

**To: Audit and Governance Committee**

**Date: 5 November 2018**

**Report of: Head of Business Improvement**

**Title of Report: The risks, challenges, and actions being taken by the Council to ensure the best possible cyber security.**

**Summary and Recommendations**

**Purpose of report: To inform the Committee on matters relating to cyber security.**

**Key decision: No**

**Executive Lead Member: Councillor Nigel Chapman**

**Policy Framework: Efficient and Effective Council**

**Recommendation: That the Committee notes the content of the report**

**Appendices:**

**Appendix A Corporate Risk Register**

1. **Purpose of this paper**
   1. This paper answers the question raised by the Audit and Governance Committee on 25th July 2018 regarding the risks, challenges, and actions being taken and what more can be done to ensure the best possible cyber security for the Council.
2. **Context**
   1. The UK Government body, National Cyber Security Centre (NCSC), which is part of Government Communications Headquarters) GCHQ, owns the National Cyber Security Strategy1.
   2. The NCSC describes cyber security as "the protection of information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, *harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, because of failing to follow security procedures.”*
   3. With councils making more local public services available digitally, getting more of their workforce online and planning greater collaboration and integration work with partner organisations – which requires the sharing of residents’ and business customers’ data – reviewing and reinforcing current cyber security arrangements is a key priority for all local authorities.
   4. Councils have data sharing protocols, data handling and management guidance, as well as different levels of access in place for different data sets and systems to manage and protect sensitive data. However, as we have seen through recent cyber-attacks including the “WannaCry” ransomware attack which had a major impact on the NHS, those with criminal or hostile intent will continue to try to breach our security to steal the data we hold and/or damage our systems. Therefore, we need to continuously review, refresh and reinforce our approach to cyber security.
   5. This paper set out the nature of these threats, our vulnerabilities and how these continue to evolve, how we assess our preparedness, and what we need to do to mitigate the risks of cyber-attack.
3. **The nature of cyber threats**
   1. As our reliance on computer networks to share information grows, so do the opportunities for those who would seek to compromise our systems and data. Malicious cyber activity knows no boundaries. Cyber criminals are broadening their efforts and expanding their modus operandi to achieve higher value pay-outs from citizens, organisations and institutions.
   2. Cyber threats fall broadly into five internationally recognised categories. Here we consider each in turn.
   3. Cyber crime
      1. Cyber-crime includes two interrelated forms of criminal activity:

Cyber-dependent crimes – crimes that can be committed only using Information and Communications Technology (ICT) devices, where the devices are both the tool for committing the crime, and the target of the crime (e.g. developing and propagating malware for financial gain, hacking to steal, damage, distort or destroy data and/or network or activity);

Cyber-enabled crimes – traditional crimes which can be increased in scale or reach using computers, computer networks or other forms of ICT (such as cyber-enabled fraud and data theft).

* + 1. Much of the most serious cyber-crime – mainly fraud, theft and extortion – continues to be perpetrated predominantly by financially motivated Russian-language organised criminal groups (OCGs) in Eastern Europe, with many of the criminal marketplace services being hosted in these countries.
    2. Even when key individuals responsible for the most damaging cyber-criminal activities against the UK are identified, it is often difficult for the UK and international law enforcement agencies to prosecute them when they are in jurisdictions with limited, or no, extradition arrangements.
  1. State sponsored threats
     1. We regularly see attempts by states and state-sponsored groups to penetrate UK networks for political, diplomatic, technological, commercial and strategic advantage, with a principal focus on the government, defence, finance, energy and telecommunications sectors.
  2. Terrorists
     1. Terrorist groups continue to aspire to conduct damaging cyber activity against the UK and its interests. The current technical capability of terrorists is judged to be low. Nonetheless the impact of even low-capability activity against the UK to date has been disproportionately high: simple defacements and doxing activity (where hacked personal details are ‘leaked’ online) enable terrorist groups and their supporters to attract media attention and intimidate their victims.
  3. Hacktivists
     1. Hacktivist groups are decentralised and issue-orientated. They form and select their targets in response to perceived grievances, introducing a vigilante quality to many of their acts. While the majority of hacktivist cyber activity is disruptive in nature (website defacement or DDoS), more able hacktivists have been able to inflict greater and lasting damage on their victims.
  4. Script Kiddies
     1. So-called ‘script kiddies’ – generally less skilled individuals who use scripts or programmes developed by others to conduct cyber-attacks – have access to hacking guides, resources and tools on the Internet. Due to the vulnerabilities found in internet-facing systems the actions of ‘script kiddies’ can, in some cases, have a disproportionately damaging impact on an affected organisation.
  5. Internal Threats
     1. Whilst not falling into the five categories of cyber threat, there are additional risks associated with internal threats – cyber-crime resulting from the activities of one or more individuals with official access to the systems and data of an organisation. This vector has the highest percentage of incidents unreported due to the risks of reputational damage.

1. **Types of vulnerabilities**
   1. In computer security terms, vulnerability is a weakness which can be exploited by an attacker to perform unauthorized actions within a computer system. There are four key areas where organisations can be exposed to cyber vulnerabilities. These are considered next.
      1. Increasing types of uncontrolled devices

Most people conceive of cyber security through the prism of protecting devices such as their desktop computer or laptop. As the Internet has become increasingly integrated into our daily lives in ways we are largely oblivious to. The ‘Internet of Things’ (IoT) creates new opportunities for exploitation and increases the potential impact of attacks. Therefore, we are no longer just vulnerable to cyber harm caused by the lack of cyber security on our own devices but by threats to the interconnected systems, whether with other organisations, or with home and personal (bring your own) devices.

* + 1. Poor security compliance

Cyber-attacks are not necessarily sophisticated or inevitable and are often the result of easily rectifiable security vulnerabilities. In most cases, it continues to be the vulnerability of the victim, rather than the ingenuity of the attacker, that is the deciding factor in the success of a cyber-attack.

It is the Council executive board that decides on where and how to invest in cyber security based on a cost-benefit assessment and it remains ultimately liable for the security of the data and systems. Only by balancing the risk to our critical systems and sensitive data from cyber-attacks, with sufficient investment in our people, technology and governance, can we reduce, though never eliminate, our exposure to potential cyber harm.

* + 1. Insufficient training and skills

In many organisations, staff members are not sufficiently cyber security aware and do not understand their responsibilities in this regard. The public is also insufficiently cyber aware. We need to ensure all our staff have the knowledge and skills that will allow us to keep pace with rapidly evolving technology and manage the associated cyber risks. This gap is not limited to the Council but represents a wider vulnerability that is being examined at a national level.

* + 1. Outdated computer systems and software

Like many organisations, we continue to use a few legacy systems until we can afford to upgrade them. Software on these systems often relies on versions that can suffer from vulnerabilities that attackers look for and have the tools to exploit.

1. **Existing Council measures of cyber security**
   1. The Council continues to invest in a range of measures to protect the systems and the data it holds from potential attacks. These measures, reflecting those recommended by the NCSC, are:
      1. User Education

On-line policies and guidance for the workforce and elected Members.

* + 1. Network Perimeter Defences

Using firewalls and scanning services; blocking insecure or unnecessary services, only allowing permitted websites to be accessed.

* + 1. Malware Protection

Block malicious emails and preventing malware being downloaded from websites. Scanning email documents and attachments using an accredited national service provider, to reduce the quantity of spam and block known threats before they reach our network.

* + 1. Password and other Security Policies

Prevent users from selecting easily guessed passwords and locks accounts after a low number of failed attempts.

Best practice guidance on how systems and data should be handled to minimise the risk of cyber-crime.

* + 1. Secure Configuration

Restrict system functionality to the minimum needed for business operation. Systematically apply to every device that is used to conduct business.

* + 1. Patch Management

Apply patches at the earliest possibility to limit exposure to known software vulnerabilities.

* + 1. Monitoring

Monitor and analyse all network activity to identify any malicious or unusual activity.

* + 1. User Access

Well maintained user access controls that restrict the applications, privileges and data that users can access.

* + 1. Device Controls

Devices within the internal gateway are used to prevent unauthorised access to critical services or inherently insecure services that may still be required internally.

Encrypting laptops and desktops to render the information if holds unreadable in the case of loss or theft of the device.

* + 1. Compliance, and Independent Assessments

Applying government’s cyber security guidance.

Using an accredited data centre provider; working to the same level as central government.

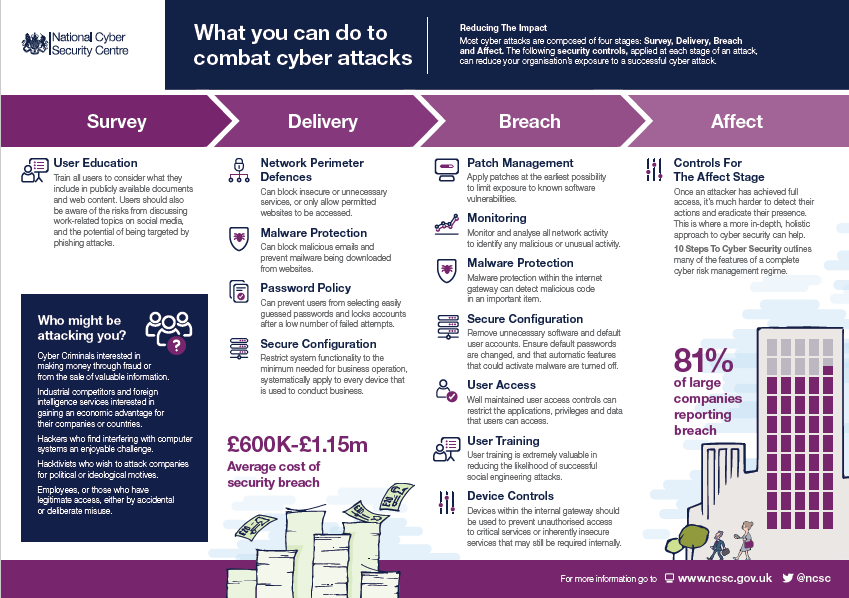
Annual, independent health check to verify the robustness of our security systems.

Complying with the Code of Connection regime which requires good cyber security, to connect to central government networks, e.g. PSN and the Health and Social Care Network.

1. **Summary of actions needed**
   1. Whilst the Council currently meets national standards of security compliance, the bar rises annually as more sophisticated techniques are used to illegally access our network and data. Central government assessment criteria for awarding compliance become more challenging and every public-sector body, us included, must continually improve our standards to pass the exacting independent assessments that we are legally obliged to take on an annual basis.
2. **What is needed to keep our ICT security defences up to date**
   1. The first step in protecting against cyber threats is to ensure our existing defences are kept up to date. This includes regularly updating security software, sometimes as frequently as on a daily or weekly basis. Other times, this occurs on a periodic basis as vendors retire or update their products.
   2. Security hardware, including such things as firewalls and proxy servers, generally need upgrading or replacing every few years, or when sophisticated threats arise that exist previously unknown vulnerabilities. Within the Councils budget preparation process for the next Medium Term Financial Plan bids have been submitted to upgrade to replace or upgrade several existing security products as follows
      1. Citrix Replacement – our remote access software (to work outside of the office) is being retired and we must replace it with another product -
      2. Sophos Security UTM - The Sophos UTM manages the remote VPN connections for the Council and all the email scanning for virus and malware. As the contract is due to expire, we need to either renew the contract or go out to tender for a replacement -
      3. Windows 2008 – The existing Windows software is about to go out of support and therefore needs replacing -
      4. Two-factor authentication (2FA)– central government compliance rules require all public-sector organisations to enforce 2FA on laptops, phones, etc. The current solution needs replacing with a more modern equivalent that is compliant. -
      5. 802.1X network point security – This work is required to secure all the network points (where computers are plugged in) across all Council offices. -
   3. Maintaining existing ICT security systems up-to-date requires capital investment. As these systems require frequent upgrades, ring-fencing an amount of capital each year would improve the pace at which emerging threats are dealt with, ensuring the security defences of the Council remain as robust as possible.
3. **Ensuring business systems are compliant**
   1. At the time of writing, several line-of-business systems are either coming to end-of-life or no longer meet compliance standards and replacing in the coming year with a not insignificant amount of time and resource on the part of service areas and the ICT team.
4. **Providing resilience in the event of a cyber-attack or disaster**
   1. The Council currently has a degree of resilience capability in the event of a sustained cyber-attack or disastrous event. Consideration needs to be given to providing an alternative disaster recovery operation centre for the executive team, support services and ICT to work from in the event of loss of St. Aldates and Town Hall. The current facilities fall well short of being adequate.
5. **Responding to new user needs and technologies**
   1. The changing and growing demands of users, and the introduction of new technologies such as iPads and voice-activated devices (e.g. Google Assistant, Amazon Alexa), requires investment in additional tools, solutions and training to use these systems and to provide the security wraparound needed to protect the data they hold or allow access to.
6. **Raising the level of awareness of staff and members**
   1. Staff and member security awareness training is another area where leadership commitment and people’s time is needed to ensure everyone understands how to safeguard the Council’s assets and information. Annual refresher courses would be of further benefit and reflect best practice elsewhere.
7. **Engaging with other authorities and security groups**
   1. The Council has the opportunity to engage with partners across the public sector through participation in the Cyber Security Information Sharing Partnership (CiSP), Warning, Advice and Reporting Points (WARPs) and Local Resilience Forum (LRFs) to protect our systems from and put in place plans to respond to cyber-attacks.
8. **Conclusions**
   1. As cyber security threats continue to grow and become ever more sophisticated, the importance of adequate and timely funding to at least maintain the existing level of assurance to the Council cannot be understated, and ideally more attention and investment given to enhance existing defences.
   2. Whilst the Council has policies and procedures in place covering the main elements of cyber security, additional awareness training would benefit all Council employees and Members, and refresher sessions on an annual basis would help ensure that those with access to Council systems and data are kept informed on the threats and mitigating actions they can take.
   3. Whilst much is being done by the ICT team to ensure that existing security systems are fit-for-purpose and compliant with national assessment criteria, the evolving threats to cyber security mean that this work remains on-going and continuously increasing in complexity and magnitude.
9. **Climate Change / Environmental Impact**
   1. There are no specific impacts arising directly from this report. The appendices set out mitigations against the Council’s corporate risks.
10. **Equalities Impact**
    1. There are no equalities impacts arising directly from this report.
11. **Financial implications**
    1. The bid for new expenditure on ICT related software and hardware will be assessed in the current budget preparation process and recommendations made to City Executive Board and Council accordingly.
12. **Legal implications**
    1. There are no legal implications directly relevant to this report but having proper arrangements to manage risk throughout the organisation is an important component of corporate governance.
13. **Appendix 1**

Appendix 1 includes a series of infographics2 published by the UK National Cyber Security Centre (part of GCHQ). These are freely distributable under the Open Government License3.

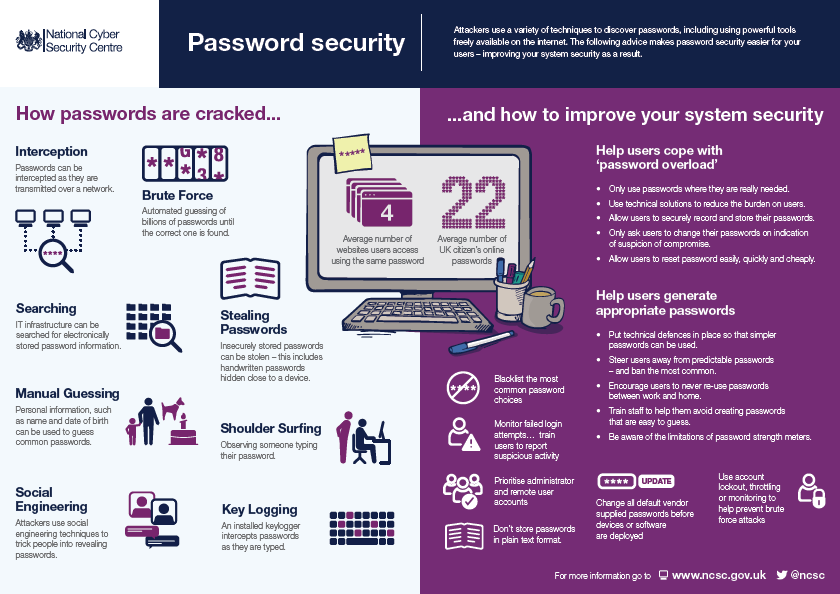
## INFOGRAPHIC 1 - WHAT WE CAN DO TO COMBAT CYBER ATTACKS



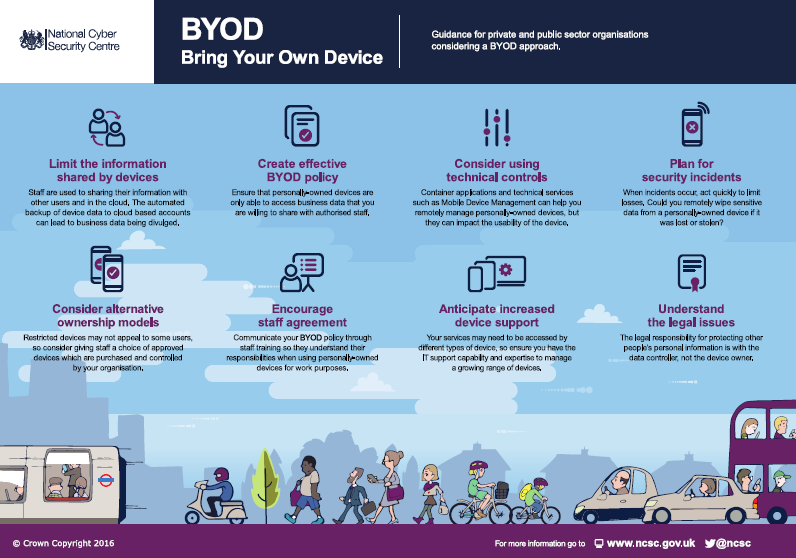
## INFOGRAPHIC 2 - TEN STEPS TO CYBER SECURITY



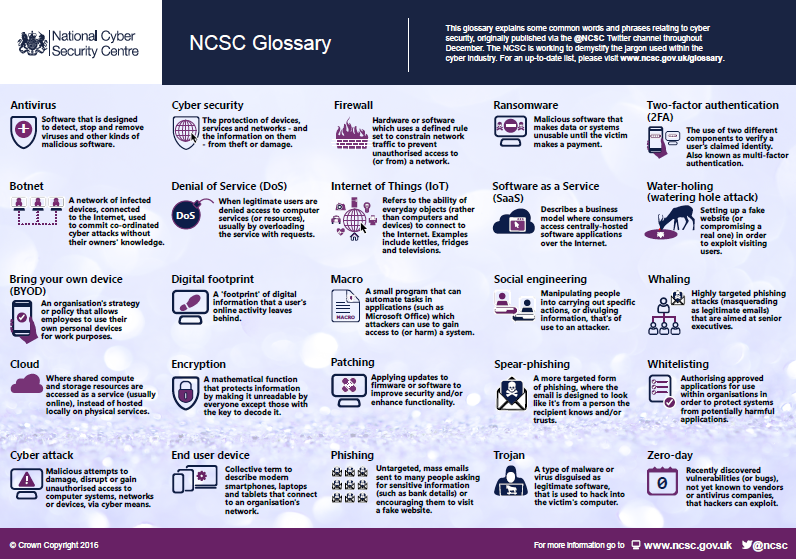
## INFOGRAPHIC 3 - PASSWORD SECURITY



## INFOGRAPHIC 4 – BRING YOUR OWN DEVICE



## INFOGRAPHIC 5 – GLOSSARY OF CYBER TERMINOLOGY



# 

# **Appendix 2 – Bibliography**

* ICT Policies, Security and Data Protection: <http://occweb/intranet/ict-induction-guide/ict-policies-security-and-data-protection>
* IT Security Policy <http://occweb/intranet/documents/it-security-policy>
* Protect Yourself Against Cyber Threats: <http://occweb/intranet/protect-yourself-against-cyber-threats>
* Cyber Security Skills Immediate Impact Fund: <https://www.gov.uk/government/publications/cyber-security-skills-immediate-impact-fund>
* The UK Government National Cyber Security Strategy 2016 – 2021: <https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021>
* NCSC Infographics <https://www.ncsc.gov.uk/information/infographics-ncsc>
* Open Government License <http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/>
* NCSC Cyber Assessment Framework <https://www.ncsc.gov.uk/guidance/nis-directive-cyber-assessment-framework>

**Name and contact details of author:-**

Name: Rocco Labellarte

Job title: Chief Technology and Information Officer

Service Area / Department: Business Improvement

Tel: 01865 25 (2349) e-mail: [rlabellarte@oxford.gov.uk](mailto:%20rlabellarte@oxford.gov.uk)

**List of background papers: None.**