Cheltenham Borough Council

Audit Committee – 12th January 2022

ICT Security Update

Tony Oladejo: ICT Audit and Compliance Manager

John Chorlton: Chief Technology Officer

Accountable member	**Martin Horwood**
Accountable officer	**Tony Oladejo (ICT Security & Compliance Manager) / John Chorlton (Chief Technology Officer)**
Ward(s) affected	**All**
Key/Significant Decision	**No**
Executive summary	To update the Audit Committee on the Cyber Security Action Plan in place, outlining the progress made against millstones to provide assurance that Cyber related risks are being managed and appropriate actions are being undertaken
Recommendations	**That the Report be noted**
Financial implications	***None*** ***Contact officer: paul.Jones@cheltenham.gov.uk***
Legal implications	***None*** **Contact officer: onelegal@tewkesbury.gov.uk**
HR implications (including learning and organisational development)	***None*** **Contact officer: Deborah.bainbridge@publicagroup.uk**
Key risks	Failure to control and secure ICT systems and data against unauthorised access including Cyber-crime attack
Corporate and community plan Implications	**None**
Environmental and climate change implications	**None**
Property/Asset Implications	**None** **Contact officer: Gemma.Bell@cheltenham.gov.uk**

1. Introduction

The ICT Service has responsibility for ICT Security on behalf of the four partner Councils (Cheltenham Borough Council, Cotswold District Council, Forest of Dean District and West Oxfordshire District Council) as well as Publica, Ubico and the Cheltenham Trust.

The ICT Service staff are employed by Publica. The infrastructure and systems they operate are owned by the Councils.

The shared ICT team supports 1500 people, around 300 servers and over 150 application systems.

2020 saw a major Cyber Security ransomware incident at Redcar & Cleveland Council. This was followed up by the Hackney Borough Council incident in 2021. A similar incident is currently being investigated at Gloucester City Council. These high profile incidents along with the international Solarwinds incident in December 2020 has certainly focused the attention of Government, Auditors and more recently Cyber Insurance providers.

During 2021, with the support of the Councils and LGA funding, we have invested in our ICT staff capabilities and Cyber Security systems as well as putting a strategy in place to move towards a Zero Trust architecture. This work is ongoing and summarised within this report.

The experience of others has shown that sadly it is no longer a question of *"if, but when something happens",* which has led to both a change of mindset to Cyber Security as well as the strategies we now employ.

We have an assured, secure, government-accredited security infrastructure that is able to evolve as the organisation changes.

However people and human behaviours remain our greatest risk. Staff awareness around Data Protection and Information Security and good practice when using technology should continue to be mandatory for all employees. ICT needs to double our efforts on staff awareness training during 2022.

2. ICT & Cyber Security Update 2021

2.1 Investment in ICT Staff Training

We have recognised that it is essential to have a team with the right skills and experience and have invested accordingly to assure we do.

Our staff currently hold the following security related qualifications..

1 x BSc (Hons) Forensic Computing and Security
1 x OSCP – Offensive Security Certified Professional (April 2021)
3 x CISSP - Certified Information Systems Security Professional
1 x CCSP - Certified Cloud Security Professional

We have staff currently studying for

1 x CISM - Certified Information Security Manager
1 x CCSP - Certified Cloud Security Professional
1 x OSEP – Offensive Security Experienced Penetration Tester
1 x OSWE – Offensive Security Web Expert

It should be noted that the professional qualifications, for example CISSP, CISM and CCSP require continuous professional education to maintain the certification, therefore ensuring the team to stay current with the latest developments.

2.2 Additional Ransomware Protection introduced during 2021

Highly secure storage is now in place protecting all on-premise data. This system keeps immutable backups for the previous 30 days that the ICT team cannot delete without raising a support case with a 3rd party and providing multiple forms of verification. This, in the event of a ransom attack, should help protect the data from the malicious actors and allow the Councils to roll back to a point in time when the data being held ransom is accessible.

This won't protect us from a ransomware attack and we will still experience downtime. However it should minimise the amount of time it takes to recover once the root cause has been identified and eradicated from the infrastructure.

2.3 Security Information and Event Management (SIEM) introduced during 2021

During the Solarwinds incident in December 2020, our investigations were significantly delayed waiting on a 3rd party to provide log data. In that case, data from the PDNS (Protective Domain Name Service) system run by the The National Cyber Security Centre (NCSC). At the time, this was not a comfortable position to be in. This, along with reviewing the learning points from other major Council Cyber incidents has led to the deployment of a SIEM system.

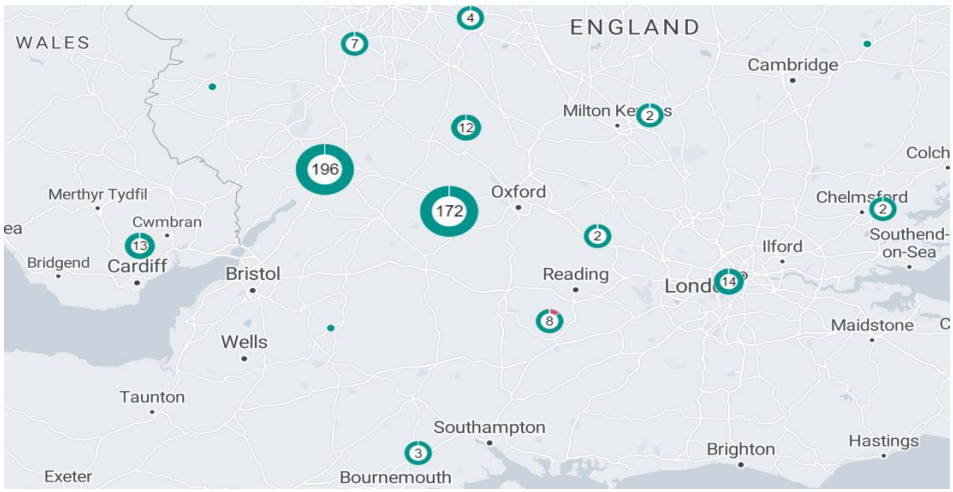
We now collect over 40 million log events every day and retain those logs for 13 months. We expect the logs reviewed to increase to 60 million a day as we enable more of our systems to pass data to the SIEM system.

Obviously a member of staff is unable to review 60 million events a day, so the platform uses Machine Learning / AI to identify threats and trends and alert accordingly.

The 40 million events each day turns into an average of 30 incidents. A typical incident is unusual behaviour. For example, a member of staff in Planning attempting a connection to a Council Tax system in a different Council.

The SIEM gives us insights to how and where our systems and devices are used. The diagram shows the location of Council laptops (from all 4 Council) that are remote to our offices. This image was taken on the 11th November 2021.

On the same day the SIEM system identified a Council employee working from Spain. When this happens, the ICT Team follows up to ensure the arrangement has been agreed by management before taking any action.



More interesting incidents are logon attempts against our Cloud Services by unknown 3rd parties. These are usually focused around senior Council Employees and Councillors with high profiles on Council websites and social media channels. As you would imagine the domain cheltenham.gov.uk is a particular target of interest.

The SIEM system allows us to collect all the security data for an incident into one place and understand the nature and vectors of the cyber threat.

In extreme cases, our system has the ability to isolate users and devices automatically.

The system has additional detection capabilities which can be explored further in a confidential cyber security briefing.

In the event of a catastrophic Cyber Attack, the SIEM is our first port of call for investigation. The system is hosted externally to our offices allowing us to understand what has happened before bringing internal systems back online.

2.4 MITRE ATT&CK framework mapping

MITRE ATT&CK is an open framework and knowledge base of adversary tactics and techniques based on real world observations. It describes the steps or tactics a hacker has to overcome to be successful with details on how each step could be achieved.

ICT are working on cross referencing the framework with the preventative measures we have in place, which will allow us to focus future security enhancements on areas where we have less protection.

We hope to be able to share this confidential information with Audit Committees during 2022 to give a visual representation of what our capabilities are and any areas of weakness that need to be addressed.

2.5 User Training & Education

Our continual approach is to mitigate Cyber security risk by educating our employees and users about safe data practices and constantly reinforcing this with training and ongoing communication messages.

All Cheltenham staff were, in October, issued with Cyber Security training via the Learning Portal.

The learning and development team will be rolling out additional online training for all staff throughout the year.

2.6 Data Loss through Shadow ICT

Shadow ICT through the use of unauthorised cloud based software continues to be a significant risk. Whilst guidance is in place for staff to use supported authorised Council systems, the nature of the Internet allows an end user to sign up and populate a cloud based application within minutes.

Thankfully this is not common in highly sensitive areas such as Finance & Revenues/Benefits.

Training and guidance will continue to be provided to reduce this risk.

2.7 Log4J Vulnerability

Almost exactly 12 months after the Solarwinds incident reported previously to the Audit Committee, the world was introduced to the log4j vulnerability. Log4j is a Java software component used by programmers around the world to add logging capabilities to their systems. It is used by most companies, from Apple through to Zoom. On 10th/11th December it became public that this component had a vulnerability which had gone undetected for up to 10 years. To trigger the vulnerability all you needed to do was get a particular string of characters into the logging system of the software that used the component. This could be via something as simple as using the characters as the username you use to login to the system. The logging system component would then create a connection with the hacker's computer. This is very easy to do and there are multiple videos available online showing you how to do it.

As you can imagine this has caused world wide panic within the tech community, vendors, companies & Government. To further complicate things, the initial “patch” to resolve the issue had additional vulnerabilities.

On 11th December our security systems were updated to monitor and specifically block attacks related to log4j. The ICT Cyber team spent the weekend learning how the vulnerability was triggered and recreated it.

Our internal systems have been tuned and focused to look for the vulnerability. Since the 13th of December, ICT has been scanning our entire infrastructure looking for software that uses log4j. We have also contacted our vendors for a position statement. At the time of writing (31st December) we have upgraded or removed all instances with 2 exceptions. The remaining instances are protected using additional network segmentation and, when the vendors release patches, will be patched immediately. Our Cyber Security visibility systems are being modified and enhanced to detect future vulnerabilities similar to log4j. This work should be completed in the first two weeks of January.

In total we detected and mitigated over 30 different installations of software containing log4j. We have no evidence that suggests this vulnerability has been used against us.

One particular problem is that future upgrades could reintroduce the vulnerability so we are going to have to remain vigilant. Currently new software solutions purchased by the Councils are evaluated, from a Cyber Security point of view, on their infrastructure components, location of data and the connectivity they need to other systems and the Internet. In the future we are going to need to evaluate the software components used in the development of the system.

2.8 Cyber Response to Gloucester City Council

On Tuesday 21st December, Cheltenham BC were notified that Gloucester City Council were infiltrated and a ransomware encryption attempt was made over the weekend of 18th/19th December. On the 20th, Gloucester City shutdown all their internal systems.

On Tuesday 21st December, the ICT put email quarantine procedures in place. All emails received from @gloucester.gov.uk were held pending a manual check by ICT staff. Simple emails, e.g. meeting requests, meeting cancellations etc were allowed through quickly. Emails with attachments and other non-text content were checked thoroughly before being allowed.

At the time of writing, 31st December, Gloucester City was still offline and is working with the NCSC & NCA to understand what happened and restore their systems.

3. Summary of ICT Security & Data Protection Risks & Mitigation

Risk	**Risk Scores (after mitigation)**	**Mitigation**
Reputation damaged due to successful Cyber Attack against Councils	**(I) 4 x (L) 3 = 12**	ICT Staff Training BCP & DR Plans Ensuring Council Leaders are aware of the risks.
Loss of ICT staff with Security Skills	**(I) 4 x (L) 3 = 12**	Flexible contracts ICT Staff Training
Data loss through user error	**(I) 4 x (L) 3 = 12**	Back up program BCP & DR Plans Incident mgt procedures
Supply Chain attacks – Especially in light of Solarwinds	**(I) 3 x (L) 3 = 9**	Reduce lateral movement across the network through the use of SIEM and

		segmentation.
Ransomware attacks – Hackney & Redcar Councils recent cyber incidents	**(I) 4 x (L) 3 = 12**	Immutable Storage, Network segmentation, Backup & DR processes.
Unsupported out of date Software applications	**(I) 4 x (L) 3 = 12**	Regular scanning to identify and remove the software. PSN Certification process forces the removal.
Shadow ICT - sensitive data in Cloud applications without security	**(I) 3 x (L) 3 = 9**	Staff training & clear guidance
Phishing Emails / Spam	**(I) 3 x (L) 3 = 9**	Awareness & training Existing anti-malware solutions which block the outbound connections. Additional capabilities are coming in April 2022 with Microsoft 365.

4 Looking forward - Plans & Challenges for 2022

4.1 Migration to Microsoft 365 from on-premise Exchange.

The move to Microsoft 365, enhancing collaboration opportunities with 3rd parties and maintaining our levels of security is going to be a security challenge. Learning from other organisations shows this can easily go out of control. We are aware we need to proceed with caution.

4.2 Deployment of additional micro segmentation

Micro segmentation allows us to control network traffic between different parts of the network. During 2022 we will be replacing our current micro segmentation product, vmware NSX with a solution to help us bridge the gap between on-premise servers and cloud hosted servers. Once this work is complete we will be able to evaluate options to move more of our computing and storage to the Cloud.

4.3 Cyber Security Insurance

It is clear the insurance industry is reacting to the increased number of Cyber Security incidents. Whilst the Councils have managed to obtain insurance this year, it can not be counted on for future years. During the Cyber Insurance renewal process in November we learnt how the Cyber Insurance industry

measures Cyber risk and we will be modifying our internal systems and configurations to better fit the industry requirements whilst maintaining high levels of security.

4.4 Continue on Zero Trust journey

We will continue to move towards a ‘Zero Trust’ approach to our security architecture as championed and used by the NCSC, GCHQ and other similar organisations. This is achieved by building trust into the user's identity, and the services they access rather than the networks and devices they connect with.

Given the age of some of the Council's core systems, this will take some time. Each new system procured will be required to support our Zero Trust ambitions.

4.5 Begin using internal Multi Factor Authentication

Whilst multi factor authentication is enforced for all devices external to our network, we will begin enabling multi factor authentication for users within our network perimeters during 2022/23. This will help us on our journey towards zero trust.

4.7 Introduction of Cheltenham Online Customer Platform

The introduction of the new Online Customer Platform at Cheltenham will be the first time Cheltenham Borough Council deploys a complex system that integrates internal systems with an online presence. All current online solutions are currently hosted and managed by the Council. This is an exciting development as Cheltenham moves towards the Cloud and the benefits this can bring, not to mention the benefits to the residents.

However, tight integration between a system hosted externally by a 3rd party and our core application systems introduced additional security challenges that need to be managed carefully. During the project implementation we will be adapting our security solutions to operate in this new climate and deploy additional monitoring.

5 Conclusion

As the risks from cyber-attack and data loss increase, the importance of having well trained staff, robust procedures and innovative solutions in place has never been greater.

The investment made to date in both staff and systems puts the Shared ICT team and the Councils it supports in a strong position, however we can’t get complacent.

Ongoing investment is essential as is ensuring that everyone plays their part in ICT security and data protection. We will continue to learn from the experiences of others and work closely with both our suppliers and key Government agencies to safeguard the services provided from disruption.

Appendix 1: Summary of specific Cyber activities in 2021

Jan 21 to Mar 21	Deployment of a new ICT monitoring tool to replace Solarwinds Liaise with procurement to add additional steps into the procurement process.	**Completed**
Apr 21 to Jun 21	Internal Audit - Malware/Anti-Virus Audit & Disaster Recovery Audits Commence Pre-PSN/Cyber Essentials Plus technical control review before recertification.	**Completed**
Jul 21 to Sept 21	Internal /Penetration Scan work commences for annual 2021 PSN submission (Delayed due to COVID and enhanced to cover new COVID deployments). External PSN audit commenced. SIEM Solution is deployed pulling together and combining all security data sources.	**Completed**
Oct 21 to Dec 21	Review PSN scan findings and mitigating any risks found where appropriate. Submit PSN Code of Connection to Cabinet Office. Continue to spread awareness of Cyber Security to staff through awareness and putting more regular information/blog posts on the portal.	**Completed**