1. Backup data regularly: It is essential to back up data files regularly and store it in a secure location, ideally an offsite cloud backup service that stores and transmits backup data encrypted.

2. Develop a disaster recovery plan (DRP): Create a clear document outlining the steps to be taken in case of cyber security incidents. Ensure all technical staff or contractors know the plan and its procedures.

3. Test your DRP regularly: Conduct regular tests of your DRP to ensure it is effective in a real-life crisis. Make updates based on the results of these tests.

4. Identify critical business functions: Identify the most critical ones and ensure they receive priority in recovery efforts.

5. Identify dependencies and ensure redundancy: Identify critical dependencies essential for normal operations, such as power and internet connectivity. Ensure that redundancy is in place to provide a backup in case of an outage.

6. Allocate recovery resources: Allocate resources required to recover from cyber incidents, such as manpower, hardware, and software.

7. Create an incident response team: Establish a team of individuals trained to respond quickly and effectively to cyber incidents.

8. Review insurance coverage: Review insurance coverage with experts and ensure it covers all potential cyber-related incidents.

9. Educate employees: Educate employees on cyber security best practices to reduce the risk of security breaches.

10. Restrict access to systems and data: Limiting employee access to systems and data minimizes a malicious insider threat. Ensure that privileged access and password controls are enforced and use two-factor authentication wherever feasible.

11. Secure the network: Implement security measures, such as firewalls and anti-virus software, to prevent cyber-attacks.

12. Keep software and system up to date: Regularly updating software and systems can prevent security breaches associated with outdated versions. Ensure that any security patches or updates are promptly installed.

13. Keep documentation current: Ensure all policies and procedures are documented accurately and trained personnel are familiar with the latest information.

14. Conduct regular training: Train all employees on the DRP, roles and responsibilities, and best practices, including the importance of cyber security hygiene.

15. Establish communication channels: Establish clear communication channels to inform all stakeholders during cyber security incidents.

By following a comprehensive disaster recovery checklist such as this, businesses can proactively prepare for a cyber security incident and minimize disruption to their operations and financial loss.