Get to Know your Incident response plan

What are Incident Response Plans?

Incident Response Plans (IR Plans) are comprehensive strategies designed to help organisations respond effectively to cyberattacks, data breaches, or other disruptive events. They should include all executive and responsible areas of your organisation including CEO, COO, IT, Security, Communications, and Legal

As General Counsel or in-house counsel, what is my role in an IR Plan?

Legal advisors play a crucial role in IR Plans as they provide vital guidance and support in navigating the complex legal landscape during and after a security breach or incident.

There is time criticality in getting legal involved. If legal isn't brought in until part-way through the breach, then incident response investigations, reports, and communications might all be discoverable in subsequent litigation and investigation.

So you need to be involved from the earliest moments your organisation has a breach.

BUT WHY?

1. Privilege
Incident response investigation and response will produce highly sensitive material. If not requested and controlled from the start by legal, this information may be discoverable in subsequent litigation and investigation.
See later in the GC Cyber Kick Start guides for a deep dive on this issue.

2. Compliance with laws and regulations:
You bring skills to the table that others don't have. Legal advisors possess in-depth knowledge of applicable laws, regulations, and industry standards related to data protection, privacy, and breach notification which are critical in the early days of breach response. You can help ensure that the organization's response aligns with legal requirements, minimizing the risk of legal consequences and potential penalties.

3. Risk management and liability mitigation:
By involving you early in the security breach, your organization can assess the legal risks associated with a security incident and develop strategies to mitigate them. Legal advisors help identify potential liabilities, evaluate contractual obligations, and guide the organization's response to minimize legal exposure.

4. Evidence preservation and chain of custody:
You are essential in assisting in preserving digital evidence and establishing a proper chain of custody. This ensures that evidence is collected, documented, and stored in a manner that maintains its integrity and admissibility in potential legal proceedings.

5 Communication with external stakeholders and regulatory notifications
It's important that you help manage communication with external parties, including law enforcement agencies, regulatory bodies, affected individuals, customers, and partners. This includes ensuring regulators are notified within strict timeframes, and in the order needed to meet your legal obligations. You also have a role to play in ensuring communications are accurate, consistent, and comply with legal requirements, safeguarding the organization's reputation and maintaining public trust.

6. Response strategy development:
You will need to contribute to the development of an effective response strategy tailored to the specific incident. You should be positioned to provide guidance on decision-making, such as whether to engage in negotiations, pursue legal action, or explore settlement options, considering your organization's situation.

Summary

In summary, you, as legal advisor to your organisation, are an indispensable part of Incident Response Planning and response.

Your expertise will help your organization navigate the legal complexities of security incidents, minimize legal exposure, and ensure a comprehensive and compliant response to protect the organization's interests and help them recover as quickly as possible.

You MUST be at the top of the call list when there is a security breach, and you need to know what to do when you get that call.

More to follow - keep following the Cyber Kick Start guides from Cyber GC.