CyberCatch

RANSOMWARE RISK ASSESSMENT WORKSHEET

Answer each of the 10 questions and calculate your Ransomware Risk Score (i.e. risk of suffering a damaging ransomware attack.)

		YES	NO
1.	Do you have a control to identify vulnerabilities in Internet-facing IT assets on an ongoing basis?	□ +10	□ +0
2.	Do you have a policy that requires patching of high-risk vulnerabilities within 24 hours or a workaround?	□ +10	□ +0
3.	Do you have a secure desktop build and separate server permissions policy?	□ +10	□ +0
4.	Do you segregate and control privileged users passwords?	□ +10	□ +0
5.	Do you require multi-factor authentication for all privileged users and for all employees with access to sensitive data?	□ +10	□ +0
6.	Do you regularly test your employees with simulated phishing attacks and provide remedial training to raise awareness?	□ +10	□ +0
7.	Do you provide quarterly training to all your employees to recognize latest phishing red flags and a suspicious activity reporting mechanism?	□ +10	□ +0
8.	Do you have a written incident response plan and is it tested periodically?	□ +10	□ +0
9.	Does your incident response plan specifically cover ransomware to detect and respond to and is it periodically tested for a ransomware scenario?	□ +10	□ +0
10.	Is all your sensitive data backed up daily and stored offline and encrypted?	□ +10	□ +0

Note: This Worksheet will not calculate, you will need to count the total points under YES for your Score. Each YES Answer is 10 points and each NO answer is zero points.

RANSOMWARE RISK SCORE RESULTS

HIGH	MODERATE	LOW
0 – 79	80 – 90	Over 90

www.cybercatch.com