CYBER SECURITY ASSESSMENT

Security Maturity Assessment Report

A clear, evidence-based view of where your organisation sits across the four pillars of the HOLKER Cyber Security Framework - and the prioritised roadmap to move you forward.

PREPARED FOR

Colne Town Council

REPORT DATE

July 2026

PREPARED BY

Carl Smith-Wilkinson - Head of Managed Services

About this assessment

This report explains, in plain terms, what your current cyber security position means for the business - not just for IT. It sets out where the biggest risks sit today, what could happen if they are left unaddressed, and a practical, phased plan to close the gap over the next 18 months, grounded in evidence gathered from your own environment.

Attackers only need to find one weak point, not defeat every defence, which is why this report looks at four distinct areas of the business and addresses them in the order that reduces risk fastest while remaining manageable to plan and resource.

What this means for your business

Overall risk position	1.50 out of 5 on average across the four areas assessed. The fundamentals are in place in most areas, but the business is not yet protected against a determined or opportunistic attacker.
Biggest current exposure	Network & Access Controls, currently at the essential baseline (Level 1) - the fundamentals are only partially in place. This is the largest single gap identified in this assessment.
Recommended first priority	Network & Access Controls. This is addressed first in the agreed roadmap because it currently carries the greatest exposure of the four pillars assessed.
Expected business benefit	A materially lower chance of a costly, disruptive incident - reduced risk of service downtime for residents, protected constituent and staff data, and a stronger position for meeting public sector compliance and audit requirements.
Immediate actions (next 30-90 days)	Close the remaining Identity gaps with enforced MFA and security awareness training, begin the Intune rollout on Endpoints, start VPN MFA enforcement on Network, and strengthen anti-phishing and DMARC policy on Email.

The four pillars

The HOLKER Cyber Security Framework groups controls into four pillars that, together, cover the areas most commonly exploited in a cyber attack.

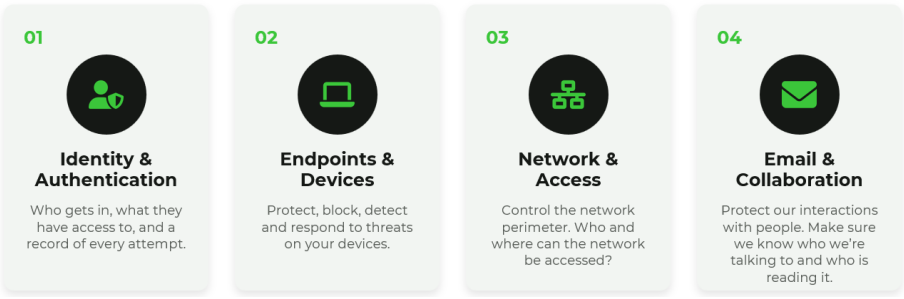

Figure 1 - The four pillars of the HOLKER Cyber Security Framework.

The five levels

Each pillar is graded from Level 1, an essential baseline, through to Level 5, a defence tailored to your organisation's specific risks. The levels are cumulative - each builds on the controls established at the level before it, so progress is never lost as you move up.

Figure 2 - The five maturity levels, applied consistently across all four pillars. Level 5 adds additional controls targeting threats unique to your business.

EXECUTIVE OVERVIEW

Summary scorecard

The table below summarises Colne Town Council's current security posture in each pillar, ranked in the order we recommend addressing them. Full detail, evidence and recommended next steps follow on the pages after.

1.50 / 5	4	2	Network
AVERAGE MATURITY	PILLARS ASSESSED	AT ESSENTIAL BASELINE	TOP PRIORITY

#	Pillar	Current level	Target	Why this matters
1	**Network & Access Controls**	**Level 1** - Essential baseline ■□□◆□	**Level 4** - Monitored & responsive	*Biggest exposure - the priority to address first.*
2	**User, Identity & Authentication**	**Level 1** - Essential baseline ■□□◆□	**Level 4** - Monitored & responsive	*Foundations set; strengthen to close key gaps.*
3	**Email & Collaboration**	**Level 2** - Managed & controlled ■■◆□□	**Level 3** - Detect & prevent	*Foundations set; strengthen to close key gaps.*
4	**Endpoints & Device Management**	**Level 2** - Managed & controlled ■■□◆□	**Level 4** - Monitored & responsive	*Well advanced - a smaller, targeted change.*

Note: levels shown reflect the position assessed as at July 2026 and should be re-confirmed at the next review. Diamond markers (◆) show the recommended target level for each pillar.

Risk summary

A quick-reference view of what is at stake in each pillar if these gaps are left unaddressed. Full detail on each risk is set out on the corresponding pillar page later in this report.

Pillar	Risk if nothing changes
Network & Access Controls	An unprotected VPN and unrestricted outbound traffic are among the most common ways ransomware groups gain a foothold.
User, Identity & Authentication	A leaked password or phishing email could still succeed while MFA isn't policy-enforced across every account.
Email & Collaboration	Without enforced DMARC, attackers can spoof your own domain to target staff, residents or suppliers directly.
Endpoints & Device Management	Without active monitoring, a genuine compromise that slips through your existing controls could go unnoticed.

Your prioritised roadmap

We recommend addressing the pillars in the agreed order below, phasing the work across the estate in a way that is manageable to plan, resource and roll out.

#	Pillar	Move	Why this priority
1	**Network & Access Controls**	L1 → L4	*Biggest exposure - the priority to address first.*
2	**User, Identity & Authentication**	L1 → L4	*Foundations set; strengthen to close key gaps.*
3	**Email & Collaboration**	L2 → L3	*Foundations set; strengthen to close key gaps.*
4	**Endpoints & Device Management**	L2 → L4	*Well advanced - a smaller, targeted change.*

Proposed 18-month roadmap

The table below phases the work across all four pillars over an 18-month programme. Identity, Endpoints and Network reach Level 4 (Monitored & responsive); Email reaches Level 3 (Detect & prevent), its agreed target. Network & Access Controls is addressed first given its current exposure, with Identity close behind.

Phase	Focus	Levels at end of phase
Phase 1 **Months 0-3**	Deploy Huntress Security Awareness Training (SAT) and Identity Threat Detection and Response (IDTR) across all licensed Microsoft 365 accounts to strengthen account security and deliver cyber security awareness training to all users. In addition, enable Huntress EDR on all devices, including the unsupported server, to extend endpoint protection across the full estate.	Identity **L2** · Endpoints **L2** · Email **L2** · Network **L1**
Phase 2 **Months 3-6**	Primary server replaced with Microsoft Intune with SSL inspection enabled and DKIM and DMARC turned on	Identity **L4** · Endpoints **L4** · Email **L3** Network **L3**
Phase 3 **Months 6-12**	External and Internal monthly penetration testing enabled with monthly security reviews.	Identity **L3** · Endpoints **L3** · Email **L3** · Network **L4**
Phase 4 **Months 12-18**	Email filtering upgraded to Mimecast with regular reviews on all aspects of security.	Identity **L4** · Endpoints **L4** · Email **L3** · Network **L4**

Timeframes are indicative and will be confirmed and costed during the review session referenced below.

PILLAR 01

User, Identity & Authentication

Proving who your users are, controlling what they can reach, and recording every attempt so attacks can be spotted and stopped.

L1	CURRENT LEVEL **Essential baseline (partially met)**

WHERE YOU ARE TODAY

You have partially met Level 1, which means some of the fundamentals are in place, but not yet applied consistently across every account.

- Joiner, mover and leaver processes are established and governed through approved access workflows
- MFA is partially deployed but not yet enforced through policy-based controls across all users and services
- Privileged account protections are in place but not fully restricted using Conditional Access and location/device controls

L4	RECOMMENDED NEXT STEP **Monitored & responsive**

Establish strong identity controls that reduce the risk of compromised accounts and give you greater visibility and control over who can access business systems and data.

HOW WE GET YOU THERE

- Level 2 - Conditional Access & Governed Access - Entra ID P1 (via Business Premium) enforcing MFA on every login, with dedicated Conditional Access policies restricting privileged accounts to known devices and locations, session lifetime limits, and HOLKER Managed IT Support running fully governed joiner/mover/leaver approval workflows
- Level 3 - Security Awareness Training & Passwordless MFA - Dark-web credential monitoring and Conditional Access enforcing passwordless / phishing-resistant MFA strength
- Level 4 - Identity Threat Detection & Response - Huntress ITDR providing 24/7 SOC-based detection of unusual sign-in activity, standalone dark-web monitoring, and Huntress Managed SAT for ongoing staff training

WHY THIS MATTERS

Identity is the front door to every other system you rely on. Reaching Level 4 closes the gap between having identity controls in place today and having them consistently enforced, actively monitored and backed by 24/7 detection - removing the reliance on individual staff members to do the right thing.

RISK IF NOTHING CHANGES

Without policy-based MFA enforcement, a phishing email or a leaked password can still succeed against anyone using a weaker sign-in method. Joiner, mover and leaver processes reduce some risk, but privileged accounts that aren't fully restricted to approved devices and locations remain an easy target if a credential is compromised, giving an attacker a route to your most sensitive systems. Any active compromises will not alert and will rely on the incident being reported.

PILLAR 02

Endpoints & Device Management

Protecting every device - block, detect, then respond - and managing your whole estate from one place to shrink the attack surface.

L2	CURRENT LEVEL Managed & controlled

WHERE YOU ARE TODAY

You have reached Level 2 (Managed), which means:

- All endpoints are protected by antivirus, and automated operating system updates (excluding the server)
- Users operate without local administrator rights by default
- ThreatLocker is providing application allowlisting, ringfencing, privilege management and default-deny execution controls

L4	RECOMMENDED NEXT STEP Monitored & responsive

Increase visibility and control across the device estate while building the ability to detect and respond to endpoint threats.

HOW WE GET YOU THERE

- Level 2 - Centralised Device Management - Microsoft Intune enrolment for centralised configuration, compliance and visibility across the estate (Level 3 application control is already in place via ThreatLocker). Decommissioning the legacy server as its running on an unsupported and insecure version of Windows.
- Level 4 - 24/7 Monitoring & Response - Huntress-managed EDR (Defender, depending on licensing) providing round-the-clock monitoring, investigation and response to suspicious activity

WHY THIS MATTERS

Application allowlisting and privilege restriction already give you strong protection against malware execution. Reaching Level 4 adds the missing pieces - centralised management and active, round-the-clock monitoring - so that if something does get through, it's caught and investigated rather than sitting undetected on a device.

RISK IF NOTHING CHANGES

ThreatLocker already stops most malicious software from running, but without centralised management through Intune, device configuration and compliance can drift out of sight. And without EDR, a genuine compromise that does slip through has no active monitoring to catch it - it could sit on a device unnoticed until it causes real damage.

PILLAR 03

Network & Access Controls

Controlling who and what can reach your networks - across the internet perimeter, wireless and physical access - guarding against outsiders and insider threats alike.

L1	CURRENT LEVEL **Essential baseline**

WHERE YOU ARE TODAY

You have reached Level 1 (Essential baseline), which means:

- Wireless network encrypted with WPA2
- You have a business-grade firewall
- Router / firewall admin interface is not reachable from the internet

L4	RECOMMENDED NEXT STEP **Monitored & responsive**

Strengthen network security by improving visibility, inspection and control of network traffic. By moving beyond basic perimeter protection, threats can be detected earlier, suspicious activity can be investigated more effectively, and the risk of compromise spreading across the network is significantly reduced.

HOW WE GET YOU THERE

- Level 2 - Hardened Firewall & VPN Authentication - FortiGate firewall with an active UTM subscription and IPS enabled on inbound policies, with multi-factor authentication enforced on all remote-access VPN connections
- Level 3 - Full Traffic Inspection & Logging - SSL inspection and IPS extended to all web traffic including encrypted connections, a default-deny outbound policy restricting traffic to approved destinations only, and all significant firewall traffic logged for investigation
- Level 4 - Active Verification & Monitoring - Vonahi internal & external penetration testing to verify controls are effective, a Huntress SIEM solution ingesting and analysing firewall logs.

WHY THIS IS THE PRIORITY

A business-grade firewall and encrypted Wi-Fi are a solid starting point, but they only protect the perimeter. Reaching Level 4 adds full visibility and control over what's happening inside that perimeter and on the connections coming through it, verified through testing and continuous monitoring - closing the two routes' attackers rely on most: an unprotected VPN and unrestricted outbound traffic.

RISK IF NOTHING CHANGES

Without MFA on remote-access VPN connections, a single compromised password is enough to grant an attacker a route straight onto the network. And without a default-deny outbound policy, malware that does land on a device is free to communicate with attacker infrastructure and exfiltrate data without restriction - this is one of the most common ways ransomware groups gain and keep a foothold.

PILLAR 04

Email & Collaboration

Defending the channel attackers use most - filtering email, protecting every click, validating senders, and keeping collaboration and file sharing safe.

L2	CURRENT LEVEL Managed & controlled

WHERE YOU ARE TODAY

You have reached Level 2 (Managed), which means:

- HOLKER Mesh Email Security provides third-party filtering and advanced threat protection
- Malicious email detection capabilities extend beyond Microsoft's native controls
- SharePoint and OneDrive sharing controls are not yet aligned to Level 2 requirements

L3	RECOMMENDED NEXT STEP Detect & prevent

Your Microsoft 365 email security provides strong protection against common threats. To reach the next level of maturity, focus on strengthening anti-phishing controls, enforcing DMARC, and improving protection against more advanced email-based attacks.

HOW WE GET YOU THERE

- Level 2 (outstanding) - Sharing & Domain Authentication - review and restrict SharePoint/OneDrive external sharing via the Microsoft 365 admin centre, and publish and enforce SPF, DKIM and DMARC with a minimum policy of quarantine
- Level 2 (outstanding) - Anti-Phishing Policy - strengthen Microsoft Defender for Office 365 Safe Links and anti-phishing protections, including user and domain impersonation controls, applied universally via Business Premium
- Level 3 - Second-Layer Filtering - extend HOLKER Mesh Email Security with QR-code link decoding and retrospective remediation, removing malicious emails that weren't identified at the point of delivery

WHY THIS MATTERS

Your Microsoft 365 protections and Mesh Email Security filtering already provide strong baseline coverage. Level 3 strengthens anti-phishing and impersonation controls and enforces DMARC, closing the more sophisticated attacks that rely on impersonating trusted senders or your own domain.

RISK IF NOTHING CHANGES

Without enforced DMARC, attackers can spoof your own domain to target your staff, residents or suppliers, and impersonation attempts that don't rely on malicious links or attachments can still slip past filtering aimed at known threats. Combined with SharePoint and OneDrive sharing settings that aren't yet locked down, there's a real risk of both inbound impersonation attacks and outbound oversharing of sensitive data.