SALISBURY CITY COUNCIL

Subject : SCC Cyber Security and IT Systems Update
Committee : Full Council
Date : 10 November 2025
Author : Jeremy Cotton, IT Support Officer

1. Report Summary:

1.1 To provide Members with an update on the cyber security measures and related work undertaken by the Council during the current financial year.

1.2 To inform Members of additional IT systems improvements completed during the year and outline planned works to further enhance system performance, data protection, and business continuity.

1.3 The following table breaks down savings made by Salisbury City Council as a result of the actions in this report

System / Change	Savings
New desk phone and broadband contract	£45,196 over the lifetime of the previous contract
New mobile phone contract	£14,832 over the lifetime of the previous previous contract
New internet connection estimation	Estimated: >£15,000 p/a Possible as a result of EDMS move.
Total Estimated Saving	£75,028

2. **Background:**

2.1 A cyber security audit was conducted in 2023, identifying several areas of weakness and risk across the Council's systems. A penetration test was carried out by the Council's managed service provider (MSP), together with a full audit of existing infrastructure.

2.2 An extensive audit report identified a range of system-level vulnerabilities, including outdated firmware, unsupported and vulnerable network hardware, the continued use of factory default administrator logins, and legacy system configurations containing known exploits. At the user level, issues were found such as the absence of two-factor authentication (2FA) across the Microsoft 365 tenant, insecure password storage (e.g., written notes), unlocked screens, and unpatched devices. The report concluded that a coordinated programme of improvements was required across hardware, software, network infrastructure, and physical security, particularly in relation to access controls and server cabinet management.

2.3 However, it is worth noting that while a number of significant issues were identified, the audit also highlighted several existing strengths within the Council's systems. These were reinforced at the Government Digital Expo held in London in September, where many of the national cyber security strategies discussed had already been adopted by Salisbury City Council or have since been implemented as a direct outcome of the penetration test.

2.4 As part of the 2025/26 budget process, the Council approved an allocation of £50,000 to implement the improvements necessary to ensure that Salisbury City Council's IT systems are compliant, resilient, and secure.

The following sections set out how these funds and associated resources have been deployed to strengthen the Council's overall cyber security posture.

3. Cyber Security Project:

User level actions:

3.1 The implementation of two-factor authentication (2FA) was identified as an immediate priority. Deployment was completed in-house within weeks of the IT Officer's appointment, at no cost to the council. All users have now been enrolled, with the exception of a small number who have opted not to install authentication apps on personal devices. For these individuals, FIDO2 security keys have been ordered to ensure consistent coverage across the organisation at a total cost of £300 for 10 devices.

3.2 It was also noted at the Government Digital Expo in London that the Head of Sophos, a leading global provider of endpoint and server security solutions, emphasised the significant risks faced by organisations that have not yet implemented two-factor authentication. Several high-profile cyber incidents were cited where attacks remained undetected for extended periods solely due to the absence of this fundamental layer of protection.

3.3 Since the introduction of 2FA at Salisbury City Council, two attempted unauthorised logins using exposed credentials have been successfully blocked. These incidents originated from international locations and demonstrate that sensitive data is now protected at a fundamental level through this additional layer of security.

3.4 The penetration test was able to make significant inroads into SCC systems not only because of 2FA not being enabled, but because of the vast amount of users who are leaving passwords in books or on post-it-notes, attached to the monitors on their desks or even next to the trackpad on their laptops, rendering a password effectively useless if physical access was gained into the building. We have invested in a password manager for all users across the council as a direct method of tackling this issue.

3.5 The rollout of the password manager is scheduled to take place in the coming weeks, with full implementation expected before Christmas, followed by staff training. The system will securely manage users' passwords across multiple platforms and has the additional capability to generate two-factor authentication (2FA) codes. This allows users to access all authorised systems securely and conveniently from their Council devices.

3.6 Users will only be required to remember a single master password, with the password manager securely storing and managing all other credentials. This measure is designed to eliminate the use of written passwords such as post it notes left near workstations, which could otherwise be exploited by an opportunist gaining physical access to Council offices.

3.7 Implementation and training costs totalled £1,000, with an ongoing subscription of £300 per month covering unlimited users across the organisation. This represents a 50% discounted rate for the first year, after which the subscription will be subject to renegotiation.

3.8 The penetration test also identified weaknesses in physical access controls within Council buildings. Engineers conducting the assessment were able to move through several areas without being challenged, and a number of lockable doors were found propped open. In some cases, server cabinets were left unsecured or held open with cleaning equipment, and keys were missing.

3.9 In response, significant improvements have been made to building security. Sean Saunders, Health and Safety Facilities Supervisor and Luke Harris, Operations Officer have overseen the introduction of a controlled door entry system requiring authorised access for all personnel entering the Guildhall building.

3.10 A new electronic door access system has been installed at the rear entrance of the Guildhall, requiring staff to use an authorised ID card to gain entry. This system was implemented in preparation for the Dawn Sturgess inquiry and has since become part of the Council's standard security infrastructure. For additional protection, it operates on a dedicated VLAN within the Council's network.

3.11 The audit identified that some users remain susceptible to phishing attacks. While new employees receive initial online training on recognising and reporting suspicious emails, this training is not routinely refreshed. Despite the Council operating three layers of email protection Barracuda, Microsoft 365, and Graphus, phishing emails can still occasionally reach users' inboxes, highlighting the need for ongoing awareness and reinforcement.

3.12 To strengthen user awareness, the Council has also subscribed to BullPhish and Dark Web Monitoring services. BullPhish provides a comprehensive suite of cyber security training materials and videos, supplemented by the option to include Council-specific content. The platform enables the scheduling of regular simulated phishing campaigns that test user responses to realistic email threats.

3.13 When a user interacts with a simulated phishing email, the system immediately issues an alert and provides targeted re-training materials to reinforce learning. Detailed reporting identifies users who may be more vulnerable to such attacks, allowing for additional support and intervention where required.

3.14 This new approach ensures that cyber awareness training is no longer limited to a single induction video or quiz completed at the start of employment. Instead, refresher courses and targeted training will be delivered on a regular basis, particularly for users identified as requiring additional support.

3.15 The Dark Web Monitoring service continuously scans the dark web for any exposed credentials linked to the Council's domain. If compromised information is detected, alerts are issued immediately, allowing IT staff to take prompt action such as resetting affected passwords to maintain account and data security.

3.16 Combined, the BullPhish and Dark Web Monitoring services cost £290 per month, equating to approximately £2,928 per year for all users across the SCC tenant. This represents a 50% discounted rate for the first year, after which the subscription will be subject to review and renegotiation.

3.17 Physical security was identified as a weakness across several Council sites. A number of server cabinets were found unlocked, missing keys, or in one extreme instance propped open with cleaning equipment. In addition, several unused network switch ports were found to be live and configured, presenting an unnecessary access risk even without direct cabinet entry.

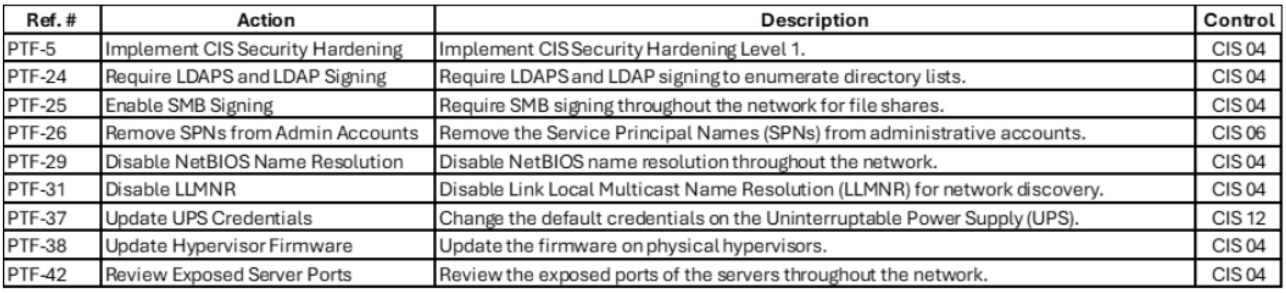
3.18 The process to replace and securely mount these cabinets is now underway, with quotations being obtained from third-party contractors for installation. The replacement cost is approximately £500 for the two cabinets in most urgent need, with further replacements planned as required. All unused network ports have now been disabled, preventing unauthorised connection to the Council's network.

3.19 The audit revealed that Salisbury City Council was still operating outdated Cisco Power over Ethernet (PoE) switches at four sites. These devices were no longer supported by the manufacturer and contained known vulnerabilities that could not be resolved through firmware updates.

3.20 To address this, the Council has replaced the legacy equipment (with one site outstanding) with new UniFi PoE switches that are fully supported and integrate directly into the existing UniFi ecosystem. This upgrade has simplified network management, improved reliability, and reduced system complexity. The total cost of replacement was £1,000.

3.21 The replacement of the network switches has enabled simpler and more efficient VLAN creation and management. This has allowed the Council to isolate critical systems such as the Guildhall door access controls and CCTV onto dedicated VLANs, enhancing security and network performance. Further segmentation is planned for Internet of Things (IoT) devices and printers to ensure continued protection and system integrity.

3.22 The Council has invested an additional £6,700 in strengthening security across both the network and endpoint devices. This investment covers a range of enhancements designed to improve system resilience and align with recognised cyber security standards, including the measures outlined below.



Ref. #	Action	Description	Control
PTF-5	Implement CIS Security Hardening	Implement CIS Security Hardening Level 1.	CIS 04
PTF-24	Require LDAPS and LDAP Signing	Require LDAPS and LDAP signing to enumerate directory lists.	CIS 04
PTF-25	Enable SMB Signing	Require SMB signing throughout the network for file shares.	CIS 04
PTF-26	Remove SPNs from Admin Accounts	Remove the Service Principal Names (SPNs) from administrative accounts.	CIS 06
PTF-29	Disable NetBIOS Name Resolution	Disable NetBIOS name resolution throughout the network.	CIS 04
PTF-31	Disable LLMNR	Disable Link Local Multicast Name Resolution (LLMNR) for network discovery.	CIS 04
PTF-37	Update UPS Credentials	Change the default credentials on the Uninterruptable Power Supply (UPS).	CIS 12
PTF-38	Update Hypervisor Firmware	Update the firmware on physical hypervisors.	CIS 04
PTF-42	Review Exposed Server Ports	Review the exposed ports of the servers throughout the network.	CIS 04

3.23 The Council will be securing all endpoints in accordance with the Centre for Internet Security (CIS) Level 1 Baseline, an internationally recognised benchmark for internet and information security best practice. This standard provides clear guidance for strengthening device configuration and reducing potential vulnerabilities across the network.

3.24 As Windows 10 approaches end-of-support, the Council has completed the majority of upgrades to Windows 11 across its device estate. For machines that were either incompatible with Windows 11 or no longer met performance standards, an investment of £13,000 has been made to procure new hardware, ensuring full compliance and reliability.

3.25 Automatic patching has now been enforced across all SCC laptops to ensure that critical Windows updates are installed promptly and cannot be indefinitely postponed by users. Reporting from the Council's third-party managed service provider indicates strong progress:

75% of devices are now fully patched and up to date.

25% of the remaining devices are scheduled for decommissioning or will be upgraded to Windows 11 in the near term.

3.26 The Council is investing in Sophos Mobile Security software to provide comprehensive protection for mobile devices, including Android phones and iPads used for events. Quotations for the software are currently being finalised; however, the investment is expected to be cost-neutral in the longer term due to planned changes in mobile device management arrangements.

3.27 As part of the Council's wider strategic plan to modernise its IT infrastructure, work has commenced on the first phase of migrating systems from on-premise servers to the cloud. The initial stage involves transferring the Electronic Document Management System (EDMS) and the two domain controllers to Microsoft Azure, creating the foundation for further cloud adoption and enabling significant cost savings in the next financial year.

3.28 The current on-premise servers, located at Bemerton Heath, operate on outdated hardware in a poorly ventilated environment. Although the systems are backed up, the backup server is situated in the same location, creating a single point of failure despite replication to the Guildhall.

3.29 The move to Microsoft Azure will deliver modern, industry-standard security controls, enhanced disaster recovery, and improved remote and site-to-site access. Built-in security features such as multi-factor authentication and encryption for data at rest and in transit will ensure compliance with relevant standards and improve resilience.

3.30 An investment of £22,000 over a calendar year has been made to complete the initial migration and cover associated maintenance and resource costs. While the full migration to cloud-based infrastructure will take place during the next financial year, these first systems form a key part of the current Cyber Security Improvement Plan.

4. Additional IT Systems Work

4.1 In addition to the cyber security improvements outlined above, the Council has a number of wider IT projects currently underway and planned for future implementation. A new corporate phone system is in the final stages of deployment, replacing the legacy Wildix system. The new solution, provided by Apogee, will deliver enhanced functionality and significant cost savings. Handsets have already been distributed, staff training has been completed, and final system configuration is now being carried out by the provider.

4.2 The Council has also transitioned away from 4Com broadband services across its sites, achieving both substantial cost savings and significantly improved connection speeds. The new broadband services have already been installed at The Pantry, The Friary, The Crematorium, and the Guildhall, with installations at the Police Station and M&S unit to follow. When combined with the new telephony system outlined in section 4.1, these changes will generate savings of over £45,000 across a five-year period.

4.3 The Council has brought mobile device management in-house through the use of Microsoft InTune, for which SCC already holds existing licences. This change reduces expenditure on the previous Sophos Mobile Device Management system and allows investment instead in Sophos Mobile Security software. This approach ensures that mobile devices—alongside laptops and servers, receive comprehensive protection against malware and other threats.

In addition, the Council's contract with SGC has now ended, and improved arrangements have been secured directly with the Three network, avoiding third-party costs. The transition to new SIM cards and the associated number porting process is scheduled to take place shortly. These changes make savings of £7416 per year for 2 years.

4.4 The Council has rolled out Printix, a cloud-based printing solution introduced in preparation for the planned decommissioning of on-premise servers next financial year. Printix enables simplified printer management, automated updates, and more secure document handling. Users can now print confidential documents to any networked printer and release them only upon arrival at the device using the free Printix app, ensuring improved confidentiality and flexibility.

4.5 The system also allows for central management of printing preferences, including a default restriction to black-and-white printing unless colour is specifically required.

Given that colour printing costs up to seven times more than black-and-white, this change has already reduced expenditure under the Council's printing contract.

4.6 Since the introduction of Printix, SCC has moved from an overspend of 5,375 units to an underspend of 36,874 units, representing a significant operational saving. The adoption of Printix also eliminates the need for on-premise print servers, which will be fully decommissioned in the next financial year.

4.7 The Council's primary internet connection contract is due to end in April 2026. This connection currently supports multiple sites, including the Guildhall, Bemerton Heath, Tollgate Road, The Crematorium, and Shop Mobility. The existing service costing over £36,000 per annum was originally required to enable the operation of the on-premise EDMS and domain controllers, and to maintain inter-site connectivity.

4.8 With the planned migration of these systems to the cloud, the Council will no longer require this level of complexity or the associated leased firewall equipment. From April/May 2026, SCC will be able to transition to its own firewalls and establish direct fibre connections to each site.

4.9 This change will deliver a substantial performance increase, with speeds rising from approximately 40 Mbps to over 500 Mbps per site, while also generating significant cost savings through the discontinuation of the existing MPLS network.

4.10 These benefits are dependent on the successful completion of the cyber security and cloud migration measures outlined earlier. Although the initial investment is considerable, it will result in a marked reduction in the Council's long-term internet and systems expenditure.

4.11 The work outlined throughout this report forms the foundation for the eventual replacement of the Council's two legacy financial management systems EDMS and Exchequer planned for 2027/28. *EDMS* has become increasingly costly to maintain, and its developer has indicated that the system will no longer be enhanced or supported in the future. *Exchequer*, while still operational, does not meet the standards of a modern financial management system.

4.12 Preliminary investigations are underway to identify and evaluate suitable replacement solutions. The introduction of a new, integrated financial system will enable the decommissioning of *EDMS* and *Exchequer*, reducing long-term IT costs and eliminating the need for associated support contracts.

5. IT Plan for 2026/27 onwards:

5.1 2026/27 – Move to Cloud / away from EDMS

- Server infrastructure to be decommissioned. All servives either moved to cloud or turned off.
- EDMS to remain supported and in cloud environment instead of on premise.

- Internet connection to be replaced at all SCC sites, moving away from expensive MPLS network.

5.2 2027/28 – Finance System

- EDMS and Exchequer to be replaced by new, modern financial package.

6. Recommendation:

It is recommended that the Committee:

6.1. Note the cyber security and IT systems update from the IT Support Officer.

7. Wards Affected: None

8. Background papers: None

9. Implications:

9.1 Financial: Within current IT budget
9.2 Legal: None
9.3 Personnel: All staff and councillors

9.4 Environmental Impact: None
9.5 Equalities Impact Statement: None