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.

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.

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.

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.

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.

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

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.

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".

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.

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.

Source:

Ahmed Khanji
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.

The questions your board needs to hear.

Here is a list of seven questions to ask to make sure your board understands how cybersecurity is being managed by your organization. Simply asking these questions will also raise awareness of the importance of cybersecurity, and the need to prioritize action.

1. **What are our most important assets and how are we protecting them?**

We know we cannot be 100% secure. Difficult decisions must be made. The BOD must make sure the organization's most important assets are secure at the highest reasonable level. Is that your customer data, your systems and operational processes, or your company IP? Asking what is being protected and what needs to be protected is an important first step. If there is no agreement on what to protect, the rest of the cybersecurity strategy is moot.

2. **What are the layers of protection we have put in place?**

Protection is done with multiple layers of defense, procedures and policies, and other risk management approaches. Boards don't need to make the decision on how to implement each of these layers, but the BOD does need to know what layers of protection are in place, and how well each layer is protecting the organization.

3. **How do we know if we've been breached? How do we detect a breach?**

The BOD would be ignoring an important part of their fiduciary responsibility if it does not ensure that the organization has both protection and detection capabilities. Since many breaches are not detected immediately after they occur, the BOD must make sure it knows how a breach is detected and agree with the risk level resulting from this approach.

4. **What are our response plans in the event of an incident?**

If a ransom is sought, what is our policy about paying it? Although the board is not likely to be part of the detailed response plan itself, the BOD does want to be sure that there is a plan. Which executives and leaders are part of the response plan? What is their role? What are the communications plans (after all, if systems are breached or unreliable, how will we communicate?). Who alerts authorities? Which authorities are alerted? Who talks to the press? Our customers? Our suppliers? Having a plan is critical to responding appropriately. It's highly unlikely the plan will be executed exactly as designed, but you don't want to wait until a breach happens to start planning how to respond.

5. **What is the board's role in the event of an incident?**

It would be helpful for the BOD to know what their role will be and to practice it. Is the board's role to decide on paying a ransom or not, to talk to the largest customers, to be available for emergency meetings with organization execs to make just-in-time decisions? An earlier article of ours discussed the importance of practicing

responses. Using fire drills and tabletop exercises to build muscle memory sounds like a luxury, but should your company have an incident, you want to be sure that response muscle is ready to work.

6. What are our business recovery plans in the event of a cyber incident?

Many execs we have interviewed have not tested their business recovery plans. There can be significant differences in the recovery from a business disruption due to a cyber incident. Data recovery might be different if all records are destroyed or corrupted by a malicious actor who encrypts files or manipulates them. BODs want to know who "owns" business recovery, whether there is a plan for how to make it happen, and if it has been tested with a cyber incident in mind?

7. Is our cybersecurity investment enough?

You can't invest enough to be 100% secure. But since a budget must be set, it is crucial that companies guarantee they have an excellent security team with the appropriate expertise to tackle technical problems and understand vulnerabilities inside the core critical functions of the business. By doing that, the company will be better prepared to allocate investment where it is most needed. Companies should evaluate their level of protection and their risk tolerance before they engage in new investments. Two ways to do this are through simulations of cyber-attacks and from penetration/vulnerability tests. These actions expose vulnerabilities, enable actions to minimize potential damage based on priority, risk exposure and budget, and ultimately ensure appropriate investment of time, money, and resources.

Boards have a unique role in helping their organizations manage cybersecurity threats. They do not have day to day management responsibility, but they do have oversight and fiduciary responsibility. Don't leave any questions about critical vulnerabilities for tomorrow. Asking the smart questions at your next board meeting might just prevent a breach from becoming a total disaster.

Source: **Dr. Keri Pearlson** is the Executive Director of the research consortium Cybersecurity at MIT Sloan (CAMS). Her research investigates organizational, strategic, management, and leadership issues in cybersecurity. Her current focus is on the board's role in cybersecurity.