Herefordshire Council

Title of report: ICT business continuity, resilience and disaster recovery

Meeting: Audit and Governance Committee

Meeting date: 12 October 2022

Report by: Interim ICT Client Lead

Classification

Open

Decision type

This is not an executive decision

Wards affected

(All Wards)

Purpose

To provide further general information relevant to the committee's wish to 'explore issues around Disaster Recovery and related risks in greater depth' and to 'consider matters in relation to ICT business continuity and cyber security resilience'.

Recommendation

That:

a) The Committee notes the current assessment of the status in all matters of scope noted above.

Key considerations

1. The committee has previously discussed the current state of concern for the ICT industry about the prevalence of cyber attacks, most prominently ransomware where systems are encrypted and access denied until a ransom is paid. This applies to private companies and governmental organisations alike and there have been several notable attacks within the local government sector resulting in severe impacts on services to communities. The threat level is high and has been exacerbated by international tensions as many attacks are thought to be the work of hostile foreign states (aimed at destabilisation) as well as criminal groups (aimed at monetary gain). All organisations will be under some form of attack on a daily basis and the primary defence is to make systems difficult to attack and govern system user behaviour.

2. The council's ICT is run by Hoople Ltd on a platform which is mostly shared with other public sector customers. In July 2022 the council engaged an Interim Client Services Lead to carry out a review of arrangements and determine a technology strategy for the future. This work is underway and scheduled to complete by the end of December 2022. Some of the work referred to in this report was not undertaken by the author of this paper but by a predecessor and is believed to be correct.

3. The request by the committee covers outstanding audit recommendations and several related general areas of ICT operations. Therefore the report covers the following content:

   a. The response to previous Internal Audit Recommendations;

   b. Resilience – how resistant is the ICT infrastructure to any loss?

   c. Business Continuity – how well can ICT continue to deliver technology services after the impact of an event?

   d. Disaster Recovery – how quickly and completely could ICT recover after a disastrous event?

   These above areas are covered in sequence in the following content.

Internal Audit Recommendations

4. The Internal Audit service (SWAP) reported on 22 April 2022 on Audit Plan Progress. There were at that stage two Priority 2 findings relevant to ICT under the heading of Disaster Recovery (page 8). The findings were as follows with response in italic font:

   a) Finding 1 - Business Continuity – by 30 June 2022

   - The council must ensure all critical services and supporting systems identified as part of its recent review of business continuity (BC) arrangements are detailed on the council's Application Masters List. The priority of all systems listed should detail their priority for recovery and hence provide a link to the Service Level Agreement (SLA) with Hoople Ltd.

     Following the audit, the application master list was updated with a prioritisation 1 and 2 indicator. This resulted in 17 Priority 1 systems, 28 Priority 2 systems and 105 others. The ICT Client Lead has viewed the list and is content that these generally align with the usual priorities for a Unitary Council. COMPLETE.

   - The back-up requirements for all systems identified on this list as processing sensitive data should also be confirmed and updated as necessary. For those systems that do require back up but where it was unclear if they were managed by Hoople Ltd (and therefore potentially not covered by the SLA), management need to obtain assurance that back up and restoration services will meet the council's system recovery requirements.

     The requirement for inclusion on the backup schedule was reviewed within the same application master list document and therefore this is considered to be up to date. Specific assurances for systems not managed by Hoople have not been sought from suppliers (as far as is known) although the note below on system procurement is relevant here. There is one significant 'system' managed by Hoople, Office 365/Teams, which has been partly licensed and adopted but not fully commissioned into the current infrastructure. It therefore has an interim back up solution which was proposed and implemented by Hoople in June 2022 but for which there are still some outstanding concerns about its robustness as this is usually an entirely Cloud based

infrastructure using the Microsoft platform. Office 365/Teams and the configuration are being re-considered as part of work towards an ICT Strategy and therefore this solution is thought to be acceptable for a limited period, to be reconsidered as part of planned Audit work in Autumn 2022 and in any event before the end of 2022.
PARTLY COMPLETE

- In future all software procurement whether through Hoople Ltd or independent of Hoople Ltd should be supported by clear back-up and recovery contractual terms. For existing systems where these terms are unclear the contact terms will be reviewed at renewal.

  Hoople have stated that they always consider DR and BCP considerations as part of their proposals and procurement and this is evidenced within the supplier assessment questionnaires used during the initiation and procurement stages. COMPLETE

b) Finding 2 - Disaster Recovery – by 30 September 2022

- The above Priority 2 action was agreed to establish whether the backup and restoration arrangements (as detailed in the SLA with Hoople) adequately supported the BC requirements of all Hoople in-scope applications"

  This was agreed verbally with no changes proposed by a previous Interim incumbent. There does not appear to be any pressing need to revisit this. COMPLETE

- Confirm the adequacy of Disaster Recovery (DR) testing to demonstrate compliance against the SLA recovery (priority) targets, for all systems with due regard to the critical services identified.

  See below

- With Hoople, undertake scenario-based test situations to inform current DR planning to reference the loss of all applications, loss of all Hoople supported services at all clients etc.

  Hoople conducts internal scheduled BCP exercises on a variety of scenarios as part of our ISMS for ISO27001 compliance, these are recorded on our compliance schedule. However there have not been any exercises conducted alongside the Council, aside from the cyber exercise of the Local Resilience Forum for the regional Tactical Response Group last December, which involved several major regional providers. Therefore the recommendation has not been met and specific systems have not been recovered against SLA targets. INCOMPLETE – the proposal is to complete this work in Q4 of 2022

- For any system that is not covered by the SLA, confirm the adequacy of their DR arrangements including the testing for critical and non-critical services.

  This work is not started as far as is known. It will require liaison and agreement with a range of suppliers assuming that this requirement is part of the contract that the Council holds (it may not be covered in some older contracts). INCOMPLETE – the proposal is to complete this work by end March 2023.

- Confirm the adequacy of DR decision making processes for those systems that are not supported by Hoople. Options include scenario-based planning/tabletop DR exercises for management. Such scenarios could reference the potential loss of the system itself, supporting hardware and so on.

Current testing and completion of a compliance log is carried out at points of major change and upgrade milestones. This may include the definition above of system loss and underlying hardware depending on the Hoople and system supplier roles. It cannot be stated that this covers all systems not supported by Hoople and it may also be worth considering these actions follow a defined schedule rather than at points of major change. PARTLY COMPLETE – proposal to review this as part of Audit work commencing in September 2022 to further define the objective and add assurance evidence where this is present.

Resilience

5. The resilience of ICT is the first stage in preventing loss of systems or data. It concerns the systems ability to withstand or recover from any shocks or events and still maintain service. This does include security but also includes concepts like redundancy where loss or failure of part of a system is immediately taken up by another component – for instance in the event of a power loss the Hoople datacentres have Uninterruptible Power Supply (UPS) that can sustain operations for a period of around 4 hours and a generator as back up. There are two main datacentres with separate routing of linkages into them. Many networking components are paired and can operate on one alone. Failover between components can be seamless and automated or manual with likely short periods of outage.

6. Resilience also has a relationship to capacity management where components are sized to meet exceptional demand and often function well below maximum for most of the time.

7. These features are built into the ICT infrastructure at design and managed throughout the lifecycle of components.

8. Resilience is also relevant to system defences. These are a key part of resisting cyber attack through technology such as Firewalls or Filters which aim to insulate the council network and users from attack. Every day malicious attacks are made on most ICT networks, filters identify suspicious content, for instance they may block some websites known to be risky or e-mail from risky sources. The software is updated very frequently, usually by suppliers and the council can also add blocks (or unblock) manually. Firewalls prevent the spread of any issues and there are often several layers.

Business Continuity

9. Hoople Ltd have provided the Interim Client Lead with a 15 page Business Continuity Plan. The document is up to date and contains all reasonable expected content of such a plan; invocation criteria, roles, process, objectives, communications, resources etc. This is a detailed operational document but it has been reviewed and approved by expert council client side scrutiny and therefore does not require escalation to this committee.

Disaster Recovery

10. In the paragraphs above note has been made of ICT resilience to avoid a disaster but planning does of course need to exist for the scenario where a disaster does happen and needs to be recovered.

11. Widespread and damaging disasters usually relate to the wholesale loss of systems or data say through fire, flood, error or, more commonly recently, cyber attack. It is important to have alternative computing hardware and facilities (such as the primary and secondary datacentre that Hoople operates) and access to a good set of data – both configuration and system data. The main means of having the access to data is by a backup where data is copied, either in real time, at intervals or say overnight and held securely. There are tiers of back up, related to system priorities, and data is first replicated to the secondary datacentre at suitable intervals and then a tape backup is taken. Tape backup is less common in recent years, options being

Cloud or third disk backup however it does give the advantage of being completely physically separated when taken and then stored securely.

12. However recovery from tape does take longer than from disk and can be problematic (as can any restore onto 'bare tin' – an unprepared server). This should be tested completely at intervals (see Audit Recommendation response in para 4b above).

General comments and currently planned work

13. The above responses are very specific to technology aspects of the areas identified by the committee. However there are other factors which significantly affect risk, the primary one for information security is human error where users might click on a link in an e-mail without considering its trustworthiness or unwittingly surrender user credentials allowing others to gain system access. These scenarios are still the most likely routes of cyber attack and the reason why the council runs simulated phishing attacks to try and educate users towards a zero trust approach.

14. There are hundreds of various scenarios and permutations of risks for system loss. Not all of these can be calculated or predicted – the exact scenario is usually unique. For instance the council may plan for loss of a building due to fire, loss of personnel due to pandemic and loss of systems due to cyber attack or component failure but these might all occur at once or more simply components which fail might be in short global supply but these are hard to plan for and might be well beyond the resources of a local council to address. It is therefore always hard to give categorical assurances about risk and likely recovery and impossible for every scenario.

15. Whilst the vast majority of ICT systems are provided to the council under its arrangements with Hoople Ltd neither the council nor Hoople are in complete control of all aspects of systems and are dependent on suppliers fulfilling their obligations and acting properly. For instance there have been widespread attacks on internet service providers which impact all ICT users as connectivity can be compromised or lost. There are also, and increasingly, a number of suppliers of 'hosted' systems which are run on their infrastructure and to which the council simply connect. They are completely responsible for safeguarding our data and reliability of system access (within the parameters the council specify when the council contract).

16. The assignment for the Interim ICT Client Lead has been noted earlier. This includes an assessment of current issues and risks and a plan to respond. The resulting work will include many aspects noted in this report such as the resilience of the ICT infrastructure and options for further technology investment which can reduce risks if this is thought to be sensible and cost effective. The planned work will include addressing any outstanding issues from Internal Audit work and the Interim ICT Client Lead has agreed a refreshed plan with SWAP for immediate further assurance work to start in September 2022.

Community impact

17. There are no immediate issues of Community Impact other than to note that loss of ICT systems would severely curtail the ability of the council to plan and deliver current services as virtually all aspects of service are underpinned by ICT systems. This is likely to grow more important as the council continues to modernise and increase digital services and ICT is already a crucial component for the internal work of the council including productivity in flexible working as has been adopted post COVID pandemic.

Environmental impact

18. There are no immediate environmental aspects to note. However it is an aspect which is important to address when planning future ICT infrastructure especially. For instance datacentres consume a lot of power for operation and cooling and it is possible to reduce this as the council plans into the future.

19. A positive aspect of increased digitisation is the reduction of paper and paper waste which can result in CO2 and cost avoidance.

20. The council takes care to ethically dispose of redundant ICT equipment in a way which ensures as much re-use as possible and to minimise waste. Disposal regulations apply here and these are adhered to via engagement of suitable contractors.

Equality duty

21. There are no immediate impacts or concerns for the Council's Equality duty. This is a factual report and there are no matters in this regard.

Resource implications

22. There are no resource implications arising from this report. Planned work is already budgeted for and underway.

Legal implications

23. This report is provided for information purposes and therefore there are no legal implications arising from the report.

Risk management

24. The entirety of this report is relevant to risk management and risk management is undertaken by Hoople Ltd covering these areas (the current Risk log has been inspected by the Interim ICT Client Lead and is satisfactory). There is no new content which suggests current risk levels should be changed. There is work underway which will reduce risk levels (Audit responses and review of ICT by Client Lead) but set against that is the increased recent threat level, especially in respect of cyber security. Therefore no change is recommended.

Consultees

25. No consultation has been undertaken for this report.

Appendices

None

Background papers

'Report of Internal Audit Activity - 2021/22 Plan Progress - as of 21st April 2022' - South West Audit Partnership (Herefordshire Council Internal Auditors) Link to report: Contents (herefordshire.gov.uk)