Australian Institute of Company Directors

ORGANISATION

Managing a data breach: Ten oversight questions for directors

A data breach of scale can be a crisis. If it is not well-managed, it can cause substantial damage to a company and its directors both financially and in terms of reputation. It can also have serious regulatory implications.[1]

Like any crisis, the breach, or the realization that a breach has occurred, can arise without warning. The response of management can be reactive rather than strategic. The role of the director is to see the wider implications associated with the incident, including to identify and oversee steps that will help to mitigate damage in the medium and longer term.

This director tool provides as list of questions to help identify issues that can arise in the context of a data breach. It aims to assist you to provide governance oversight with appropriate care and diligence should the need arise. This is not a list for management of all steps that might be necessary or desirable.

1. Is the investigation independent?

The natural response of company management to a cyber incident is to ask the head of IT or the chief information security officer (if the company has one) to investigate and report. However, it is most likely that these officers and their departments had primary responsibility for preventing the breach. Accordingly, any report they produce might be challenged for lack of objectivity or completeness. For any serious incident with implications for existing systems and processes, the company should obtain an independent report.

Recommendation: 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.

1. As recently as 21 August 2020, the Australian Securities and Investments Commission (ASIC) commenced proceedings against a financial services provider in relation to alleged weakness in business systems and risk management identified because of a cyber-attack.

2. Is evidence being preserved?

A common challenge with data breach investigations is the existence of evidence. Steps taken to prevent a breach that is underway, and/or to shut down a system that is part of a compromise, can erase evidence regarding the time, manner, source and/or other characteristics of the attack. In addition, the steps taken by IT personnel, including the time they were taken and the order in which they occurred, can be relevant to interpreting information relating to the breach when circumstances allow.

Recommendation: Raise the issue of record-keeping and evidence with the management team. 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.

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

There is a risk that those investigating the breach or reporting on the breach will include in their communications or reports, conclusions regarding cause and responsibility. Documents containing conclusions of this kind can be damaging in subsequent legal proceedings or regulatory investigations. As a procedural matter, it is better for the investigators to focus on identifying facts associated with the cause of the breach and allow evaluative assessments to take place subsequently as part of the company governance process.

Recommendation: 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. If the forensic investigation takes place for the purpose of preparing legal advice it will be protected from disclosure to third parties by legal professional privilege.

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

A data breach can impact a discrete data set such as a list of names and addresses or a dataset with mixed subject matter. A common data breach of the second kind is where an email of a company employee has been compromised. Depending on the role of the employee and the frequency with which email is archived or deleted, personal information that is sensitive in nature might be found in employee performance reports, medical and sick leave reports, customer complaints, industrial incident reports, payroll and bonus information. Strategic and confidential information might be contained in customer requests, IT architecture and security frameworks and financial information associated with sales and profitability. Minimising the damage that arises from a data breach requires rapid identification of each category of compromised information and its associated stakeholders. Generally speaking, the sooner the parties who may be adversely affected are advised of the incident, the more likely they will regard your management of the incident as competent and candid.

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.

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

A common data breach remediation involves calling the recipient of a misdirected email and asking them not to open but to delete the contents of the message sent in error. In other cases, lost or compromised devices can be locked or wiped remotely before information is lost. It is reasonably common practice to change all the passwords and require all users to re-authenticate when there is a possibility that access credentials have been compromised. There is also a common situation where the information lost is not sensitive or particularly useful – perhaps comprising only a name and address or a name and a phone number – but it is suspected that the information is in the hands of a criminal operation that may use it for phishing or a phone scam. In this situation, a warning note to the individuals concerned to be on guard in relation to unsolicited contacts may help to prevent harm.

Recommendation: 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.

6. Has the company breached applicable regulatory obligations? Should we be in touch with the regulator?

All Australian companies with revenue of more than $2 million per annum are subject to Australian Privacy Principle 11[2], which requires such steps as are reasonable in the circumstances to protect personal information from misuse, interference, loss unauthorized access, modification or disclosure. Does the data breach indicate that company failed to take reasonable steps in the circumstances? Financial services companies regulated by the Australian Prudential Regulatory Authority are subject to CPS 234[3] and are obliged to notify the regulator if an incident may compromise a core system.

It may be prudent to contact the regulator even where there is no notification obligation in order to ensure the regulator learns of the incident from the company, has an understanding of the steps being taken to address the issue and, perhaps, to forestall adverse public comment. Consideration should also be given to contacting the Australian Cyber Security Centre (ACSC) to report the attack, obtain assistance and possibly additional information regarding the associated malware and oblique or the experience of other companies.

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

2. Office of the Australian Information Commissioner, Chapter 11: APP 11 – Security of personal information, [website], https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-11-app-11-security-of-personal-information/, (accessed 14 September 2020).
3. Australian Prudential and Regulation Authority, 2019, Prudential Standard CPS 234 Information Security, July, https://www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf, (accessed 14 September 2020).

7. Has the company breached applicable contractual obligations?

A data breach can seriously damage commercial relationships with customers and suppliers and may give rise to breach of contract. The most obvious cases are where the attack targets intellectual property that may be licensed or shared with a venture partner and where the subject matter compromised by the breach is subject to contractual duties of secrecy. If your company's business is to provide a platform for the use of third parties or the processing of third-party information the breach may give rise to a claim by customers under their contracts for supply. In some cases, a service will be supplied directly into the information system of your customer and/or the information that has been compromised includes the security architecture of a customer or partner. Consider whether you have provided any customers with responses to data security questionnaires or statements regarding your security posture which might be inconsistent with or at least brought into question by the data breach.

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

8. What is our communications strategy?

A major data breach is newsworthy. Information can reach the media if news of the breach is communicated broadly within the company, if there is a leak from a supplier, because compromised information has been published, a customer system was down, and/or an ill-considered public explanation given that suggests the company has suffered an attack. Uncontrolled communication regarding the data breach can be as bad as the data breach itself.

If the subject matter of the data breach and the risk of harm to data subjects is such that you are obliged to notify under the mandatory data breach notification scheme and the Privacy Act 1988 (Privacy Act), or you elect to contact affected individuals so they have the opportunity to prevent potential harm, the breach will become generally known as a result of your communications.

Recommendation: 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.

9. Make sure the report is complete

If the data breach involves personal information and is likely to result in serious harm to any individual, the mandatory data breach notification provisions of the Privacy Act require notification of the Office of the Australian Information Commissioner and the data subject soon as practicable. However, the notification must include a description of the data breach including the kind or kinds of information concerned. Where a data 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 data breach and the kind or kinds of information concerned in accordance with this requirement.

Having a good understanding of what has happened is also necessary for assessing whether or not serious harm is likely to be suffered by any data subject. Your assessment of the likelihood of serious harm changes substantially if you believe you have a sophisticated organized criminal attacker and/or that information was exfiltrated from your system at scale.

Recommendation: Make sure your forensic investigator provides a clear picture of the information available about the following issues:

- 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 your 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 captured and appropriate action taken?

If your company has a data breach response policy, and/or follows any of the standard guidelines, review, remediation and adaptation following the incident will be prescribed. This process is often focused 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 incident will also expose gaps in the allocation of responsibilities, gaps in mechanisms for communication and coordination between different stakeholders and highlight information and issues that should be monitored and reported. The latter are procedural governance issues where directors can provide valuable insight and oversight.

Recommendation: 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.

Conclusion

Having the right information technology operating efficiently and effectively is fundamental to the success of a modern business enterprise. If the system is not up and running, revenue can be lost. If the security of the system is compromised, the trust of customers, suppliers and regulators can be irreparably damaged. In the context of risk oversight of data breaches, effective directors need to ensure the strategic issues at stake are identified so that regulatory obligations are complied with and unnecessary operational and reputational damage is avoided.
The questions in this tool will help you to anticipate and moderate risks and challenges associated with a data breach incident.

Related AICD Director Tools

- *National security compliance for directors*
- *The consumer data right framework*
- *Data and privacy governance*

About the author

Patrick Fair GAICD BEc LLB CIPM FAISA, is the principal of Patrick Fair Associates; an Adjunct Professor at the School of Information Technology, Faculty of Science, Engineering and Built Environmental, Deakin University; the Chairman of the Communications Security Reference Panel at the Communications Alliance; and General Adviser for LexisNexis Practical Guidance Cybersecurity, Data Protection and Privacy.

About us

The Australian Institute of Company Directors is committed to strengthening society through world-class governance. We aim to be the independent and trusted voice of governance, building the capability of a community of leaders for the benefit of society. Our membership includes directors and senior leaders from business, government and the not-for-profit sectors.

For more information t: 1300 739 119 w: aicd.com.au

07236-6-33_20