Incident Response Plan Checklist

Every organization can experience a breach.

According to Inc., 60% of all companies that suffer a data breach are forced into bankruptcy within six months. We don't want you to be in that group. So this checklist can help you start the process of developing a well-thought-out incident response plan (IRP). If the plan is well-designed and executed, you can reduce risks significantly.

How to use this checklist:

1) Review the list. Items on the list are what you need in a basic IRP

2) Make notes and mark down the areas you need to work on

3) Share this with your team when you are done.
Your team needs to be aware of the plan for execution.

Preparation for a Breach

Who is the incident handler?

☐ Do you have communication paths designed so that an inbound email will get to the right person?

If not, the steps to get this set up are:

☐ Do you have functional logging to help you determine the scope of the incident?

Action items:

Detection and Analysis

How will you determine the scope of an incident?

Who will lead the process of incident handling?

If it is a significant incident, do you have a retainer with a third party? Yes

Who is responsible for communicating with the security researcher?

Contact Kobalt at sales@kobalt.io when you need guidance on developing your plan and process.

Incident Response Plan Checklist

Containment, Eradication and Recovery

What do you do to contain a breach? What don't you do? Will you take production systems offline?

How will you validate that your patch/security measure has eliminated the vulnerability?

Who is responsible for making the decision about the blackmail demand?

If you agree to pay for data recovery, who provides the budget?

What is your procedure for communicating the breach authorities and customers?

Who is responsible for communicating details on the breach to clients, press, privacy commissioners, others? Do you have draft communications ready to go?

Does your IRP capture your contractual obligations for communication? Does it capture regulatory obligations?

How do you validate there are no other breaches in your systems?

Post-Incident Activities

Who needs to be involved in the post-incident activities?

Contact Kobalt at sales@kobalt.io when you need guidance on developing your plan and process.