SECURITY INCIDENT RESPONSE: BACK TO BASICS FOR GENERAL COUNSEL

NOVEMBER 2023

Weil

You take a call from your head of IT or chief information security officer ("CISO"), late on a Friday night (hackers love to ruin weekends), *"We think the business has been subject to a cyber-attack"*. As general counsel ("GC"), your responsibility is to manage risk, and it is likely that you will be required to take a lead role in responding to this security incident. You need to mobilise and fast. Below we set out a rundown of the key considerations and actions that should be front of mind when you put down the phone...

1. FAIL TO PREPARE AND PREPARE TO FAIL

The organisation's response planning should have begun long before you take the call. Consider it a matter of when, not if, your organisation will encounter a security incident ("**Incident**"). The more prepared you are, the more likely it is that you, and the organisation, will be able to navigate this significant and stressful event effectively, minimise external scrutiny and limit the damage to the organisation's reputation and valuation.

Your response planning should involve, as a minimum, an assessment of the organisation's risk profile by conducting regular vulnerability scans and penetration testing. Such assessment will enable you to identify vulnerabilities and risk factors so that you can formulate a tailored strategy for navigating Incidents when they occur. Document the strategy formally in a security incident response plan ("**Plan**"). Include clear and suitably detailed policies and procedures in it to halt an Incident, minimise damage and prevent future occurrences; but ensure this requirement is balanced against the need for the Plan to be practical and easy to read and implement in an emergency. If it is too long, technical, or prescriptive, the Plan may be more of a hindrance than a help.

Whilst the Plan will require sufficient detail to guide those involved through an Incident, it should recognise and acknowledge that not all Incidents are predictable, and should allow for flexibility and deviations as appropriate to address novel Incidents. Ideally, your Plan will provide guidance on documenting deviations that are deemed necessary, so that in the event that a regulator queries why the Plan was not followed, you can provide the rationale for this.

Regular testing of the Plan is essential (for example, by way of simulation or table top exercises), to ensure that it is 'fit for purpose' (particularly in light of the rapidly evolving threat environment), that weaknesses are identified and remediated and that all appropriate stakeholders are familiar with it and understand their roles and the expectations of them in the event of an Incident. Familiarity with the Plan, and what is required, will help to contain the inevitable panic associated with an Incident and optimise response times, which is crucial in containing harm caused by an Incident.

You should familiarise yourself with the technical language in the Plan. Understanding the difference between a credential compromise, a DDOS and a phish will mean that you are on the front foot when your CISO and/or Head of IT needs to discuss the Incident with you. A thorough Plan will identify the different types of possible Incidents within scope and provide a glossary of common technical terms.

When you take the call, even if you are very familiar with its contents, take a moment to consult the Plan. In the heat of the moment, it is easy to miss an important step/consideration. As noted above, there may be Incidents that require you to divert from the prescribed procedures; a firm understanding of the organisation's formal Incident policy and baseline as to the response will mean that you can assess, swiftly and appropriately, whether deviations are necessary.

If your organisation does not have a Plan in place, put one in place as a matter of priority, particularly in light of the fact that many privacy and cyber regulations expressly require certain organisations to adopt policies, procedures, and in some cases, written plans, to address Incidents.

2. INCIDENT RESPONSE TEAM

Your Plan should outline who should be involved in the Incident response (which may be dictated by the nature of the Incident), and their contact details, as well as a prescribed 'notification list', which may include individuals who may not necessarily be part of the Incident response team, but who are sufficiently senior to warrant being notified. The prescribed lists should act as a baseline, but again, you may need to deviate and make a decision as to a notification (for example, if the Head of IT is on holiday and you cannot reach them). It is prudent to communicate by phone or video conference, at least in the initial stages. Committing information to paper or email, before the next steps have been established, may jeopardise any legal privilege over the contents. See Section 6 below for further discussion of legal privilege.

Once the Incident response team has been informed and a meeting called, a determination as to the actions necessary for containment, eradication and recovery of the Incident should be made. All actions and next steps should be as specific as possible, and the lines of communication and reporting channels clear to minimise any misalignment on process. Collaboration and unity between those involved in responding to an Incident is vital and you should set the tone for such co-operation.

3. INITIAL IMPACT ANALYSIS

In short order, you need to gather as much information about what has happened as possible. Accept that in the early stages, the information available may be very limited. Identifying and establishing what you know, and what you do not, will help to guide and determine next steps, prioritise the investigation and categorise the Incident. A robust Plan will contain a list of the questions to be posed and answered at each stage of the Incident detection, containment and recovery. Involving third parties, such as forensic experts to help with the investigation may well be necessary.

As soon as possible, establish whether personal data, special category data, financial data and any other data which is subject to regulation, has been impacted by the Incident, so that a determination can be made as to whether there are, or may be, regulatory requirements for reporting the Incident. The timelines for regulatory reporting can be very short; in certain jurisdictions notification is required to a data supervisory authority within as little as one hour of the Incident being discovered. Compliance with such timeframes should be considered as early on in the Incident response as possible. See Section 5 below for further discussion of notifications.

If the Incident is likely to threaten business continuity, you will need to invoke the organisation's business continuity and disaster recovery plans, which may involve the coordination of a separate team. You will need to consider the limitations of the organisation, particularly with respect to crisis management capabilities and forensic IT expertise, so that you can determine whether you need to engage third parties to advise the organisation, such as PR, external legal counsel and forensic IT consultants. If the Incident involves ransomware, take legal advice before making a payment, as in certain jurisdictions, making such a payment may expose the organisation to civil and criminal penalties.

4. COMMUNICATIONS

Careful management of the narrative concerning the Incident, particularly with customers and shareholders, will be critical in preserving, and limiting damage to, the organisation's reputation. Further, any statement made may have an impact on future litigation relating to the Incident. Communications to those internally, but outside of the Incident response team and the prescribed notification list, should be made on a strictly 'need-to-know' basis and validated by you and/or an alternative appropriately senior stakeholder prior to sending. All external communications about an Incident (including the media) and the response to parties (individuals or corporations) should require similar approval and sign-off and if relevant/appropriate, the approval from the organisation's PR/communications/investor relations team/s. You should be consulted before any response is made to a request from a regulator, law enforcement agency or stock exchange(s) to determine the appropriate response.

5. NOTIFICATIONS

With the help of your external legal counsel, you will be responsible for assessing whether any kind of contact with or a formal notification to, a data or financial regulator, a supervisory or governmental body, or other third parties (such as the organisation's insurer, law enforcement, employees, customers or suppliers) is required and for making any contact/notification. For example, if there has been a breach of personal data, a notification to a data supervisory authority may be required; if your organisation is regulated in the UK by the Financial Conduct Authority, a notification may be required if the Incident is reasonably believed to be 'material' and/or if there is a suspected fraudulent element. In the US, publicly traded companies must report a 'material' cybersecurity incident within four days of determining it is material under the Securities and Exchange Commission's Cybersecurity Rules.

Whilst the timeframes within which a notification must be made can be very short, this should not undermine the need to analyse, critically, whether an assessment needs to be, or should be made and what information to include. You should assume that anything that is communicated in a notification may become public (in the UK, a notification concerning a personal data breach, to the Information Commissioner's Office will be made public; certain US states also maintain public databases of reported incidents), so you should ensure that what is included is accurate, notwithstanding the fact that you might not yet know the full picture.

6. LEGAL PROFESSIONAL PRIVILEGE ("LPP")

Investigations of the Incident may involve the creation of documents analysing the Incident (or communications about the Incident, such as emails), which the organisation may wish to maintain subject to applicable LPP to the fullest extent possible under applicable law in relevant jurisdictions. Such LPP may be deemed to be waived if it is not asserted at the outset of the investigation and/or might not extend to areas of the investigation in which the legal team are not involved. Accordingly, you should implement appropriate steps in the Plan, and during the initial phase of the Incident response, to preserve LPP and ensure that the Incident is documented (and such documents are appropriately disseminated) based on your advice.

FOR MORE INFORMATION

If you would like more information about the topics raised in this briefing, please speak to your regular contact at Weil or to any of the authors listed below.

BARRY FISHLEY

+44 20 7903 1410
barry.fishley@weil.com

BRIONY POLLARD

+44 20 7903 1372
briony.pollard@weil.com

WEIL.COM

#97864250

Weil