Checklist

What to include in your cybersecurity incident response plan

Before an incident

- □ Make a list of key data and systems
- □ Backup data
- □ Implement antivirus, firewall, and other security tools
- □ Create standardized security protocols
- □ Teach employees about cybersecurity best practices
- □ Build a response team
- □ Develop internal and external communication plans
- □ Test the plan to make sure it’s ready to be implemented
- □ Monitor for threats like unusual network activity, altered files, and suspicious logins

During an incident

- □ Notify the response team
- □ Isolate affected systems
- □ Remove the malware and backdoors
- □ Patch vulnerabilities
- □ Restore systems to clean versions

Stop threat and recover

- □ Analyze logs to understand how the breach occurred
- □ Determine the scope of the compromise
- □ Notify customers and stakeholders within legal guidelines