



Regardless of the business size, it is critical to take measures to prevent cyber attacks and/or emergencies by having a set plan ready to go if one does occur. Every minute of downtime can cost an organization thousands of dollars, don't be a victim of a cyber attack. When implementing a recovery plan to protect and secure your data use this checklist to make sure your bases are covered:



IDENTIFY

- Have you established a computer, software and hardware asset inventory list?
- Have you established ownership of all data?
- Are security policies written, enforced and updated?
- Have you classified data by its usage and sensitivity?
- Do you have an emergency response plan?



PROTECT

- Is your security software current?
- Do you have automatic software updates turned on?
- Do you enforce strong pass phrases and strong authentication to access accounts?
- Do you restrict access to information through user, function, project, and document security settings?
- Do you back up your data on a regular basis?
- Do you use encrypted data backups?
- Do you have strict rules for what employees can install and keep on their work computers?
- Do you have a firewall?
- Do you have a policy to delete, without opening, emails from unknown sources?
- Have all employees received security training to protect client data and have been educated on current threats?



DETECT

- Do you receive automatic application alerts that include: intrusion, prevention, and spam management?
- Does your organization blacklist known threats?
- Does your organization whitelist valid sites?



RESPOND

- Does IT personnel regularly review backup logs to verify backups are complete?
- Are random restores done to verify data is accessible?
- Does your organization provide ongoing security training and education on current threats?
- Does your IT review the IT/HR policies annually to keep up with constantly evolving technology?
- Have you systematically evaluated all potential sources of disruption to your business?



RECOVER

- Do you maintain a list of employees, customers, and suppliers at an off-site location?
- If you lost a critical system, do you have a predetermined plan to restore the system?
- Is your business resumption plan securely stored in a remote location?
- Do you randomly test your business resumption plan along with your site emergency plan?
- Do you and your employees know what to do in the case of an emergency?

This document is for informational purposes only. Stars Information Solutions & Digitech Systems, LLC. is not liable for errors, omissions or inadequacies. Please consult an appropriate compliance expert to understand your needs. This information is subject to change.

Sources: <https://databreachinsurancequote.com/wp-content/uploads/2012/09/Cyber-Security-checklist.pdf>; <https://staysafeonline.org>

Plan today to keep your organization cyber secure.

Contact us if you need help with your plan! • www.StarsTek.com