CLYDE&CO X Gridware

INSIGHT | JULY 21ST 2021

Managing a data breach

Critical questions for company leaders

Data breaches can trigger significant crises for businesses, creating financial loss, reputational risks and denting consumer and stakeholder confidence. They pose a range of critical questions for company leaders.

Here are our thoughts on 10 questions Directors should be asking (and answering!) to ensure their organisations' interests are looked after in the immediate and longer terms.

A data breach can be a serious crisis. While many know this intuitively and shudder at the thought, spare a thought for those executives that have lived and breathed it and know only too well the crippling impact it can have on their operations.

Corporate Australia's last two to three years' worth of experience with data breaches shows us that public **confidence** in a business can be significantly impacted and the **cost and time** involved in remediation and recovery can be a substantial drain on the business while it deals with data breach incidents.

If not well-managed, a data breach event can cause substantial damage to a company and its directors too, both financially and in terms of reputation.

And this is without mentioning the serious regulatory implications that can eventuate, including:

- Consumer class action claims
- B2B loss recovery proceedings
- Regulatory investigations

The response of management and leadership is often reactive (and panicked) rather than strategic.

The role of the director in the modern corporation should be to see the wider implications associated with the incident and initiate the right next steps to mitigate damage in the medium and longer term.

Recently, the Australian Institute of Company Directors ("AICD") issued a thought leadership paper on oversight questions for company leaders. I found it an insightful summary of advice I myself have given leaders of various clients we've had across many different industries in the wake of data breaches.

For the benefit of our networks and readers, we've summarised the key takeaways in our view for each of the questions that directors should ask in the wake of a data breach. We also quote from part of the recommendation points under each question.

These questions – if asked at the right time – can help uncover key issues in the moment of a data breach. They provide a trustable, bankable list of inquiries that can help reduce the pain and improve the chance of a much more productive rebound out the other side.

1. Is the investigation in the aftermath of the breach independent?

In a nutshell, to ask in-house teams to investigate a breach risks giving rise to (essentially) conflicts of interest. It is likely that in such cases the very people investigating the breach were those tasked with preventing it in the first place.

A common occurrence we observe is data breach victims asking their Managed IT providers, the team primarily involved with setting up the IT network environment to contain or provide any form of investigative advice about the data breach. Any resulting view could suffer from a serious lack of objectivity.

The AICD thus recommends:

Have a senior officer other than the head of IT or chief information security officer engage a third-party IT forensics specialist to investigate and report. Have the investigator primarily engaged by an officer outside the IT and IT security teams.

Australian Institute of Company Directors

2. Is important evidence being preserved?

Steps taken to prevent a breach that is underway or to shut down a system that is part of a compromise can lead to the erasure of key evidence about the nature of the attack. The importance of preserving evidence, then, is paramount to analysis, recovery, and proactive guarding against future issues. Without an effective log management and retention program, the critical forensic information which management needs can often be lost by the time a forensic analyst can begin an investigation.

The AICD recommendation:

Make sure the independent forensic investigators get to the system as soon as possible and take an image. Ask that a record of the state of the system at the time of the breach is retained and that procedural steps are being recorded and reported.

Australian Institute of Company Directors

3. Will the investigation produce documents that may be used against the company?

Those investigating the breach may uncover some documents the conclusions in which may be damaging in legal or regulatory investigations. This is a matter for organisations' compliance, risk, and governance functions, not investigators putting together a fact base. Investigators need to focus on identifying facts associated with the cause of the breach and allow these respective functions to play their relevant role.

The AICD recommendation on this sensitive area:

> *Ensure that investigators focus on identifying and reporting factual information. Separate assessments of responsibility can be the focus of a subsequent governance process. Have the General Counsel of the company, or an external law firm, engage the forensic investigators for the purpose of providing legal advice and restrict circulation of the forensic report to those making decisions regarding the legal interests of the company.*
>
> Australian Institute of Company Directors

4. Have we identified the relevant categories of information that have been compromised and stakeholders associated with them?

"Data breaches" can be of varied types. Some examples include:

- Discrete elements of broader data sets (e.g. names, addresses)
- Email address of employees of a company
- Customer information

to name but a few.

Minimising the damage that arises from a data breach requires rapid **identification of each category** of compromised information and its associated stakeholders. In most cases, advising affected parties sooner is more likely to mean that they will regard management of the incident as competent and candid.

The AICD recommendation:

> *Make sure there is a rapid review and analysis of potentially compromised information, including the extent to which the information gives rise to contractual or regulatory obligations, and identify the extent to which any key stakeholder relationships may be at risk.*
>
> Australian Institute of Company Directors

5. Have we considered the best ways to limit the possible damage?

In the moment of a data breach / incident, cool heads need to prevail. While the broader reputational concerns that result in the moment are understandable, they need to be (at least temporarily) put to the side to consider how — in sheer immediate and practical terms — the impact of a data breach may be limited.

In many cases, the information lost or compromised may not be particularly sensitive or useful, with the majority of concern over its loss coming from its potential use in phishing or phone scams (for instance).

Immediately practical actions following a breach may range from an email asking recipients not to open an email to changing passwords and requiring all users to authenticate their accounts. Whatever the case may be, in the immediate aftermath, think **practically and pragmatically** to limit the imminent damage.

The AICD recommendation captures this succinctly:

> *Turn your mind to practical steps that might mitigate or prevent potential harm arising from the compromise. Foremost among these is advising and warning the data subjects that they may be at risk.*
>
> Australian Institute of Company Directors

6. Has the company breached applicable regulatory obligations? Should we notify the regulator?

All Australian companies with an annual revenue of more than $3 million p.a. are considered 'APP entities' under the Privacy Act 1988 (C'th), and as such may be subject to investigation and notification obligations following a data breach.

When an APP entity suspects that there may have been unauthorised access to or disclosure or loss of personal information it holds, it is required to carry out a reasonable and expeditious assessment to determine whether an eligible data breach has occurred. The Office of the Australian Information Commissioner (OAIC) expects that entities subject to a data breach will complete this assessment within 30 days

of discovering the incident, if not sooner. Organisations need to be cognisant of this time frame when responding to a data breach, as a failure to do so may result in a higher level of scrutiny from the OAIC and others if notification is eventually required.

When determining whether a data breach is notifiable, APP entities must consider the extent, if any, of unauthorised access to its network, whether the data breach is likely to result in serious harm to affected individuals, and whether any remedial steps can be taken to prevent harm occurring. If unauthorised access and a likelihood of serious harm are confirmed, and no remedial steps are available, an APP entity will be under an obligation to notify the OAIC and affected individuals as soon as practicable. The question leaders should be asking is:

Do the circumstances of the incident suggest that notification is required? What technical and legal assistance do I need to assess this? What can I do to prevent harm from occurring?

In addition to obligations under the Privacy Act, financial services companies that are regulated by the Australian Prudential Regulatory Authority are subject to additional assessment obligations such as CPS 234. These companies may be required to notify the regulator in the event an incident occurs which compromises a core system. Other overlapping State and Territory Privacy Laws and regulations may also apply to specific industries and in addition to those discussed above.

While the situation varies from industry to industry, leaders need to be aware of the applicable legal and regulatory obligations and should be prepared to conduct an assessment to determine whether notification to a regulator is necessary. Legal advice from leading breach coach privacy counsel who have experience managing data breach investigations and working with regulators and law enforcement bodies day to day is critical. While there are several law firms that 'do this work', there are some that have specialised in cyber incident response and it pays to get good counsel from those specialty firms.

The AICD recommendation in this regard is to:

Be proactive in communicating with regulators and take advantage of the cyber-attack defence expertise provided by the ACSC.

Australian Institute of Company Directors

7. Has the company breached applicable contractual obligations?

This is one of the most serious and pressing questions to consider.

A data breach can damage commercial relationships with customers and suppliers and may give rise to **breach of contract**. As a result, it is crucial that all commercial contracts are assessed following a data breach to determine whether notification is required. If so, it is important to act fast and decisively to notify customers and suppliers of the breach, as this will help preserve any existing business relationships.

Important considerations are whether intellectual property has been lost, whether the data breach violated the contractual duty of confidentiality, and whether notification of a suspected or confirmed data breach is enshrined within the contract itself. Beyond data risk, you should consider whether the incident places any of your suppliers at risk of lateral attack against their systems and ensure that you advise them accordingly of what security steps need to be taken to prevent this from occurring (for example issuing a warning about phishing emails being propagated).

When considering whether notification to customers and suppliers is necessary, it is important to look at the circumstances of the breach holistically and decide whether it is in the best interests of all parties to advise them on what has occurred. Managing a multi-party data breach incident is complex and requires a well-considered strategy, to ensure that all affected parties' interests are well-managed, and that third party B2B claims are minimised. The AICD recommendation mimics the above and recommends a consideration of the commercial relationship and what impact notification might have.

Consider how news of the data breach will impact your relationships with your customers and any contractual obligations may have been breached.

Australian Institute *of* Company Directors

8. What is the communications strategy?

Data and cybersecurity are a major news interest today and there is no getting away from this fact.

Information can reach the media if news of the breach is communicated broadly within the company, if there is a leak from a supplier or in a myriad of other ways.

As one company director has aptly noted, "uncontrolled communication regarding the data breach can be as bad as the data breach itself". Thus, the pertinent AICD recommendation, which states:

> *Consider a strategy to take control of information regarding the incident. Prepare to handle enquiries and the substance of the information to be communicated. Take steps to ensure that key stakeholders are advised by you rather than finding about it from public sources.*
>
> Australian Institute of Company Directors

9. Make sure any report or analysis is complete

In most cases where data breaches require mandatory notification to the **OAIC** or relevant industry bodies, they require a **description of the breach** including the kind or kinds of information concerned.

Where a breach is likely to be notifiable, a key part of the investigation must be aimed at **learning enough about what has happened** to enable the company to accurately describe the breach.

An assessment of the likelihood of serious harm changes substantially if — for instance — an organised, criminal threat actor is involved.

Thus, the **AICD recommends** that your forensic investigator should provide a "clear picture" of the information available about issues including:

- the method of attack;
- whether any harmful code was used in the attack;
- whether any social engineering was used in the attack;
- the date and time the attack first occurred;

- each step taken as part of the attack and the date and time of each step;
- the systems and information accessible to the attacker and the period during which each was accessible;
- any evidence that information was deleted, modified or exfiltrated from the system and our conclusion on that evidence;
- any evidence that a system or software was deleted, modified or exfiltrated from the system and your conclusion on that evidence;
- any evidence or inference regarding the identity of the attacker;
- any evidence or inference regarding the reasons for the attack;
- all available information regarding the information that was or is suspected to have been compromised;
- if a back-up was used to re-establish operations, the period for which data has been lost and a description of the subject information;
- whether or not personal information was compromised, and your assessment of the likelihood of serious harm to any data subject;
- whether you are confident that the compromise has been remediated including whether all ongoing means of access to the system by the attacker (including access to accounts and passwords) have been updated and checked; and
- the recommendation to prevent a recurrence and when these steps will be complete.

10. Has the company taken steps to ensure that lessons arising from the incident have been learnt and actioned?

This may seem like a no-brainer, but it is remarkable how often this important, future-oriented point is missed in action.

Companies that are in more advanced stages of maturity in their overall cybersecurity posture will have standard guidelines to review, remediate and change following an incident.

A good, mature process should see a focus on improving the security architecture or defensive arsenal maintained by the business, improving logging of incidents, reporting of breaches and the resources and time devoted to security.

The **AICD recommendation** is for companies to:

> *remain engaged with the debriefing and remediation process following the breach with a view to improving monitoring, reporting and oversight of the cyber security framework maintained by the company.*
>
> Australian Institute of Company Directors

"I want to thank legal and incident response specialists Clyde & Co for their assistance to Gridware and myself in preparing this article. We regularly collaborate with their team on data breach and cyber incident investigations, including several of the largest and most complex incidents in Australia to date. Let us know if you would like us to introduce you to the Clyde & Co team to discuss your legal risk and gain a better understanding of the regulatory risk landscape."

Ahmed Khanji

(CEO, GRIDWARE)

Ahmed Khanji is the CEO of Gridware, a leading cybersecurity consultancy based in Sydney, Australia. An emerging thought leader in cybersecurity, Ahmed is an Adjunct Professor at Western Sydney University and regularly contributes to cybersecurity conversations in Australia. As well as his extensive background as a security advisor to large Australian enterprises, he is a regular keynote speaker and guest lecturer on offensive cybersecurity topics and blockchain.

Reece Corbett-Wilkins

(PARTNER, CLYDE & CO)

Reece is a leading member of Clyde & Co's cyber incident response team and has experience acting in a range of local, regional, and global incidents affecting government agencies and private sector organisations of all sizes, operating across all industry sectors.