Tyne and Wear Fire
and Rescue Authority

TYNE AND WEAR FIRE AND RESCUE AUTHORITY Item No 10

MEETING: GOVERNANCE COMMITTEE

SUBJECT: CYBER RESILIENCE UPDATE

JOINT REPORT OF THE CHIEF FIRE OFFICER/CHIEF EXECUTIVE (THE CLERK TO THE AUTHORITY) THE FINANCE DIRECTOR AND THE PERSONNEL ADVISOR TO THE AUTHORITY

1 INTRODUCTION

1.1 The purpose of this paper is update Governance Committee on Cyber Resilience arrangements within Tyne and Wear Fire and Rescue Service (TWFRS) for 2023/24 (year to date).

2 BACKGROUND

2.1 Cyber resilience is a strategic approach to enable an organisation to maintain critical functions, limit the impact of cyber disruptions, and ensure rapid re-establishment of normal operations following a cyber incident.

2.2 Currently TWFRS has a variety of different systems (both corporate and control room) that need to be safeguarded, the majority of which are predominately hosted onsite. The Service has a limited number of cloud hosted services, with the most common being Office 365. These are also safeguarded, and there are a variety of controls in place.

3 CYBER SERCURITY ARRANGEMENTS AND PERFORMANCE

3.1 All TWFRS ICT policies and procedures are up to date and reflect the appropriate measures required to ensure staff understand what is required to safeguard themselves and the Service systems. Policies and procedures include Information Security, Acceptable Use, Cyber Security, and Change Control.

3.2 TWFRS Control Room systems are managed by the prime contractor, and are subject to ensuring security compliance in order to maintain connection to the Emergency Services communications network via a Code of Connection issued by the Home Office.

3.3 The following, whilst not an exhaustive list, show the types of controls and monitoring mechanisms TWFRS has in place to ensure the Service can maintain an overall good security posture:

3.3.1 Office 365 and Email security – currently the Service only allows traffic and communications from "known" verified organisations. As a result, TWFRS have one of the highest C-TAG email security scores of all the public sector organisations in the North East. We are one of only three fire services in the UK to achieve 'epic' rating. Additionally, data is Geo-fenced (UK only) to prevent foreign attack vectors from trying to access our systems (all non-UK traffic is automatically dropped).

3.3.2 Onsite security – The Service has many physical and logical controls in place to prevent unauthorised access to on-premises systems such as door access controls, CCTV cameras, alarms, user access controls etc. Both physical and logical access controls have associated audit logs and records.

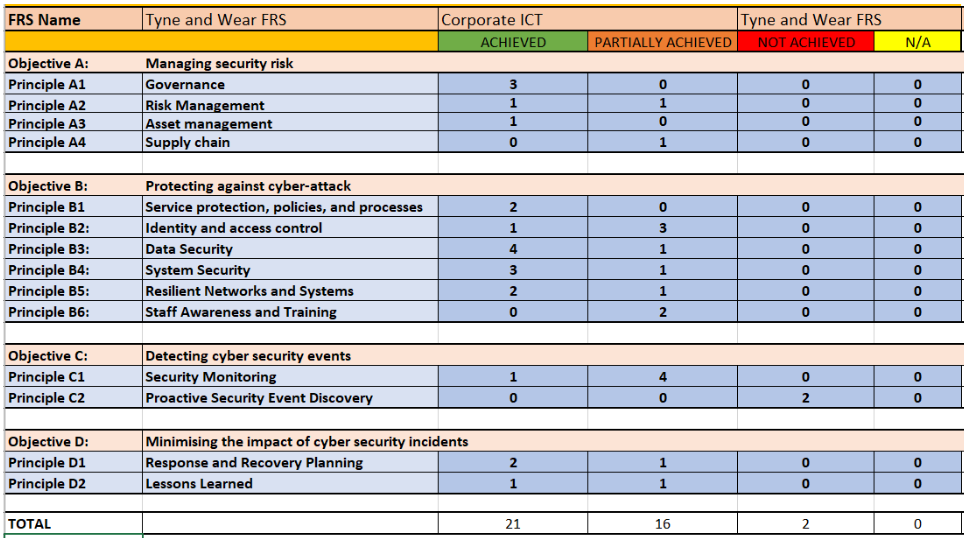
3.3.3 The Service operates as per industry best practice in terms of providing systems and infrastructure resilience along with backups and storage. All systems have dual power, diverse routes, and the Service operates a complete disaster recovery architecture by adopting a replica datacentre at a separate location, of which all corporate systems replicate on a daily basis. Additionally all backups and stored to disk initially then recorded to multiple tape libraries and then stored in fire proof secure safes at opposite sites.

3.3.4 The ICT Department keep a record the number of cyber related incidents (within department local indicators). To date for 2023/24, there have been zero known cyber-attack attempts, and zero subsequent incidents to report. There have been 164 phishing emails, none of which have resulted in a cyber incident.

3.3.5 Frequent cyber test simulations and table top exercises are carried out by the ICT Department to ensure that the team are familiar with, and practiced in, the Cyber Incident Response process in the event that that it is ever required. Additionally this helps to ensure the process is refined and suitable for the Service. Additionally, the Service has been working to raise awareness across the organisation by educating staff on safe practices and the value of ensuring technology is used in a safe manner.

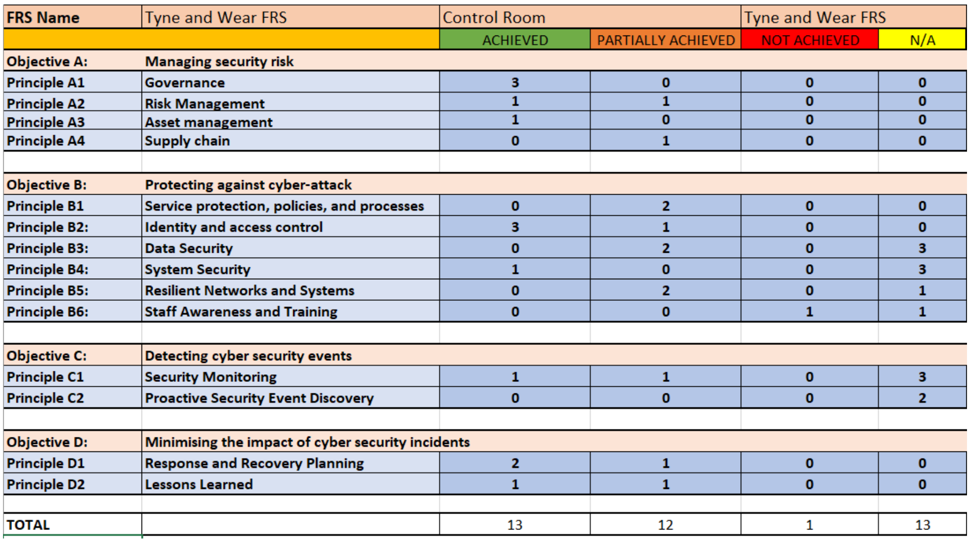
3.4 In 2023, the National Fire Chief's Council (NFCC) commissioned IBM to complete a Cyber Assessment within various fire and rescue services. In April 2023, TWFRS undertook this process. The audit looked at the measures and controls that were in place and was able to offer areas for improvement as a result of the audit. The corporate and control room systems were audited separately. The main areas for improvement were focused on improving staff awareness and needing a more proactive monitoring and detection tool to support the Service. The results can be seen below:

3.4.1 Corporate ICT results:



FRS Name	Tyne and Wear FRS	Corporate ICT		Tyne and Wear FRS	
		ACHIEVED	PARTIALLY ACHIEVED	NOT ACHIEVED	N/A
Objective A:	**Managing security risk**				
Principle A1	**Governance**	3	0	0	0
Principle A2	**Risk Management**	1	1	0	0
Principle A3	**Asset management**	1	0	0	0
Principle A4	**Supply chain**	0	1	0	0
Objective B:	**Protecting against cyber-attack**				
Principle B1	**Service protection, policies, and processes**	2	0	0	0
Principle B2:	**Identity and access control**	1	3	0	0
Principle B3:	**Data Security**	4	1	0	0
Principle B4:	**System Security**	3	1	0	0
Principle B5:	**Resilient Networks and Systems**	2	1	0	0
Principle B6:	**Staff Awareness and Training**	0	2	0	0
Objective C:	**Detecting cyber security events**				
Principle C1	**Security Monitoring**	1	4	0	0
Principle C2	**Proactive Security Event Discovery**	0	0	2	0
Objective D:	**Minimising the impact of cyber security incidents**				
Principle D1	**Response and Recovery Planning**	2	1	0	0
Principle D2	**Lessons Learned**	1	1	0	0
TOTAL		21	16	2	0

3.4.2 Control Room ICT results:



FRS Name	Tyne and Wear FRS	Control Room		Tyne and Wear FRS	
		ACHIEVED	PARTIALLY ACHIEVED	NOT ACHIEVED	N/A
Objective A:	**Managing security risk**				
Principle A1	**Governance**	3	0	0	0
Principle A2	**Risk Management**	1	1	0	0
Principle A3	**Asset management**	1	0	0	0
Principle A4	**Supply chain**	0	1	0	0
Objective B:	**Protecting against cyber-attack**				
Principle B1	**Service protection, policies, and processes**	0	2	0	0
Principle B2:	**Identity and access control**	3	1	0	0
Principle B3:	**Data Security**	0	2	0	3
Principle B4:	**System Security**	1	0	0	3
Principle B5:	**Resilient Networks and Systems**	0	2	0	1
Principle B6:	**Staff Awareness and Training**	0	0	1	1
Objective C:	**Detecting cyber security events**				
Principle C1	**Security Monitoring**	1	1	0	3
Principle C2	**Proactive Security Event Discovery**	0	0	0	2
Objective D:	**Minimising the impact of cyber security incidents**				
Principle D1	**Response and Recovery Planning**	2	1	0	0
Principle D2	**Lessons Learned**	1	1	0	0
TOTAL		13	12	1	13

3.5 As part of the Service's commitment to working towards Cyber Essentials, annual ICT security audits are carried out and these reports help the Service obtain the Airwave Code of Connection from the Home Office.

3.6 Future focus in this area include addressing the areas for improvement from the IBM audit by adopting new proactive systems such as SIEM and IDS. Additionally ensuring dedicated roles and responsibilities within the ICT Department to support achieving and maintaining Cyber Essentials.

4 BENEFITS

4.1 The key benefits of a Cyber Resilient approach are:

- Presents a strategic approach to organisational resilience;
- Increased ability to limit the impact of cyber disruptions;

- Enhanced ability to maintain critical functions;
- Rapid re-establishment of normal operations following a cyber incident;
- Supports core characteristics of good business continuity and organisational responsibility.

5 RISK MANAGEMENT

5.1 The risk of cyber attack or cyber disruption is ever present. Along with the ever-changing landscape with Digital and Data, the threats will continue to evolve and as our reliance on technology increases the impact will likely increase as a result.

5.2 The Service's robust approach to cyber resilience helps continue to mitigate risks and the potential impact, as far as possible within acceptable tolerances.

5.3 As the cyber landscape continues to change, we will be ready to adopt these changes to ensure the safety of the Service and our communities.

6 FINANCIAL IMPLICATIONS

6.1 There are no financial implications in respect of this report.

7 EQUALITY AND FAIRNESS IMPLICATIONS

7.1 There are no equality and fairness implications in respect of this report.

8 HEALTH AND SAFETY IMPLICATIONS

8.1 There are no health and safety implications in respect of this report.

9 RECOMMENDATIONS

9.1 Members are recommended to:

a) Note the contents of this report
b) Receive further reports as appropriate.

BACKGROUND PAPERS

N/A