Chichester District Council

ICT Security Plan

Our proactive approach to protecting against ICT security threats and breaches.

Contents

Background 3
Why (have a Security Plan): 3
Strategic Focus 3
Key Threats 3
What (will we do): 4
Develop a Business Model for Information Security 4
Create an Information Security Framework 4
How (will we do it): 4
Designed-In Security (by default) 4
Security Scorecard (compliance, IT governance & risk) 5
When (will we do it): 5
Critical Success Factors (Actions) 5
CSF 1: ICT Security Scorecard 5
CSF 2: Zero Trust 6
CSF 3: Audit of Current Security Measures 6
CSF 4: Enterprise Architecture Mapping Project 6
CSF 5: Microsoft 365 Project 6
CSF 6: ICT Change Management & Configuration Management Data Base 6
Appendix 1: Information Security Framework 7

Background

Imagine trying to deliver Council services today without the use of technology and communication systems. While the benefits are clear increasing reliance on IT, the pace of technological innovation and the complexity of system interdependencies are continually creating new risks and challenges.

Cyber-attacks by both opportunist and professional criminals are on the rise. In the past year targeted threats to our sector have increased in both volume and sophistication, encouraged by the disruption caused by Covid-19. The Public Sector is now seen as a legitimate target but, despite National Intelligence agency support, we have seen multiple attacks on local government agencies causing disruption for thousands of residents and costing millions of pounds to resolve.

Maintaining CDC's secure perimeter is our foremost priority. But the changing demands on our IT estate supporting digital channels and remote working styles, coupled with the escalating threats we face necessitate a more sophisticated defensive strategy. Through our new Security Plan we will review, refocus and consolidate our position, building on our existing cyber resilience capabilities. More evolution than revolution, this will reflect "the whole as greater than the sum parts", with the objective to be better positioned to deal with the shifting threats we face.

***Why (have a Security Plan)*:**

Strategic Focus

Our critical to quality requirement is simple, to keep the Council working securely and effectively. In order to support the Council's objectives, our security plan will continue to provide assurance in both today's and tomorrow's business environment. As new complex risks emerge, proactive and consolidated actions must replace passive and transferred mitigations.

Recent Central Government and National Cyber Security Centre guidance identify new specific 'threat vectors':

1. Cyber criminals continue to consider councils as attractive target.
2. Increased cyber risks due to expansion in home/remote working.
3. Ransomware attacks represent the greatest risk to the council.
4. Growing adoption of 'cloud' technologies require re-evaluation of legacy security position.

Key Threats

Specifically, for Chichester District Council, these are can be consolidated into three key threats:

1. Stealing sensitive data: we hold large amounts of personally identifiable information (PII) that can be easily exploited or sold by criminals. We also hold an abundance of financial data from on-line services, such as payments for council taxes and parking permits. This data is highly sought after by cyber criminals for use in fraud and blackmail cases.
2. Disrupting services: we are also vulnerable to attacks designed to disrupt digital services. Techniques such as ransomware are particularly devastating.
3. Exploiting the cloud: whilst cloud migration offers opportunities to reduce costs and create efficiencies, as well as increasing remote working capabilities, it also provides more attack surfaces, e.g. file sharing capabilities. Without the right security policies and strong and reliable infrastructure, critical data can be inadvertently exposed online.

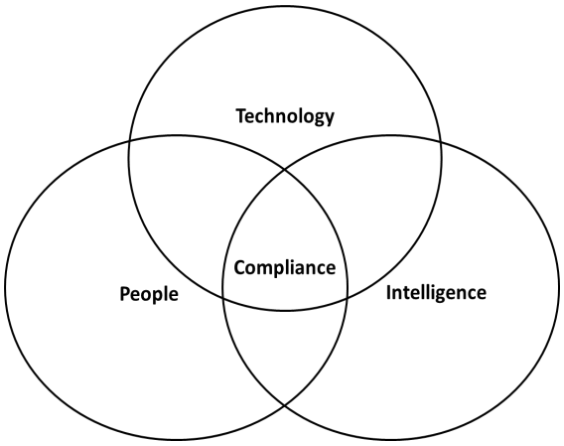
***What (will we do)*:**

Develop a Business Model for Information Security

Our new consolidated approach begins with the creation of a simple business model, which is easy to understand and accessible to all. Within each strand actions and activities focus on holistic risk reduction, simple monitoring and providing management with improved oversight and assurance.

In addition using the model will help overcome a number of false assumptions highlighted in recent MHCLG and NCSC guidance.

- Cyber security is often viewed as a technical issue, rather than a business issue, and is not seen as being everyone's responsibility.
- There is no single solution that can mitigate 'cyber risk', as issues vary in size, severity and context.
- The potentially overwhelming amount of guidance paradoxically leads to a lack of clarity and confusion.



Create an Information Security Framework

Next, we take the Business Model and apply it to various aspects within our existing IT estate. This provides the basis for repositioning and consolidating all the interrelated aspects of our current cyber security activities. From here we will undertake a gap analysis, taking into account the changing nature of the risk environment and the emergence of new key threats. This is used to inform our priority 'Critical Success Factor' actions.

A full description of our framework can be found at Appendix 1, which has been created on the new security principle; **that the content, information and the knowledge based on it must be adequately protected, regardless of how it is handled, processed, transported or stored**. This is a fundamental departure from our traditional network and system security approach. Historically, on-premises models followed the 'trust but verify' principle, with the focus placed on established network and perimeter security. The need to accommodate more flexible and remote working patterns, as well as the increasing commercial pressures to adopt cloud based applications, necessitates our move towards a 'borderless' security strategy.

***How (will we do it)*:**

Taking the Information Security Framework activities/actions and turn them into quantifiable goals (intangible and non-measurable) and objectives (tangible targets). Representing a state of constant vigilance, 360° defence and continuous improvement, this will provide a balance between outcomes (goals) and outputs (objectives) against which progress can be monitored.

Designed-In Security (by default)

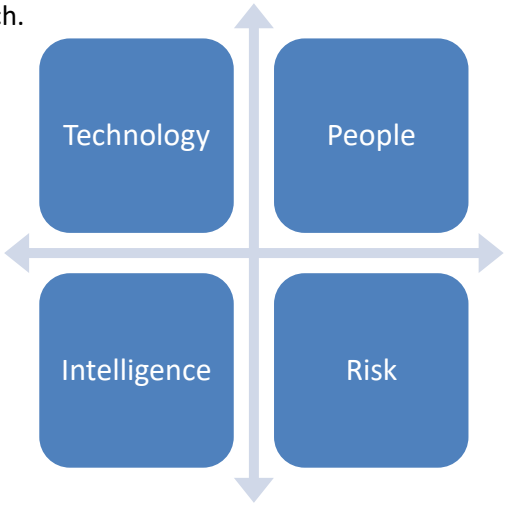
Reducing risk through improved cyber security analysis. Vulnerability to attacks can be reduced if analysis is conducted across an entire user journey. Consideration of the software, data handoffs

and user touchpoints will improve build plans and our ability to maintain services in a secure manner. As will considering the full supply chain and lifecycle during the procurement process.

Building on our legacy strengths we will adopt solutions that, whilst integrating with our existing security environment, move us towards a 'borderless' or Zero Trust position. Moving to a Zero Trust model we will need to apply new design principles to all future improvements across our network and systems. Operationally it requires all users, even those inside the network, to be authenticated, authorised and continuously validated against security configurations before access is granted to applications and data. We will, however, design this without the need for users to continually re-enter passwords or security credentials. Adding this layer of security will be critical as we incorporate more cloud-based applications rendering our perimeter 'borderless'.

Security Scorecard (compliance, IT governance & risk)

In the absence of any widely accepted industry-standard approaches to cybersecurity measurements or technical metrics, we have developed a scorecard approach. Combined these SMART measures will provide an 'at a glance' assessment of our 'we are secure' status. The outputs from each inform our continuous improvement cycle, while the outcomes provide stakeholder group assurance of the effectiveness of our plan.



When (will we do it):

Critical Success Factors (Actions)

CSF 1: ICT Security Scorecard

By end of Q1 2021 we will develop our scorecard. Thereafter it will be updated quarterly, with an annual review of the relevance of monitored measures.

Technology:

- Mean time to patch covered systems
- Number of patches deployed
- Vulnerability scan coverage
- % of systems without known high vulnerabilities
- Firewall statistics

Intelligence:

- TrackITs raised / completed
- Laptops replaced
- Blocked internet access attempts

People:

- Employee's trained: education programme
- Nos. of internal emails blocked / external blocked
- Nos. of discovered / reported malware

Risk:

- Unplanned system interruptions
- Back-up / DR tested
- Maintain PSN accreditation
- Option appraise alternative assurance frameworks
- Review corporate/service;
    - Recovery Point Objectives
    - Recovery Time Objectives
    - Service Delivery Objectives
    - Maximum Tolerable Outages
    - Allowable Interruption Window

CSF 2: Zero Trust

By the end of Q1 2021, we will define and agree our Zero Trust model and implementation principles. Then use the findings to inform our developing Network Refresh Project (ICT Service Plan 2021-22) outcomes.

CSF 3: Audit of Current Security Measures

By the end of Q2 2021, we will have undertaken an exercise grouping all existing cyber security monitoring (i.e. NCSC Early Warning-NEWS, PDNS, MailCheck, and Ops.Mgr.), intelligence sources and staff engagement activities. Specific focus will be placed on existing capabilities focusing on ransomware, phishing and password spraying. A gap analysis will then inform options for engaging with a managed security service provider (MSSP) to provide enhanced security monitoring and incident response capabilities.

CSF 4: Enterprise Architecture Mapping Project

To be completed by the end of Q4 2021. Understanding all aspects of our Enterprise Architecture (EA) is fundamental if we are to successfully manage our IT estate in a continually evolving world. Creating an EA diagram will provide a compact single schematic overview. It will, for the first time, link together business architecture (the key service processes IT support, corporate IT capabilities and stakeholders), the data and information flows supporting each activity and, identify the technology infrastructure and core applications used in each process.

It is complicated and complex. But once complete, will provide a thorough capability that will enhance our ability to manage the business, information, process, and technology changes necessary to execute the Council's strategy.

CSF 5: Microsoft 365 Project

By end of December 2021 we plan to have delivered full Microsoft 365 functionality across the Council. This is a major project and represents a significant move into the 'cloud' environment. Through this project we will be incorporating a borderless security position requiring a review of all current ICT policies and procedures.

CSF 6: ICT Change Management & Configuration Management Data Base

By end of Q1 2021 we will have introduced our new Change Management Process. Assessing security impacts within our change management activities will enhance our IT service management capabilities. We will also explore the benefits of having a configuration management database (CMDB), and the associated advantages it offers under CSF2 and CSF4.

Appendix 1: Information Security Framework

(1) Technology: Robust Infrastructure (hardware, software, network, OS, storage)

IT Function	Activities & Actions
Architecture	• Robust picture of systems infrastructure • Secure-by-design • Security designed into procurement
Monitoring	• Monitoring strategy & supporting policies • Continuously monitor all systems and networks • Analyse logs for unusual activity that could indicate an attack • Consider Cyber Threat intelligence solution
Secure configuration	• Introduction of new change management process • Apply security patches • Ensure secure configuration of all systems is maintained • Create system inventory / Define baseline build for all devices
Network security	• Protect network from attack • Defend network perimeter / filter out unauthorised access and malicious content • Monitor and test security controls / network configuration

(2) People: increasing workforce capability

IT Function	Activities & Actions
User education & awareness	• User security policies • Staff training • Ongoing cyber risk awareness training & support • Share knowledge of incidents affecting other LA's
Home & Mobile working	• Mobile working policy • Apply secure baseline and build to all devices • Protect data in transit and at rest
Removable media controls	• Removable media policy • Limit media types and use • Scan all media for malware before importing
Malware prevention	• Malware relevant polices • Establish anti-malware defences

(3) Intelligence: threat and contextual based

IT Function	Activities / Actions
Incident management	• Establish incident response & disaster recovery capability • Test incident management plans • Active participation in Information sharing networks (e.g. WARP)
Asset management	• Devices, information & systems • Develop Configuration Management Database
Asset retention and disposal	• Policies and procedures • Audits
Managing user privileges	• Establish effective management processes • Limit number of privilege accounts

- Limit user privileges & monitor user activity
- Control access to activity and audit logs