How Counsel Can Effectively Lead Data Breach Investigations

By **Oliver Price and Kevin Hughes** (October 14, 2022)

Oliver Price

Kevin Hughes

As cybersecurity incidents and data breaches become more prevalent and more complex, so do the resulting legal implications.

Lawyers and legal professionals are increasingly positioned at the center of these events, having to act as the interlocutor between disparate technical teams — from understanding cyberinsurance policies to reporting to the appropriate regulatory authorities in multiple jurisdictions.

Therefore, having realistic expectations on how to approach an incident response investigation is crucial. Utilizing the experience gained through collaborating with legal professionals during these investigations, including standing shoulder-to-shoulder with general counsel, technical information and pitfalls that legal professionals should be aware of have been identified and collected.

All of this sits within the wider context of an increased risk of litigation as a result of any missteps made in response to an incident. The latest example being Optus, which already appears to be the target of a class action in Australia after personal data on 9.8 million customers was stolen only a few weeks ago.

This increased litigation risk further underlines the importance of legal guidance throughout.

The topic of legal consequences and particulars surrounding cybersecurity incidents has been thoroughly covered. Increasingly, however, organizations facing cybersecurity incidents are relying on their general counsel to take a leading role in the incident response and management of these types of situations.

This reliance on the general counsel inevitably places significant pressure on that individual to quickly gain control of complex and technical subject matter during a time that is already typified by an extreme lack of information.

In the immediate response to an incident, details regarding what exactly happened, or what systems, networks and information were affected, can be challenging to gather.

Because time is of the essence, it is also common for these situations to see a large number of new teams and relationships form quickly, including through the need to utilize outside expertise, such as specialist incident response teams.

Managing an External Incident Responder

During the critical first few hours and days of an incident, when working with an external incident response team, the general counsel is responsible for ensuring proper progress is being made.

However, how is it possible to spot the difference between a response team making progress under difficult circumstances, and a team incapable of providing necessary

answers to advise senior leadership on the current state of risk and operational impact?

While it is difficult to reduce incident response to a checklist, for the first week or two, a daily meeting to track progress of the incident response team should be expected, with a briefing on the following:

Investigation

- What compromised systems have been found?

- What are the next pieces of evidence to be collected and when is this expected to be completed?

Containment

- What technology or processes are now in place to detect suspicious activity?

- How complete is the coverage and implementation of these technologies or processes?

- When will implementation be completed?

- What measures have been taken to remove malicious access — e.g., resetting compromised accounts and removing compromised systems?

- When will these measures be completed?

Remediation

- What measures can be taken to reduce the likelihood of an attack in the near future before the incident investigation is complete?

- When will these measures be completed?

Managing a Ransom Negotiation

A more specific, yet common, question that general counsel is often required to advise on is how to engage with extortion, or more specifically, paying a ransom.

The topic of potential legal and moral consequences of actually paying a ransom has also been thoroughly discussed, but the question of whether to engage in negotiation, even in bad faith without the intent to pay a ransom, is often not considered until an event occurs.

Simply engaging with the threat actor regarding paying the ransom can allow a victim organization to obtain additional time before the release of data or another attack.

Further, this can also provide an opportunity for the victim organization to request more information on what data might have been stolen during the attack, or any other details relevant to the response and investigation.

This is not an area where an organization should be handling interactions with the threat actor alone.

Experienced negotiators are critical to reducing the chance of negative outcomes, while also maximizing the chance to secure additional benefits from the interaction.

Again, trying to completely capture the process in a short checklist is an oversimplification of a challenging situation, but general counsel should expect the following from their briefings with negotiators.

Risk Management

- Clear advice on the risks and benefits associated with the various negotiation options.

- Clear expectations on timings for subsequent activity from both the threat actor and the negotiation team.

- Document who was engaged for negotiations — preferably via counsel — what sanctions checks were conducted, and any interactions with law enforcement or government agencies

Data Gathering

- A clear understanding of what data the negotiator is trying to obtain during the negotiation and the importance.

- Information on what data has been stolen by the threat actor — ideally a full list of the files — and a description of how they were able to gain access to the organizations' systems.

Ransom — If an Organization Decides It Wants to Consider Payment

- An expectation of what the likely discount that can be negotiated is, based on previous experience negotiating with this group.

- Advice on whether this threat group is likely to honor their word and provide decryption keys and delete stolen data, based on previous experience negotiating with this group.

- Advice on how they can assist in legal and regulatory checks to provide assurance that the threat group is not linked to a sanctioned entity.

Gathering Information for Regulators

Another, perhaps more familiar, area that general counsel is often required to lead, is interacting with regulators on the impact and extent of a cyber incident.

Without getting into the specifics of the many and varied regulations that organizations find themselves beholden to, gathering evidence and information for regulators is a critical element of an incident response investigation.

In the first few days and weeks, while the investigation is at its most chaotic, the questions that should be asked can be summarized into the following:

Impact

- What, if any, data has been taken or lost?

- What is the potential service impact and what impact is this going to have on the users who rely on those services?

Preexisting Controls

- What controls did the organization have in place to prevent this kind of incident from occurring?

New Controls

- What new actions has the organization taken to respond to this incident and reduce the chance of this happening again?

Comments

Some of these responses can be prepared well in advance — for example, a brief description of the security controls the organization has in place — while others require assistance from the external incident investigation team and the organization's operations teams.

Knowing that these are going to be the questions to answer in the first few days, however, should allow general counsel time to build this into the agenda for incident response management meetings and ensure answers are being prepared before the questions arrive.

Every cybersecurity incident and data breach is different, but from a legal perspective, the overall approach to incident response investigation remains largely the same.

Knowing what questions to ask an external incident responder to ensure appropriate progress is being made, how to effectively manage the ransom negotiation process to buy time and gather unknown details, and what information to collect for regulators to reduce or prevent penalties are all foundational elements.

Oliver Price and Kevin Hughes are senior directors in the cybersecurity group at FTI Consulting.