armour INSURANCE

Developing a Cyber Incident Response Plan

Plans should consist of 4 key elements:

1. **Prepare**
2. **Observe**
3. **Resolve**
4. **Understand**

Prepare

- Set clear objectives for your incident response strategy and develop a comprehensive plan to strengthen your organization's security, visibility, and recovery capabilities.
- Establish a robust backup system to support data restoration during downtime or disruptions.
- Regularly update and patch your software and hardware to minimize vulnerabilities.
- Test your incident response plan, analyze the results, and refine your plan accordingly.

Observe

- Continuously monitor your networks, systems, and connected devices to proactively identify any potential threats.
- Make it a regular practice to generate comprehensive reports and carefully document all events and potential incidents that occur. With a thorough analysis of these occurrences, determine when it is necessary to activate your incident response plan.
- Consider determining the most suitable frequency and intensity for your monitoring efforts, whether it involves maintaining a constant 24/7 view, or adopting a more flexible as-needed approach.

Resolve

To effectively address and mitigate the threat, it is crucial to have a thorough understanding of the situation.

- Take immediate action by disconnecting systems and devices to prevent further harm.
- Implement measures to isolate systems, suspend employee access, and detect/prevent any additional intrusions.
- Restore systems from backup to completely eliminate the intrusion.
- Ensure all devices are protected by running anti-malware/anti-virus software and promptly patching/updating if vulnerabilities are identified.
- Preserve evidence/documentation to assist in analysis and establish preventive measures for future incidents.

*This is also the stage where you would be in contact with a cyber insurance company. They can provide guidance and may have their response team handle things from there.

Understand

- Determine the root cause of the incident, collaborate closely with the response team, and carefully assess the effectiveness of response processes.
- Develop a comprehensive document that captures valuable lessons learned and outlines necessary adjustments for future incidents.
- Thoroughly document the steps taken to uncover and resolve the incident, creating a valuable resource for expediting recovery and improving overall effectiveness.