Cybersecurity & Disaster Recovery Planning

Work through these questions with your IT team to ensure you're ready to face anything that threatens your ability to keep your business running.

Business Continuity & Disaster Recovery

Is the Business Continuity/Disaster Recovery plan documented and regularly tested?

Does this plan account for disruptions related to natural disasters (earthquake, hurricane, snowstorm), power outages (both temporary and prolonged), cybersecurity threats, and software/equipment failure?

What is the Recovery Time Objective (RTO)?

RTO is the time goal to restore service after a disruption.

What is the Recovery Point Objective (RPO)?

RPO is the acceptable time threshold of data loss.

Backups

What servers, desktops, and core business data are backed up?

How often are they backed up? Are those backups tested on a regular schedule?

What levels of redundancy are in place?

If a server or other portion of your infrastructure fails, will it be automatically moved to different hardware without disruption?

Are there spare, pre-configured computers available to put into critical infrastructure?

Does this include critical office and shop computers? What is the expected timeframe to replace a machine? If a pre-configured PC isn't available, what is the SLA from the 3rd party hardware supplier?

Digital Safety

What layers are in place to prevent a cybersecurity incident?

Is anti-virus software in place and up to date? Are firewall policies audited regularly to ensure only required ports are open? Is there a monitoring/on-call policy to react to alerts quickly? Are there blocks in place to prevent connections to countries that are not required for business?

Which users have local rights to install software (or viruses)?

Why? What software or process requires this? Do any IT (or other) users operate with domain admin rights on their day-to-day accounts?

Is web traffic monitored and filtered?

Are spam and threat protection enabled on the mail server?

Are all end users regularly trained and tested on cybersecurity?

Can they identify aspects of ransomware, phishing, forged emails or websites?

Is the Wi-Fi secured and monitored with “guest access” policies (if necessary)?

Next Steps

Schedule meeting for follow-up on: ____