Appendix 1(d)

Cambridgeshire County Council

Cyber Security Strategy 2023 - 28

V.10

Julian Patmore
6-1-2023

Contents

Introduction

A Cyber Security strategy seeks to provide a comprehensive plan for an organisation to protect its digital assets and minimise the risk of cyber security incidents. A cyber security strategy should outline the steps an organisation will take to protect its networks, systems, and data from unauthorised access, use, disclosure, disruption, modification, or destruction.

This cyber security strategy will help the council to:

- Identify potential threats and vulnerabilities to its digital assets
- Prioritise cyber security investments and allocate resources effectively
- Implement appropriate cyber security controls and processes
- Respond quickly and effectively to cyber security incidents
- Ensure compliance with applicable laws, regulations, and industry standards
- Develop a cyber security culture and promote awareness of cyber security risks among employees
- Build trust and confidence with stakeholders, customers, and partners
- Continuously improve its cyber security posture over time.

A Cyber Security strategy is a critical component of the council's overall risk management framework and can help to protect against the increasing threat of cyber-attacks and other digital risks.

The Cyber Security team is responsible for implementing the cyber security strategy and policy.

All employees of the council are responsible for following the cyber security policies and reporting any suspected cyber security incidents.

Exec Summary

Executive Summary

Overview & context

Like many organisations, the Council faces significant and wide-ranging cyber threats. The continuous growth and evolution of systems brings with it the potential for more vulnerabilities to be exploited. We therefore need to ensure that our defences are as robust as possible, protecting not only against technical and workforce vulnerabilities, but also understanding the threats, and having a comprehensive knowledge of our data and digital assets.

The Council has invested significant resource in strengthening our position over the last 18 months. The Cyber Strategy is one of the many outcomes of this work and it supports a vision of becoming 'a recognised leader within local government in cyber security'. To achieve this vision, we propose a holistic, multi-layered approach that includes preparedness, response and recovery.

The Strategy adopts national, government and industry standards and has five cyber objectives. To support these objectives, it includes a comprehensive set of outcomes. These not only cover technical themes, but also address the human element, governance and management of our cyber intelligence.

Objective 1: Manage cyber security risks

Outcomes in this area cover the need to manage risk through established governance and clear accountability. The Council needs a comprehensive understanding of its digital assets and information about all Council data should be documented and updated regularly.

The Council should understand and manage the potential risks emanating from commercial suppliers, including appropriate cyber security due diligence, contractual provisions and the need for regular reviews and audits.

It is important to understand the potential impact of a cyber incident on Council functions and the need mitigate these. This could potentially involve cross-organisation cyber exercises to obtain a comprehensive view of impacts and plan accordingly.

The Council should be able to access relevant and actionable cyber security data that enables effective risk management. Likewise, it needs visibility of cyber security assurances to make effective decisions with the confidence that it has appropriate cyber security measures in place to manage the risks to its functions.

There are benefits to be gained from forming strategic partnerships with the private sector, academia and other councils to enhance proactive defence through sharing intelligence, best practices and collaborating on initiatives.

Objective 2: Protect against cyber attacks

This objective involves implementing measures to prevent unauthorised access, compromise, or damage to the council's digital systems and data by external or internal threat actors.

The Council has adopted a ‘defence in depth’ approach which uses layers of mechanisms to combat cyber threat; this mitigates the risks and gives increased overall resilience. It also manages user access and responsibilities robustly to enhance security and resilience.

The Council is adopting a ‘keep it simple’ infrastructure which reduces the security threat landscape, improves management, reduces exposure and inevitably reduces cost. They are also adopting a ‘zero trust’ environment which ensures the Council is safe from unsanctioned users or high-risk connections.

System logs and workflows are used to provide alerts and the aim is to move from a reactive to a proactive security service which enables automatic remediation if an incident occurs.

ITDS works to industry standards and frameworks to ensure strong security and for cost avoidance. It runs a regular patch management programme to ensure all systems are configured securely and as up-to-date as possible and has enforced industry recommended strong passphrases throughout the workforce.

The council is developing shared capabilities with other organizations to increase resilience against cyber-attacks, including sharing threat intelligence, participating in cyber security exercises, and developing joint incident response plans.

Lastly, the Council’s should have data classification in place to ensure all data is used and accessed appropriately, using a defined data ownership model with appropriate labelling, protection and management in place.

Objective 3: Detect cyber security events

This critical objective involves implementing measures to monitor the council's digital systems and data for suspicious activity or potential security breaches.

The Council should implement a comprehensive monitoring systems of network traffic, system events and user activity and should seek to provide 24*7 monitoring for all digital systems as well as using automated technologies to reduce the need for manual intervention.

There are good defences in place, but these are currently disparate. Work is underway to centralise these, and this will ultimately speed up security event detection.

The development of Data Loss Prevention (DLP) capabilities would be beneficial and would enable detection of insider threats and unauthorised data removal.

Key to the strengthening of Council cyber defences is the need to share capabilities, plans and exercises with other organisations. The Council should take every opportunity to practise its Cyber Incident Response Plan with these organisations.

The rise of artificial intelligence will inevitably lead to it being used in cyber crime and the Council will need to respond in kind by implementing AI powered cyber prevention technologies. This will further enable collaborative cyber detection with other organisations.

Objective 4: Minimise the impact of cyber security incidents

Minimising the impact of cyber security incidents is critical for local councils to limit subsequent impact on the council's operations, systems, data, and reputation.

Preparation is key and this includes maintaining the authority's incident response plan. It is incumbent on services to keep their business continuity plans updated.

For business areas to return to normal operations, data recovery is vital, and this relies on successful backups. Regular testing should take place to confirm that backups are retrievable.

Strong defences should be used to check individuals who access our systems or data, with continuous validation to authorise and retain access, 'least privilege' and device encryption by default.

In the event of a cyber incident, incident response procedures should be deployed with pre-defined plans and roles and responsibilities. The Council has several cyber incident playbooks which could be activated in this scenario. If necessary, IT will take services offline to protect Council data from further attack.

An area that should be addressed is the ability to identify the impact of new malware so that response can be managed effectively.

Whilst system and data restoration is important for services to return to normal after a security incident, to avoid further compromise, systems must be fully secure, patched and any remedial work undertaken **before** they are made available. This should be followed by a period of heightened security monitoring.

All cyber incidents should be followed up with a review of lessons learned to inform the Council's planning and response to future attacks.

Objective 5: Develop the right cyber security skills, knowledge, and culture

This objective is essential if the council is to ensure that its workforce can effectively manage cyber security risks and respond to security incidents.

Within IT, the Council must attract and retain staff skilled in cyber security and expand its resource in this area to deal with the increasing threat. Employee mental wellbeing should be considered as cyber security is a high stress environment. The Council should fund and provide regular training and development opportunities for any IT employees working in the cyber security environment.

Ultimately, the Council should aspire to have an appropriately resourced, dedicated Security Operations Centre capability to provide effective cyber event detection and response.

Cyber security is everyone's responsibility and Council the workforce is a key line of defence. The Council should promote a cyber security culture through awareness training and education campaigns, highlighting the need for cyber vigilance.

Achieving the Vision

A number of steps are needed to achieve this ambitious vision, and these are included in detail within the strategy. These steps will, however, need commitment from the Council.

Current and future tasks required to implement the strategy objectives are also included in detail.

Context

The increasing prevalence of cybercrime poses a significant threat to all organisations, particularly governmental ones. The nature of these threats can vary, ranging from organised criminal activities and state-sponsored disruption to insider threats from disgruntled employees. Furthermore, as IT systems continue to evolve and introduce new features, they may also introduce vulnerabilities that can be exploited by 'malicious actors' (any person or organization that intentionally causes harm in the cyber environment).

In the context of the local council, the busy and often rushed workforce may be more susceptible to making mistakes that can compromise the security of the council's systems and data. Additionally, the council has not previously prioritised cyber security, which led to cyber security falling behind in the list of priorities. This has meant the council's security posture is not as strong as it should be.

Over the past 18 months a lot of work has been done in this space, with an independent review being performed by the Department for Levelling Up, Housing and Communities (DLUHC) with recommendations actioned and a strategic review of the council's underlying infrastructure, end user devices, policies and organisational structure to improve the situation.

This strategy is part of that work and uses the Government's own Cyber Security Strategy as a framework

Our Digital, Data and Technology Roadmap to which this Cyber Security Strategy is intrinsically linked are outlined briefly below. The full documents can be found in this repository

Digital Strategy - The Digital Strategy seeks to set out the drivers, vision and plans for services delivered by IT & Digital over the next five years, for Cambridgeshire County Council.

Data Strategy - This focusses on the value of data as a core asset. It emphasizes the importance of data maintenance, quality and best practice whilst also promoting data availability and accessibility to those who need it.

Technology Strategy - The Technology Roadmap uses the themes outlined in the main Digital Strategy and details the proposed technologies that will be delivered to help achieve each theme's vision. It should also be read in conjunction with the Digital Strategy Action Plan.

Vision

The strategy's vision is:

"To be recognised as a leader within local government in cyber security in the next 5 years, taking a risk-based approach to protecting our digital assets and ensuring the confidentiality, integrity, and availability of our systems and data. We will achieve this by implementing best practices and continuous improvement, fostering a culture of cyber security awareness, and collaborating with stakeholders to ensure the highest level of protection against cyber threats."

Core

Achieving this Vision will require a new approach that not only protects the council but will have cyber resilience at its core.

Cyber resilience goes beyond just preventing attacks and detecting them in a timely manner. It involves having a holistic approach to cybersecurity that includes preparedness, response, and recovery, and focuses on ensuring that the council can withstand and quickly recover from any cyber security incidents.

Standards

The strategy will adopt and be based on the following standards

- NCSC Cyber Assurance Framework
- Government Minimum Cyber security standards (June 2016)
- Government Functional Standard Govs 007: Security 6 (Security Standard)

Although not mentioned in the national strategy, the Council is also working towards the following industry standards certified policies:

- Public Services Network (PSN) Code of Connection
- Cyber Essentials Plus

- Payment Card Industry Data Security Standard (PCI DSS)
- Information Security Management ISO/IEC 27001

Objectives

The strategy will have 5 objectives

The objectives of the strategy are to

1. Manage cyber security risks
2. Protect against cyber-attacks
3. Detect cyber security events
4. Minimise the impact of cyber security incidents
5. Develop the right cyber security skills, knowledge and culture

Objective 1: Manage cyber security risks

Managing cyber security risks is a critical objective for the council. This objective involves identifying, assessing, and prioritising potential cyber threats and vulnerabilities that could impact the council's systems, data, and operations.

Outcome 1: The council has established governance arrangements with clear accountability enabling effective management of cyber risks at all levels of the council

Governance & Accountability - A governance framework exists that provides clear roles and responsibilities for cyber security, sets the tone from the top, and ensures cyber security risks are managed effectively.

A holistic approach needs to be taken on cyber security that is not just from an IT perspective. All areas of the organisation need to be involved, with specific collaboration from Information Governance, Risk & Assurance, Comms, Property and HR.

There are 2 boards that support this function:

- Strategic Cyber Security board – Responsible for Cyber policy decisions
- Operational Cyber Security board - Responsible for operational security (OpSec)

Currently an annual IT health check is performed and remediation actions are carried out reduce the risk and support the Public Services Network (PSN) application. To support the rapidly changing nature of OpSec, the Council should move from an annual assessment model to a continual assessment model where evolving risks can be identified and remediated in a more timely manner. Standards set by the NCSC and Cyber Essentials\Plus programme require critical severity vulnerabilities to be mitigated within 7 days, and high severity vulnerabilities to be mitigated in 14 days.

A clear and comprehensive cycle of audits against the various policies and procedures are to be undertaken on a regular basis. The regularity of these audits should be driven by a risk based approach to minimise the risk.

A clear Cyber Incident Response Team (CIRT) and Cyber Incident Response Plan (CIRP) have been established with several available playbooks. These playbooks are aregularly practiced and this needs to continue in order to refine the effectiveness of these playbooks and develop new ones as new threats arise or are exposed.

Outcome 2: The council has comprehensive visibility and understanding of its digital assets enabling it to identify and manage vulnerabilities and the cyber security risks they present

Document Digital Systems – Documentation for all digital systems used by the council should be reviewed, amended, and created as required. This documentation should include the purpose, function, and dependencies of the digital systems.

The council should ensure that all systems have a valid and up-to-date Data Protection Impact Assessment (DPIA) to help identify and minimise any data protection risks.

The Council should implement a Configuration Management Database (CMDB) aligned with IT Infrastructure Library (ITIL) best practices to ensure a comprehensive view of the council's infrastructure and interdependencies are captured and are easily accessible.

Outcome 3: The council has comprehensive visibility of the data it handles and shares so that it can appropriately assess and respond to the risks it presents

Document Data - Document all data held by the council, including its classification, location, and sensitivity. This documentation should be regularly reviewed and updated. The documentation should include data flow diagrams to assist in Cyber incidents.

Ensure that the data conforms to the Council's Information Governance policies and procedures.

The council should leverage features in new and existing systems that support the automatic labelling of new data at creation by data owners, and the retrospective labelling of existing data. This

will allow the life cycle of data to be managed automatically with minimal manual input. This labelling should be included in any planned migration of data.

Outcome 4: The council understands and manages risks emanating from commercial suppliers

The council should develop a supplier management framework that ensures all suppliers are subject to appropriate cyber security due diligence and contractual provisions. This should include regular supplier reviews and audits.

This framework should include standard questionnaires to help manage this process for current and prospective suppliers which should be included in all current and future contracts and acquisitions.

Where appropriate, suppliers should be invited to take part in regular Cyber rehearsals to practise and minimise the impact of any potential Cyber incidents. We should seek to establish this capacity in future contractual arrangements, including elements of Cyber response requirements of suppliers.

Outcome 5: The council understands the threat it faces relative to its functions in order to plan appropriate mitigations, at both an organisational and cross-government level

The council should develop an understanding of the cyber security threats faced by the council and the potential impact of these threats. This should include regular threat intelligence gathering and analysis.

The process of threat analysis should be automated and combined with existing knowledge provided by a SIEM solution to automatically highlight risks. A future enhancement to this process should include the use of Security Orchestration And Remediation (SOAR) technologies to reduce the manual intervention required and improve response times to threats and incidents. AI should be utilised wherever possible to reduce manual intervention.

The council should seek to organise and become involved in cross-organisation Cyber exercises to understand and plan for the wider issues caused by industry sector cyber incidents.

Outcome 6: The council has timely access to relevant and actionable cyber security data that enhances their ability to make effective risk management decisions

The council should ensure that all employees have access to up-to-date cyber security information, including policies, procedures, guidance and training. Regular user facing Cyber exercises, such as Phishing simulations and passphrase testing, should be undertaken to raise awareness and measure effectiveness of current educational measures and the councils risk exposure.

Cyber threat feeds and Dark Web monitoring should be implemented into a future SOAR solution to improve response times and reduce risk.

Outcome 7: The council's cyber security assurance provides the council with the visibility it needs to make effective decisions and the confidence that it has appropriate cyber security measures in place to manage the risks to its functions

The council should establish visibility over the council's IT infrastructure and digital systems, including Security Information Event Management (SIEM) and automated monitoring of capacity and

performance of systems. This will enable the council to detect and respond to cyber security incidents.

The council should conduct a thorough assessment of the council's systems, networks, and assets to identify potential vulnerabilities and threats. This assessment should cover both technical and non-technical aspects, such as policies, procedures, and human factors.

The council should implement a robust vulnerability management program to regularly identify, assess, and mitigate vulnerabilities in the council's infrastructure and software. This should include continuous scanning, patching, and updating of systems.

The Council should ensure that appropriate security controls are in place to protect the council's critical assets. This includes, but is not limited to firewalls, intrusion detection and prevention systems, access controls, encryption, and other relevant security measures.

Outcome 8: Strategic partnerships with the private sector, academia and other councils are further embedded to enhance proactive defence

The council should establish strategic partnerships with other organisations in the public and private sector to share threat intelligence, best practices, and to collaborate on cyber security initiatives.

The council should establish a dedicated Security Operations Centre (SOC) to manage the Cyber threat. This could be in partnership with other organisations or paid third parties initially, while the capability is built. This collaboration may continue longer term or be replaced with a dedicated model subject to measured effectiveness.

Objective 2: Protect against cyber attacks

Protecting against cyber-attacks is a critical objective for any organisation, including local councils. It is imperative the council and their reputation are protected by establishing some cyber defences. Do nothing is no longer an option!

This objective involves implementing measures to prevent unauthorised access, compromise, or damage to the council's digital systems and data by external or internal threat actors. So, putting in place security controls and processes that can mitigate commodity attacks will go some way to making the council a hard target.

Adopting a defence in depth approach to mitigate risks through the full range of potential attacks will give the council more resilience to cope with attacks that use more bespoke tools and techniques.

A user education and awareness program would inform users to be aware of risks of discussing or sharing work related conversations to help avoid the potential of being targeted by phishing attacks.

Outcome 9: The council adopts a common approach to 'secure by design' to ensure that appropriate and proportionate cyber security measures are embedded within the technology government uses, and that the security of digital services is continually assured throughout their lifecycle

The councils are ensuring that all infrastructure, digital systems and applications are designed and built with security in mind, incorporating security controls and principles throughout their lifecycle. The councils have adopted a defence in depth strategy - which is the use of a layered approach - when designing the security posture. From a cloud perspective there are firewalls, email and web

filtering systems and a centralised endpoint management platform. From the Data Centre perspective there are multi zoned firewalls, web and email filtering plus AV software on all infrastructure and endpoints. The network perimeter defences are there to detect and block downloads, malicious domains and direct internet access. This makes it difficult for an attack to be carried out, provides detection easier and reduces the impact of any compromise.

From a user perspective the principle of least privilege and separation of duties is implemented. Users only have access to resources which are required to fulfil their employment duties. Also, certain processes cannot be just completed by a single person or system – which leads to a single point of failure – by making sure responsibilities are distributed.

From an infrastructure perspective the councils are moving towards a 'keep it simple' service which reduces the security threat landscape, improves management, reduces exposure and inevitably reduces cost. Along with this the councils make sure – as part of industry and vendor best practice – implement security on default configuration settings. The councils are regularly testing and reviewing their backup and restore procedures - by implementing simple services within the cloud such as snapshots - which reduce the recovery time objective.

The councils are now moving away from 'trust but verify' towards a 'zero trust' environment. This is where any access to any resource needs to be justified and monitored. This model enables the councils to stay resilient, secure, optimise remote access and reduces the attack surface. Enforcing dynamic policies at the endpoint provides granular and secure control to access resources. A zero-trust model ensures the councils are safe from unsanctioned users or high-risk connections.

Outcome 10: The council deploys cyber security controls commensurate with their risk profile to ensure that risks to their functions are managed proportionately

One of the essential requirements to prevent any Cyber-attacks is knowing what, where when and how to deploy controls across the organisation. As stated above the councils have implemented a defence in depth strategy which is continuously evolving and improving based on new and sophisticated cyber threats.

The councils have deployed a range of security controls – in the cloud and on premise - to protect against cyber-attacks, including next generation application firewalls, email and web filtering, anti-malware software, network segmentation, SIEM, DLP and access controls. These controls are regularly reviewed and updated as part of regulatory compliance and service improvement.

The SMH Data Centre is controlled using TDSI and monitored 24/7/365 by the CCTV Control Centre. Main council buildings – Sand Martin House and New Shire Hall - are also monitored by CCTV and controlled by TDSI. The councils have a numerous policies and procedures that help reduce threats and identify risks such as CIRP.

The councils undertake scheduled and regular infrastructure maintenance to make sure the environment is up to date with any vendor patches or critical updates to avoid any security vulnerabilities.

The councils have implemented a SIEM logging tool which provides a centralised repository of syslog's, events and enables workflows to be setup for alerting. The long-term goal is to move

towards a SOAR solution which will complement what is being done today by moving from a re-active to a pro-active cyber security service by enabling automation remediation – through artificial intelligence - when security incidents happen.

Outcome 11: The council's technology is appropriately configured, with standard profiles for common technology and architectures being developed and continuously updated

The councils ensure that all digital systems and applications are configured securely, including regular patch management and updates to software and hardware – via the scheduled maintenance windows -, and the use of strong passphrases. The councils – along with their partners – try to make sure that industry standards and frameworks – such as such as NCSC Cyber, NIST Cyber and Risk, Cyber Essentials Plus, ISO27001, ITIL and PCI DSS - are implemented not just for security reasons but as a rule of thumb and for cost avoidance. Vendor or industry reference architecture and solution designs are regularly consulted and incorporated in all ICT implementations.

Outcome 12: Shared capabilities, tools and services tackle 'common' cyber security issues at scale

The councils are developing shared capabilities with other organizations to increase resilience against cyber-attacks, including sharing threat intelligence, participating in cyber security exercises, and developing joint incident response plans. The councils have regular meetings – and attend webinars – with NCSC, DLUHC, OWASP and NLAWarp. This enables the councils to obtain government funding, advice, and guidelines for managing cyber threats and incidents. The councils need to also collaborate with the LGA and SOCITM to understand what other local authorities are experiencing and doing within the cyber space.

Outcome 13: The council's data is classified appropriately and handled and shared in a way commensurate to the risk it presents

The councils should be looking to have a data classification and categorisation model where data classification is used to ensure that all data is classified according to its sensitivity and accessed appropriately by staff who perform that job function. This should include the use of encryption and access controls to protect sensitive data.

Before a data classification framework can be implemented it is paramount that a data ownership model is also defined. The councils need to clearly define the data roles and responsibilities for data owner, controller, processor and custodian.

The council's data policy needs to incorporate how data is labelled, protected (rest, transit and use) and managed. In terms of data classification - the councils need to make sure data types with similar levels of risk sensitivity are grouped together – the need to include restricted, confidential, internal and public are just a few examples. In terms of the management of data the councils should have

various policies and procedures which should cover things like access, retention, disposal, and encryption.

Objective 3: Detect cyber security events

The objective of detecting cyber security events is critical for the council to quickly identify and respond to potential security incidents. This objective involves implementing measures to monitor the council's digital systems and data for suspicious activity or potential security breaches.

Outcome 14: Networks, systems, applications and end points are monitored to provide proportionate internal detection capability

The council should implement a comprehensive monitoring system that includes logging and analysis of network traffic, system events, and user activity. This should include the use of intrusion detection/prevention systems, security information and event management (SIEM) tools, and regular security assessments.

The council should seek to provide a 24*7 monitoring for all digital systems, but careful thought must be given as to the impact of this on existing teams. SOAR (Security Orchestration, Automation and Response) technologies, including AI, should be used to reduce the manual interventions required to rectify detected cyber security events.

The Council has good defences in the areas of edge network protection (firewalls), email filtering, malicious website protection and antivirus. While all these systems all provide logging, this logging of events is not currently centralised for easy centralised detection and each system need to be accessed individually to build a complete picture. This adds time to any current detection efforts and reduces effectiveness.

Work is underway on centralising the security solution logs with the implementation of a Security Information and Event Management (SIEM) platform. Having the security logs located in a single location will speed up the process of cyber security event detection.

The Council is moving away from a traditional data centre trusted model to a more modern Zero Trust Network Architecture (ZTNA). The deployment of ZTNA will provide vulnerability and threat detection within the network to complement the current detections done on the network edge firewalls.

The council should look to build on the work being done on detecting client behaviour anomalies by improving the network detection capabilities within the cloud environment replacing the conventional data centre.

Not all Cyber Threats are external. The Council should develop Data Loss Prevention (DLP) capabilities as part of any new technology implementation. DLP will enable detection of insider threats and data exfiltration scenarios. As data exfiltration commonly precedes a ransomware attack, detection of data exfiltration would allow the amount of data exfiltrated to be minimised along with raising a flag for a potential ransomware attack being in progress.

Outcome 15: Shared detection capability provides detection at scale

Shared Capabilities - Develop shared capabilities with other organisations to increase detection capabilities, including sharing threat intelligence, participating in cyber security exercises, and developing joint incident response plans.

The Council currently has a practiced Cyber Incident Response Plan (CIRP), a defined core and complete Cyber Incidence Response Team (CIRT), and a set of cyber playbooks for us with incidents. Detection is a key part of these playbooks, and the Council should continue to rehearse and refine these playbooks on a regular basis. The Council should take every opportunity to practice the CIRP with other organisations.

The rise of AI and the ever-decreasing costs of implementing it mean that AI will be misused as a tool by attackers. The Council will need to respond in kind to increase the speed and accuracy of response. Implementation of AI co-pilot or AI powered technologies will improve the speed and accuracy of detection.

With a more mature detection capability, the Council will be able to provide and consume indicators of compromise (IOC) feeds to and from other organisations. This will enable collaborative working in Cyber detection, reduce the effort and increase the speed of detection of cyber events.

Objective 4: Minimise the impact of cyber security incidents

Our authority will be targeted by malicious threats/cybercriminals. This is a risk we have accepted, but with all risks, we need to plan on how to mitigate/minimise the damage cyber security incidents could cause. Minimising the impact of cyber security incidents is critical for local councils to ensure that any impact is limited on the council's operations, systems, data, and reputation.

Outcome 16: The council is fully prepared to respond to cyber incidents

Prepare – Maintain and regularly update the authority's incident response plan. This plan should include clear roles and responsibilities, communication procedures, and escalation processes. Authorities should be building services in a resilient manner, with both cloud and on premises resistance to cyber-attacks. Any critical path or single points of failure should be identified and should be a managed risk. IT management should be engaging with the business to ask for teams BCP's to be updated regularly. Regular testing should be undertaken to confirm any backups taken can be used in anger.

The authorities should regularly check its security posture via Penetration testing. Firewall policies should be regularly reviewed. The authority should implement a Zero Trust Networking Access model. This would require all users, whether in or outside the authorities network, to be authenticated, authorised, and continuously validated for security configuration and posture before being granted or keeping access to applications and data. In addition, the authority should use the least privilege model when assigning permissions to users to access resources. Laptops and Mobiles devices used by staff should be encrypted by default and all accounts guarded by MFA.

Outcome 17: The Council rapidly responds to cyber incidents

Rapid Response – To ensure that the incident response team can respond quickly to any cyber security incident the authority should enact their pre-defined incident response plan with assigned roles and responsibilities for staff to react in a managed and efficient manner. The authority has created several Cyber incident playbooks which can be activated to deal with incidents in an appropriate manner. These play books will manage the incident.

The authority's cyber incident plan has dedicated teams to perform various tasks which are not limited to:

1. Survey The damage – Ascertain what damage has been caused and what systems have been compromised. Understand how systems have been compromised.

2. Limit Further Damage – Look to limit further damage but taking systems offline, segregating systems, or blocking traffic.

3. Record Details – Take log files and backups from an affected system this could be used during a criminal prosecution or to claim cyber insurance.

4. Inform – You need to inform affected users and senior stakeholders about the scope and scale of the breach. Also, inform any regulatory bodies if required.

Other resources will be pulled into the team if necessary with representation from Information Governance, Communications, HR and Property.

An important area for improvement is the Council's capability to identify the impact of new malware. Currently the Council must rely on third parties which can take several days to provide answers. Knowing the impact of malware that has been executed is critical in scoping the impact of the malware on the IT infrastructure and guiding the nature of any mitigations that need to be put in place.

If required and necessary, IT will take services offline to protect council data from further attack.

Outcome 18: The council restores systems and assets affected by cyber security incidents and resumes the operation of its functions with minimal disruption

Restore Systems – During an attack, and in the aftermath of an attack everyone will be working towards restoring affected systems and data to their pre-incident state as quickly as possible. Whilst doing so is the end goal it is important to ensure that the system is fully secure and fully patched and that any remedial work to improve the system has been performed.

The authority would need to create an incident checklist to confirm all tasks have been completed and that the system can be restored to the pre-incident level. This checklist would need to be owned by senior stakeholders and if engaged 3rd parties to confirm the system is now secure. We would not look to bring systems online until we are confident that we have identified and resolved any issues as failure to do so could lead to further systems being compromised and could exacerbate any issues.

Once the system has been restored the authority should look to introduce a heightened period of monitoring to identify any new or residual threats that may be exposed because of bringing the system back online.

Outcome 19: Lessons learned from cyber incidents drive improvements in the council's cyber security

Lessons Learned – After a cyber security breach we will need to learn from mistakes or areas of oversight.

Conduct a post-incident review to identify areas for improvement in the incident response plan and processes and implement changes to prevent similar incidents from occurring in the future.

Review the current Cyber Incident Playbooks and look to identify any weakness in them. Were they effective in this instance? Did we use the right playbook to deal with this incident? Do we need to update them? Do we need a new category of playbook?

The authority should review the tools it used to reduce or minimise disruption. Where these the right tools to use? The authority should look to identify new tools and make a business case as to what improvements they can make during the next incident.

The authority must be honest about any mistakes or failings when dealing with an incident. These mistakes should be used as learning opportunities and help to identified areas of training.

Objective 5: Develop the right cyber security skills, knowledge, and culture

The objective of developing the right cyber security skills, knowledge and culture is critical for the council to ensure that their workforce is equipped with the necessary skills and knowledge to effectively manage cyber security risks and respond to security incidents.

Outcome 20: All organisational cyber security skills requirements are understood

Understand Current Skills - Conduct a skills gap analysis to identify the current cyber security skills and knowledge within the council and identify areas for improvement. An education plan should then be created to develop cyber security skills.

Outcome 21: The council attracts and retains the diverse cyber security workforce it needs to be resilient

Attract and retain staff - Develop strategies to attract and retain skilled cyber security professionals, including offering competitive salaries and benefits, opportunities for professional development, and creating a positive and inclusive workplace culture.

The Council must build more capability in Cyber Response which will be very challenging in the current timeframe given the global shortage of qualified and experience Cyber Security Staff. A procurement is underway to provide modern apprenticeships in this field for current and future staff upskilling.

The mental health of cyber security personnel is an important consideration. Cyber security personnel are particularly prone to burnout and the Council needs to take measures to prevent this. The use of AI co-pilot technologies and assistance from third parties can reduce the workload and stress of cyber security staff and also enhance response times. Mental health needs to be very closely monitored during any incident to reduce the likelihood of staff sickness.

Ultimately the Council should aspire to have an appropriately resourced dedicated Security Operations Centre capability to provide effective cyber event detection and response. This could be enhanced using AI co-pilot technology, third party managed solutions or shared capability with other partner organisations. The NCSC provide valuable advice on building a SOC here: https://www.ncsc.gov.uk/collection/building-a-security-operations-centre

Outcome 22: The council continuously develops its cyber security workforce to ensure that it has and retains the skills it needs

Develop Workforce - Provide regular training and development opportunities to enhance the skills and knowledge of the cyber security team and other relevant staff members. This should include technical training as well as soft skills training such as communication and teamwork.

The Council has already instigated a series of cyber rehearsals By continuing these rehearsals, and widening them to include partner organisations, the Council can improve the overall cyber response of it's own and partner organisations.

A useful approach to cyber security staffing is to develop internal staff and attract new talent using apprenticeships. A varying level of available apprenticeships will match existing staff capabilities and allow for onward development opportunities.

Apprenticeships often use vendor neutral training to be as applicable to as many employers as possible. The Council should seek to supplement these vendor neutral qualifications with industry recognised cyber qualifications and vendor specific training aligned with technical solutions in use at the Council.

Many cyber security qualifications require provable continuous professional development, so the Council should seek to establish a budget to support this development.

Outcome 23: The council has a cyber security culture that empowers its people to learn, question and challenge, enabling continuous improvements in behaviours and resulting in sustainable change

Culture - Promote a cyber security culture throughout the council by raising awareness of cyber security risks and best practices and encouraging a proactive and vigilant approach to cyber security.

It is important to baseline the current cyber behaviours of staff. By baselining this behaviour, the effectiveness of cyber security awareness campaigns and tests can be measured on an ongoing basis.

Cyber security is everyone's responsibility and by carrying out a continuous education program this can be highlighted at all levels. The Council should be careful to implement any testing using a "no blame" culture to ensure the engagement of staff.

Achieving the Vision

The strategy builds on the good work that has already been achieved to date, however, it recognises that there is still more to do to build its resilience in face of the continually evolving threat landscape that presents itself. This landscape is dynamic and changes at an increasing exponential rate, the vision that has been laid out, is ambitious and will need commitment from the council. To achieve this the following steps will be taken:

1. Implement this strategy with its clear set of objectives and outcomes within.
2. Implement best practices and continuous improvement to ensure that the council's systems and data are secure. This includes but not limited to regular vulnerability assessments, penetration testing, and security audits.
3. Foster a culture of cyber security awareness by providing regular training and awareness programs for all staff across the council, highlighting the importance of good cyber hygiene practices, and encouraging reporting of any suspicious activity or incidents.
4. Adopt the NCSC's Cyber Assessment Framework (CAF)
5. Adopt the NCSC's Target Operating Model for a SecOps function
6. Collaborate with stakeholders, including other local councils, government agencies, and private sector organisations, to share knowledge and best practices, and work together to ensure the highest level of protection against cyber threats.
7. Ensure that cyber security is embedded throughout the council's operations and decision-making processes, including procurement, IT system development and maintenance, and incident response planning.
8. Ensure that Cyber Security is continued to be recognised as a high-level risk on the council's risk register and that appropriate measures are continually refreshed as when threats and mitigations change
9. Continuously monitor and evaluate the effectiveness of the council's cyber security measures and adjust the strategy and objectives as needed to ensure that the vision is achieved within the next 5 years.

Implementation

The implementation of this strategy is split between Now and Next for each of the objectives. Now are activities that are currently being undertaken and or will be completed in the next 18 months. Next will look at our longer-term ambitions.

Objective 1: Manage cyber security risks

Now	**Next**
Enhanced governance and accountability across the council in relation to cyber security at both strategic and operational levels Enhanced asset discovery and management discovery measures across the council Develop a proactive vulnerability management process using internal and external testing to meet NCSC and Cyber Essentials\Plus standards Re-certify PSN accreditation Further embed strategic partnerships with the private sector, academia and other local authorities	Achieve Cyber Essentials Plus accreditation Map systemic risks in council's supply chain working alongside the council's procurement strategy Enhanced automated, live threat information shared at scale across partners Implement the proactive vulnerability management process Align to PSN replacement Ensure all systems have a completed Data Protection Impact Assessment (DPIA)

Continue working with internal audit managing and monitoring current and future cyber risks Ensure all new systems have a completed Data Protection Impact Assessment (DPIA) and Data Flow Diagrams Continue to practice and develop CIRT\CIRP processes Manage and monitor the Cyber risks caused by human behaviour including Phsihing and Passphrase management Develop cyber specific supplier questionnaires and develop contracts to embed Cyber management into the supply chain	Conduct a thorough assessment of the systems, networks, and assets to identify potential vulnerabilities and threats. This assessment should cover both technical and non-technical aspects, such as policies, procedures, and human factors Implement a Configuration Management Database Develop data labelling and policies to support the confidentiality, integrity and authenticity of council data Extend cyber threat exercises to suppliers and partners Implement SOAR technologies with automated threat and dark web monitoring feeds Introduce AI technologies where available to automate workload and increase detection and remediation effectiveness

Objective 2: Protect against cyber attacks

Now	**Next**
Implement Zero-trust/Trust verify networking principles Manage, upgrade or remove legacy technology across the estate Common configuration for common digital products and services developed and shared Refresh infrastructure management policies Automation through zero touch deployment Classifying and categorising data – AD Group membership Appropriate network and user controls Centralised hub/spoke connectivity Defence in depth strategy	Harnessing of emerging technologies to enhance cyber security Adopt the government's future 'secure by design' framework Implement best practices and industry standards & frameworks Machine Learning/Artificial Intelligence – Introduce DevOps and AIOps Identify roles and responsibilities Attribute-based access control Introduce NAC (802.1x) on the wired/wireless environments Distributed physical with centralised logical connectivity. Align WAN networking to cloud connectivity.

Industry Cyber Certification	Introduce more layers of security without complexity and performance being impacted
SIEM	Implement a SOAR/SOC service for managing and monitoring a pro-active Authentication, Authorisation, Accounting and Auditing service.
Collaboration	Build relationships other authorities and professional bodies to learn, explore and implement
Infrastructure Peer Review	Engage with third parties for impartial reviews on whether best practices, standards and frameworks are being implemented
Data Policy	Classify, categorise, protect and manage
Support & Maintenance	Achieving Cyber Essentials Plus. All software and hardware on the production environment needs to be supported.

Objective 3: Detect cyber security events

Now	**Next**
Comprehensive and proportionate detection capability developed across the council.	Every digital system to have 24/7 security monitoring.
Consolidate existing security solutions logs into SEIM solution.	Harnessing future technology and AI to grow and accelerate the detection of cyber security events.
Enhance internal capability to forensically identify the payload of new threats.	Adopt the government's common language for organisations to record information about cyber security incidents and 'near misses'.
Internal threats and vulnerabilities detection capability to be enhanced as part of Zero Trust design principles	Expand cyber exercises to include partner organisations for enhanced collective response.
Continue to practice and refine response to cyber events.	Use automated technologies for sharing threat intelligence with other organisations.
Develop Data Loss Prevention (DLP) capabilities to minimise data breach incidents and provide early warning of other potential attacks	Improve capability to detect network based events in new cloud infrastructure.
	Implement a Security Orchestration, Automation and Response (SOAR) service to automatically detect if an event is happening

Objective 4: Minimise the impact of cyber security incidents

Now	Next
Routine cyber security exercising of council critical functions. Finalise and communicate the Cyber Incident Response Plan. Enhance the regular Testing of DR and Backup Systems When onboarding suppliers confirm their security posture and practices.	Independent review (lessons learnt) process for all serious security incidents and vulnerabilities Implement a SOAR service that automatically takes services offline on detection of an event Work with departments to ensure that Business Continuity Plans reflect potential outages to systems

Objective 5: Develop the right cyber security skills, knowledge and culture

Now	Next
Finalise recruitment of SecOps Apprentice Ensure there is a resilient number of CISSP certified staff to lead on cyber incidents Deliver a programme of cyber security culture improvements Work with Cyber Griffin a London Police initiative to build on the council's knowledge and awareness Promote good mental health practice amongst staff Continue cyber incident rehearsals and involve more Council staff outside of IT Establish the delivery model for the Security Operations Centre (SOC)	Implement cyber security testing, to better understand the council's risk and target user education Provide budget for continuous professional development Widen cyber incident rehearsal to include staff from Council partner organisations Implement the defined SOC