Disaster Recovery Planning for Small and Medium Businesses (SMBs) – Key Considerations

Division/department	*Which parts of the organization are distinct and have different information system requirements?*
Service	*What organizational services are supported by the information systems?*
Corporate or community impact	*What is the impact of the loss of the service(s) to the organization or to the community?*
Risk analysis	*What are the risks associated with downtime and recovery? What are the associated mitigations?*
Actions	*Who has specific responsibilities within each phase of the DRP and how are they contacted?*
Contacts	*Who else may need to be notified during recovery operations?*
Technical assets	*What technical assets (hardware, OS, or software) are required to support recovery? Are they up-to-date, patched and available?*
Dependencies	*What dependencies are there for information systems and other resources to support initial and full recovery?*
Build instructions	*What does the recovery team need to know to support partial or full recovery build/rebuild of your information systems?*
Other mitigations	*What other mitigations may be required to support each phase of the disaster recovery, and return to safe and secure normal operations?*

RECOVERY ACTIONS – ARE YOU READY?

If you suffer a disruption, recovery should be done in a phased approach where remediation steps are prioritized. ***(National Institute of Standards and Technology Special Publication 800-61 Rev. 2 Computer Security Incident Handling)***

While there is often a business urgency to recover from a breach, taking steps to a safe and secure recovery is crucial to ensuring that the organization can return to normal operations. Recovery may include restoring systems from clean backups or rebuilding systems from scratch.

Depending on your infrastructure, early phases should focus on ensuring security when initial, often essential, systems are brought back online. Later phases should focus on bringing other systems and features online, longer-term changes, systems improvements and assessments with the aim of improving performance and security. This should also include any changes to breach procedures and personnel training. Recovery activities can include:

- Restoring systems to normal operation
- Confirming that the systems are functioning normally
- Remediating vulnerabilities to prevent similar incidents
- Restoring systems from clean backups
- Rebuilding systems from scratch
- Replacing compromised files with clean versions
- Installing patches
- Reviewing access controls
- Changing passwords/passphrases and updating the password manager
- Tightening network perimeter security
- Increasing system logging and/or monitoring
- Introducing additional security controls
- Conducting vulnerability testing, penetration testing and other activities to ‘prove’ that the system has been hardened against similar attacks
- Conducting a security assessment
- Reviewing and revising procedures
- Training or retraining staff