deal with incidents when they occur.

4 Stakeholder engagement

Preparing for and responding to serious cyber and data security incidents requires C-executive suite engagement and the full backing of the Board.

Explain to the Board, in language they understand, the top risks facing the organisation and the plan for managing them.

Antonis Patrikios

Partner, Co-Head of Global Privacy and Cybersecurity group, London
D +44 20 7246 7798
antonis.patrikios@dentons.com

Allison Jetton Bender

Partner
Washington DC, United States
D +1 202 496 7362
allison.bender@dentons.com

Robyn Chatwood

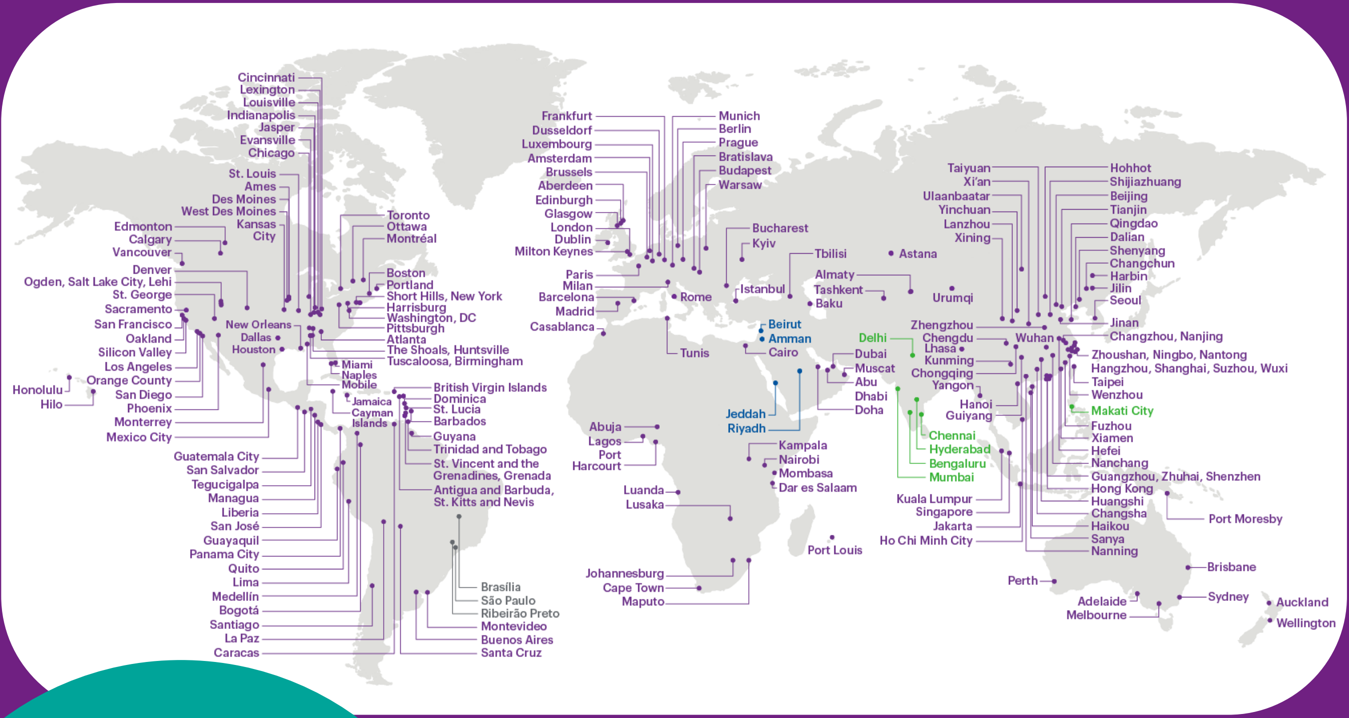
Partner
Melbourne, Australia
D+ 61 3 9194 8330
robyn.chatwood@dentons.com

Ken Dai

Partner
Shanghai, China
D +86 21 5878 1965
jianmin.dai@dentons.cn

大成 DENTONS

Market-leading data and cyber experts around the globe: Our purpose is to help you unlock the power of your data while reducing risk and achieving operational compliance. With 230+ dedicated partners and fee earners advising in 80+ jurisdictions worldwide, we support leading and cutting-edge businesses to develop and deliver complex global data projects, provide cybersecurity compliance and preparedness, respond to incidents through our integrated cyber breach solution and ensure that your data is used optimally, is secured and complies with governing legislation.



230+ data privacy and cyber security experts in 80+ jurisdictions worldwide

Tier 1 – Data protection and cyber security
Legal 500 UK 2023

The LEGAL 500

> **“The team were extremely focused on delivering an excellent standard of work for our company. I found all members very collaborative and focused on finding solutions which were appropriate for our business.”**
>
> *Legal 500 2023 – Data protection and cyber security*

> **“Dentons’ privacy team contains many expert practitioners that are able to provide pragmatic and commercial advice in a timely manner.”**
>
> *Legal 500 2023 – Data protection and cyber security*

> **“The team has very strong knowledge of privacy law and its application to the sectors in which we operate.”**
>
> *Chambers UK 2023 – Data Protection & Information Law*