The Readiness Checklist

PREPARING FOR THE GAME

risk crew

Shelter from the Storm

Whether you are an SMB or enterprise-level organisation, and no matter what industry, it's vital that you are prepared for ransomware attacks. This readiness checklist includes basic practices for protecting against ransomware attacks. We do recommend consulting an expert if one is available to you.

☐	Staff have received information security awareness training explaining how to identify and respond to a phishing attack within the last 3 months.
☐	Staff have been instructed on how and where to report security incidents.
☐	Staff have been subjected to simulated phishing attacks within the last 3 months.
☐	Incident Response Team members have received ransomware response training.
☐	Set up a crypto wallet.
☐	Backups are routinely conducted, encrypted and maintained offline.
☐	Backup and backup procedures have been tested for accuracy.
☐	Incident Response Plans and procedures are in place and have been tested within the last 6 months.
☐	Business Continuity Plans and procedures are in place and have been tested within the last 6 months.
☐	Disaster Recovery Plans and procedures are in place and have been tested within the last 6 months.
☐	Internet-facing vulnerabilities & misconfigurations identified in routine vulnerability scanning & security penetration testing have been identified and mitigated within 5 days of discovery.
☐	Cyber insurance policy is reviewed for applicability, aligned to critical business assets & recovery objectives.
☐	Strong spam filters are deployed on mail services and end clients.
☐	Multi-factor Authentication (MFA) is deployed for access to all services (to the highest extent possible), particularly for webmail, Virtual Private Networks (VPNs) and accounts that access critical systems.
☐	Standard security builds are established and maintained for all devices connected to the network.
☐	Remote Desktop Protocol (RDP) and all other remote desktop services have been removed and are only allowed by approved sessions.
☐	Change Management procedures are established and implemented.
☐	Software, operating systems, applications and firmware are updated immediately following their release, prioritising the patching of critical security vulnerabilities on internet-facing servers and software processing internet data, such as web browsers, browser plugins and document readers.
☐	All network connected devices are properly configured & all applicable security features are enabled.
☐	Ports and protocols that are not being used for business purposes are disabled.
☐	Inbound and outbound Server Message Block (SMB) protocols have been removed, disabled or block if not required for a critical business function.
☐	Antivirus, anti-malware software & signatures are implemented on all critical systems & kept up to date.