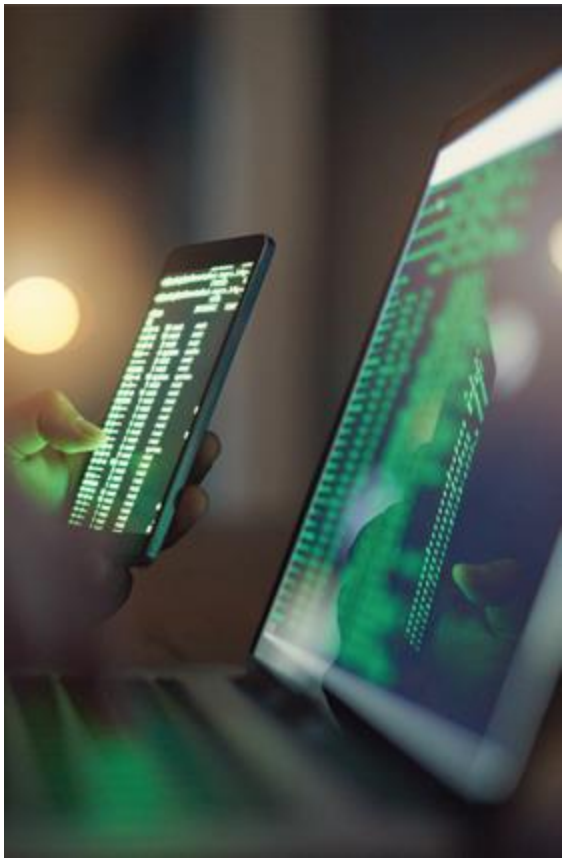
FAQs

Cyber Incident **Response Plan**



What is an Incident Response Plan and why is it important for our risk management?

A **Cyber Incident Response Plan (IRP)** is a document that outlines an organizations' playbook to respond to an actual or suspected Cyber incident. The goal of an IRP is to limit the overall damages of a cyber incident by planning policies and procedures to respond in a coordinated manner. An IRP starts by defining what an incident is. It will identify essential stakeholders from the C-Suite, Legal, HR, Communications and IT. It will also identify external first responders such as legal counsel (AKA the breach coach), forensic investigators and public relations firm. An IRP will generally classify different cyber incidents, identify roles and outline steps to respond based on severity.

Why does it matter?

It is well established that timeliness of response and preparation correlate to substantially reducing the total cost of cyber incidents. Additionally, there are practical business issues that should be addressed prior to a cyber incident such as how to define a potential incident and communicate that definition to employees and other stakeholders. It is also beneficial to identify critical external vendors *prior* to an actual event.

Where to start?

Building an Incident Response Plan is a separate exercise from purchasing cyber insurance, but it is worth nothing that cyber insurance policies allow for immediate access to first responders.

Start the process by reviewing the carrier's 'vendor panel' of pre-approved first responders that would serve you under a covered claim. Ask your broker to help you vet these vendors and consider drafting preliminary contracts with them. Cyber insurance carriers may also provide access to IRP templates that you can use as a starting point, as a best practice, this document should be drafted by an attorney that specializes in privacy and data security.

In your process to identify a breach coach – you should also inquire on resources available to draft an IRP to your business's specific risks and needs. Industries with higher volumes of third party Personally Identifiable Information (PII) and Protected Health Information (PHI) should especially consider this approach due to potential for legal liability and regulatory investigations. There is nuance as to drafting an IRP from a legal perspective that can assist in mitigating those risks.

We have an incident response plan. What's next?

Once you've built your IRP, the next step is to stress test the IRP against the most likely cyber incidents that might impact your organization. This process is typically called a tabletop exercise. The designated stakeholders noted in the IRP come together for a roundtable-exercise and respond to a simulated cyber event, challenging the team to respond with decisions and next steps in real-time. The breach coach will lead a tabletop exercise and provide a report with recommendations for improvement. The business can use this report to refine the IRP over time. The IRP should be a living document that is adjusted over time and stress-tested on a regular basis to contemplate new and emerging risks.

SUMMARY:

- **Businesses have traditionally seen the value in disaster response planning and are applying the same concept to Cyber risk.**
- **An Incident Response Plan is a practical document that outlines how a business should respond to a cyber incident and identifies the parties that are responsible for steps in the process.**
- **A well-crafted Incident Response Plan can reduce the magnitude of a Cyber event.**
- **Incident Response Planning is made easier by utilizing the resources of your Cyber insurance policy.**
- **The IRP should be completed by a qualified attorney and stress-tested to assure it's comprehensive and effective.**