

Risk Identifier	CR-09
Risk Title	Cyber Security


Risk Description
 The council must have resilient and robust cyber security is in place. If it does not then the organisation is at risk of being more exposed to network vulnerabilities such as cyber-attacks and system failures leading to reputational damage, liability issues and loss of service provision.

Risk Owner
 Nicola Wittman

Directorate Responsible
 Commercial & Digital Change Management

Original Risk		
Likelihood	Impact	Score
3	4	12

Residual Risk		
Likelihood	Impact	Score
2	4	8

Risk direction
 Stable 

Cabinet Member
 Councillor Lees

Key Dates	
Date Registered	5th June 2024
Last update	5th June 2024

Background
 There is a risk that cyber criminals will successfully conduct a ransomware attack, denying our users access to our corporate IT systems and the information they store and process, impacting our ability to deliver our core services.

Service Area Affected
 All

Triggers
 National events, such as a general Election, increase risk of cyber attacks.

Risk Type
 Threat

Risk Response Category
 Reduce

Risk Response	Risk Response Actionee	RAG Status	Progress Update	Next Scheduled Update
Systems and information backups	Alan Mose	Green	In place	
system hardening and lockdown ie Vulnerabiltu patching	Alan Mose	Amber	Further staffing resources are required	
NCSC Services and Warps membership and active participation	Alan Mose	Green	In place	
Continued investment in new technologies and dedicated officer resource	Nicola Wittman	Amber	Access to more funding required and dedicated officer resource	
Phishing Campaigns and training	Alan Mose	Red	Phishing funding has been removed by ECC	
Incident Mangement	Nicola Wittman Alan Mose	Green	In place	

Key for RAG status of risk response	
R	Control is not in place or working or progress has slipped

A	Control is not working efficiently and some challenges remain
G	Control is working or predominantly in hand or completed