

3 Strategies for Long-Term Ransomware Defense



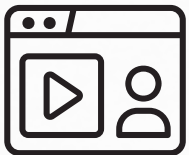
1 Periodic Security Audits

Regularly Schedule and Conduct Comprehensive Security Audits. This will help identify vulnerabilities in your infrastructure, allowing you to stay ahead of potential threats and ensure that protective measures remain effective as technologies evolve and new threats emerge.



2 Continuous Team Training

The Landscape of Cyber Threats is Constantly Shifting. To prevent the majority of ransomware attacks, routinely train and retrain your team. Make sure they are aware of the latest tactics employed by cybercriminals, and know how to recognize and avoid them. By fostering a culture of vigilance and cyber-awareness, you can reduce the risk of human error leading to a breach.



3 Simulated Ransomware Drills

Much Like Fire Drills, Regular Simulated Ransomware Attack Drills can be Invaluable. But your cyber insurance carrier may have a preferred vendor. Communicate with your cyber insurance company and have them validate your response company. The time needed to have legal and insurance approval to proceed may be crucial.