

# Ransomware Prevention Checklist for CXOs



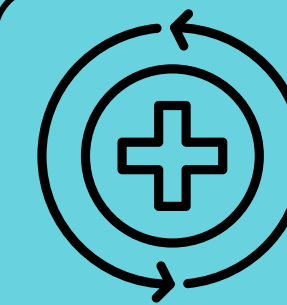
## Fireproofing

- ✓ **Multifactor authentication (MFA)** on all remote-access and privileged accounts
- ✓ **Email filtering + phishing detection tools** to reduce malicious entry points
- ✓ **Zero trust access** to ensure users only access what they need
- ✓ **Patch management** to fix known vulnerabilities before attackers exploit them
- ✓ **Security awareness training**—your staff is the first line of defense
- ✓ **Network segmentation**, which keeps ransomware from spreading inside your network
- ✓ **Endpoint-detection-and-response (EDR) agents** on all devices, including ones that access your network remotely



## Extinguishers & Alarms

- ✓ **SIEM (security information and event management)** for centralized monitoring, investigation, and response
- ✓ **24/7 security operations center (SOC)** or managed detection and response (MDR)
- ✓ **Behavior-based alerts** to catch anomalies like encryption behavior (where data shows signs of being actively compromised)
- ✓ **Real-time threat intelligence feeds** that watch for indicators of compromise (IOCs), or known signs of a cyberattack



## Evacuation & Recovery

- ✓ **Incident response plan (IRP)** that defines roles, decisions, and communication protocols
- ✓ **Offline backups** that can't be encrypted or deleted by attackers
- ✓ **Crisis communication strategy** (internal, external, legal, regulatory)
- ✓ **Pre-vetted external partners** for cyberinsurance, forensics, and legal counsel

wyretechnology.com

WYRE

WE WILL CROP THIS BLACK PART OFF AFTER THE DESIGN IS DONE. DON'T WORRY ABOUT FILLING IT WITH ANYTHING :))