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 standardised security protocols
- [ ] Teach employees about cybersecurity best practices
- [ ] Build a response plan and assign roles
- [ ] Develop internal and external communication plans
- [ ] Test and rehearse plans (tabletop exercises, simulations)
- [ ] Monitor for threats like unusual network activity, altered files, and suspicious logins

During an incident

- [ ] Initiate the response plan
- [ ] Isolate affected systems
- [ ] Remove any malware and backdoors
- [ ] Patch vulnerabilities
- [ ] Restore systems to clean versions
- [ ] Preserve evidence (logs, files, disk images)

After an incident

- [ ] Analyse logs to understand how the breach occurred
- [ ] Determine the scope of the compromise
- [ ] Notify customers, stakeholders, and regulators within legal guidelines
- [ ] Engage third-party vendors and the police
- [ ] Conduct a post-incident review
- [ ] Update plans and security controls, policies, and training based on lessons learned