Cyber Incident Response Plan

OVERVIEW

An Incident Response Plan is a written document which is approved by the senior leadership team, that helps your organization before, during, and after a confirmed or suspected security incident. Your IRP will clarify roles and responsibilities and will provide guidance on key activities. It should also include a cybersecurity list of key people who may be needed during a crisis.

BEFORE A CYBERSECURITY INCIDENT

- **Train the staff**. All staff need to understand their role in maintaining and improving the security of the organization. That includes knowing how to report suspicious events. Be gracious when people report false alarms. Reward people who come forward to report suspicious events as part of your commitment to a culture of security. • Review your plan with an attorney. Your attorney may instruct you to use a completely different IRP template. Attorneys often have preferences on how to engage with outside incident response vendors, law enforcement, and other stakeholders.
- **Meet your local laws**. In coordination with your local police. The time to figure out how to notify LEA representatives.
- **Print IRP documents** and the associated contact list and give a copy to everyone you expect to play a role in an incident. During an incident, your internal email, chat, and document storage services may be down or inaccessible.
- **Develop an incident staffing and stakeholder plan.** What roles will everyone play? Which people and groups will need to be notified that won't be top of mind during the incident? Examples include the board of directors, key investors, and critical partners.
- **Review this plan quarterly**. The best IRPs are living documents that evolve with business changes.
- **Prepare press responses in advance.** If a reporter calls you, claiming to have data stolen from your file servers, what will you say? Having a good "holding statement" will help.

- **Select an outside technical resource/firm** that will investigate potential compromises.
- **Conduct an attack simulation exercise,** sometimes called a tabletop exercise, the exercise might start with the head of communications receiving an email from a reporter about rumors of a hack. The facilitator will provide other updates during the game to see how everyone plays their role. Every sports team rehearses, and you should too!

DURING A CYBERSECURITY INCIDENT

- **Assign an Incident Manager (IM**). This person leads the response. They manage communication flows, update stakeholders, and delegate tasks. However, the IM does not perform any technical duties. During a time of crisis, time dilation affects people's perception of time passing. The IM will monitor the clock to avoid that common problem.
- **Assign Tech Manager (TM).** The TM will serve as the subject matter expert. They will bring in other internal and possibly external technical experts (with the consent of the IM and possibly your attorney!)
- **Assign Communications Manager (CM).** The CM will interact with reporters, post updates on social media, and may interact with external stakeholders (like shareholders).

AFTER A CYBERSECURITY INCIDENT

- **Conduct postmortem.** The IM will report out the known incident timeline and ask for additions and edits. They will then ask for analysis from the incident response team and suggest areas for improvement.
- **Update policies and procedures** based on the postmortem meeting.
- **Communicate** the findings to your staff. Transparency builds trust and many staff will appreciate hearing how seriously the executives consider security. That's how you build a culture of security.

Read also (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf)

Note: This might Note a fully detailed IRP it was prepared during my internship at internee.pk