Agenda item: 15

Warwickshire Joint Audit and Standards Committee Report Summary

Meeting Date: 23rd January. 2024

Subject: Cyber Security

Contact details: Stephen Russell

Purpose of the Report:

The purpose of this report is to provide JASC with an update on the activity and priorities across Cyber Security to enable assurance that this is an area that is being appropriately managed.

Recommendation:

It is recommended that JASC comment and note the contents of this report

Background:

Cyber Security is a critical function and activity for Warwickshire in ensuring that Warwickshire Police's IT systems, services, and underlying technology are "secure by design" ensuring that IT systems have the appropriate level of security, confidentiality, integrity and availability.

Within the remit of governance, risk and control JASC will review from time to time the effectiveness of selected governance and assurance arrangements. Cyber Security has been selected as one of these areas for a 'deep dive' review

Executive summary

The report introduces the role and function of Cyber Security in terms of structure, roles and responsibilities. The report identifies the key national requirements we are required to achieve and our assessed level of performance and sets out key priorities and areas of focus for the coming year and how we will approach achieving this.

Introduction to the Cyber security Team

The cyber security team at Warwickshire Police sits within the architecture practice of Digital Services. The team consists of one Cyber Security Architect and one Cyber Security Engineer who work closely with the rest of Digital Services, Information Assurance, and the Change team within Warwickshire. This is a newly formed in-house team replacing the capability that was previously supplied through contractors during the Evolve project.

The team has representation at Digital Services senior leadership level, presents to the Information Assurance Board, attends local resilience forum meetings with third party agencies and sit on the national cyber standards and policy board to help shape cyber security at a national level.

In terms of training the Cyber Security Architect holds a master's degree in computer science with cyber security, is a ISC2 CISSP (Certified Information Systems Security Professional) and is a Microsoft Certified Security Architect Expert. The Cyber Security Officer is working towards his ISC Certified in Cyber Security qualification. Training in cyber security is an ongoing process and both members of the team continue to attend training and gain both certification and experience.

Part of the role of the cyber security team to provide assurance and guidance for both business-as-usual activities and project-based activity as well as ensuring that Warwickshire police abide to national standards and codes of connection that we are required to as a Police Force. These Codes of Connection are applied to all organisations that access national policing applications and hold police data. This involves ensuring that technical controls and systems, as well as local policies and procedures adhere to the policies, standards and guidance set nationally. Whilst the team does engage with the Cyber-crime unit to share knowledge, the team is an internal function for Warwickshire Police itself and is not involved in crime reporting, other than to report any cyber-criminal activity against the force itself.

We work closely with the Warwickshire change team to ensure that any project delivering large-scale change or new capabilities passes through the correct gates to ensure that it meets the cyber security requirements of the force. Any risk that a new/changed system introduces to the force must be mitigated to an acceptable level (as per the forces risk tolerance) and is signed off at an appropriate level, ranging from Information Asset Owners (IAOs) to the Senior Information Risk Owner (SIRO) who is the force Deputy Chief Constable (DCC).

National Accreditation and Assurance

As a police force, we are required to meet the requirements of various codes of connection, as well as being part of a national scoring system in terms of cyber security and information assurance controls.

Firstly, in the last 6 months Warwickshire have successfully applied for and gained certificates of connection for all required systems, this includes national sign off for Airwave (Police Radios) and the Public Services Network (PSN). This is through assurance of our policies, procedures results/remediation of IT Health checks (more details below).

Secondly, there has been a change in the way that National Policing is assured in terms of information assurance and cyber security. In the past a yearly submission known as the Governance and Information Risk Return (GIRR) was made to the home office and a point-in-time decision was made on the force's adherence to national standards and their

connection to the PSN-P (Public Services Network for Policing). This has now been replaced with a more dynamic mechanism for assuring police forces – this is known as the Security Assessment for Policing or SyAP. This new mechanism provides ongoing assurance, rather than a point-in-time approach, which allows for dynamic changes in a force's "score."

The SyAp is based upon industry best practice and is based upon the US NIST (National Institute of Standards and Technology) Cyber Security Framework[1]. Forces are now scored between 1 and 5 on 110 cyber security and information security controls covering the key areas, as defined by the NIST framework of Identify, Protect, Detect, Respond and Recover. Whilst the Force do not hold ISO27001/ISO270002 the controls in NIST are broadly similar and are what nationally we are obliged to work to.

Over the last 6 months the Warwickshire Cyber Security team, working alongside the Information Assurance team have been working to improve Warwickshire's overall security posture, focussing on areas of the SyAp that the force scored the lowest. In this time the force has achieved an average score of 2.0 across the 110 controls, which is in-line with the national baseline as set by the Home Office, it is also above the national average for police forces.

As a force, we want to exceed baselines and constantly improve our security posture, we are therefore continuing to work on areas where improvement is desired, and we are using the SyAp to assist us with this. The Due to Warwickshire being above the national average, discussions have also been held with Police Digital Services, about us helping other forces to improve their security, to increase the national posture as part of the national "Defend as one" strategy.

IT Infrastructure

Over the last few years, the Warwickshire Police IT infrastructure has been largely rebuilt as the force transitioned out of the Alliance with West Mercia. From a Cyber Security perspective this puts the force in a positive position because it means that a lot of technical debt has been removed leaving the force with a new IT estate.

Many aspects of the Force IT system have been built following the National Enabling Programme, which was ran by Police Digital Services (PDS). As part of this programme blueprints were shared with forces nationally, which followed industry best practices and allowed forces to modernise their IT estate following a set of nationally assured guidelines.

These blueprints covered many areas including:

- End user devices (laptops, desktops)
- Authentication methods i.e., how user's login to Force systems and what controls there are to ensure this is secure.
- Productivity suite controls such as ensuring common applications such as Outlook for email or Teams for communication are securely.
- Monitoring – The force network is monitored 24/7 by the NMC.

Following this blueprint has allowed the Force to rapidly deploy a more modern IT infrastructure for officers and staff.

Work is continuing within Digital Services to continue to improve our underlying IT infrastructure and further improve our security. Two key areas of focus are what is known as "Zero-Trust" and Supply Chain Risk Management.

[1] Cybersecurity Framework | NIST

Firstly, Zero-trust is a well utilised model which has three guiding principles which are verify explicitly, least privilege and assume breach. Warwickshire are looking to use technology and policy to allow us to implement a zero-trust environment within our IT infrastructure, which is designed to transparently (to the user) improve our security posture by ensuring access to police data is only given to the right people, at the right time for the right duration. This will help us reduce the change for malware or suspicious actors to move laterally through the organisations IT infrastructure and reduce the attach surface of the force.

Secondly, we are working with PDS nationally as well as a local offering for a third-party risk management service. In the last 12 months, Force supply chains have been breached, which has been recognised as a risk both to Warwickshire Police but also at a national level. As such the cyber security team is engaged with specialist companies that offer services that help to monitor and assure third parties and allow the force to see what organisations pose the greatest risk to our organisation and allow us to report upon and mitigate this risk. At the same time PDS is looking to procure a similar service to cover the largest suppliers to policing to help monitor and report upon any risks that they pose, to help from a national perspective. A 2-pronged approach is being used here, as the PDS offering will only cover the larger suppliers and to receive a greater level of coverage a local solution is also in the planning cycle.

Any new systems must pass a series of gates including:

- Security Review Group (Lead by Information Assurance, attended by Cyber Security)
- Technical Design Authority (Lead by the architecture practice which includes Cyber Security)
- Change Board (Lead by Digital Services Service management, attended by Cyber Security)
- Transition Board (Lead by Digital Services Service management, attended by Cyber Security)

As part of the transition to live service all systems must be correctly catalogued and accepted into live by our Managed Service Provider (MSP) and service delivery team. Software is recorded and hardware asset tagged.

Cyber Incident Response

In the last 6 months, the cyber security team have developed a new Cyber Incident Response Plan that would be enacted in the case of a cyber security incident affecting the force. This plan has been reviewed and signed off by Police Digital Services from a national level and feedback on it has been positive. This plan will be tested yearly and reported on internally.

In brief, this plan details:

- Roles and Responsibilities
    - This is vital to ensure the correct personnel are involved at the correct time and are fully aware of their remit within the response to an incident.
    - This includes personnel within Digital Services as well as the wider force.
- Communication
    - This includes communication methods as well as alternatives should they be required.
    - Escalation procedures
    - Reporting procedures internally and externally e.g., to National Crime Agency, Information Commissioners Office, NCSC, PDS.

- Response Process
    - Developed based upon NCSC best practice.
    - Split into clearly defined sections including triage, analyse, contain/mitigate, remediation, recover.
- Reporting and Lessons learned.
    - Process to report upon the incident
    - Process for lessons learned & feedback loop to improve plan.

This plan will be tested annually using a range of techniques including read throughs, scenarios and tabletop exercises.

Organisational Security Awareness

A vital part of cyber security is ensuring that users of IT systems are aware of security risks and ensuring a high level of organisation learning. The force has many technical and physical controls in place such as access control on doors, network firewalls and CCTV, these are all very important, however so is the human aspect. The 2023 NCSC Cyber breaches survey[2] showed that 79% of business and 83% of charities in the survey experienced a phishing attack in the last 12 months. In Warwickshire our technical protection block thousands of phishing attempts a year, however some will always slip through, and this is where user awareness is key.

In the last 6 months the cyber security team have implemented the following measures to improve the level of cyber security awareness at Warwickshire:

- Physical Security Awareness
    - A key part of cyber security is physically securing Police sites and equipment.
    - Communications are sent out force wide to ensure that Officers and Staff are aware of physical security such as checking ID badges, not holding doors open, securing windows.
- Phishing Awareness
    - Worked with Corporate Communications to update and rationalise phishing guidance on the forces internal Intranet.
    - Implemented a “Report Message” button that allows users to report a suspicious email with a single click. This deletes the message and sends a copy to Digital Services for investigation. From 22/10 to 23/11 our users reported 113 emails for investigation by our service desk and cyber security team.
    - Implemented a warning displayed on emails sent from senders who have not emailed the user before – this is in addition to a warning showed when receiving an email from an external email address.
- Phishing Simulation
    - Conducted a phishing simulation – This entails the sending of a benign phishing email to force mailboxes.
        - Members of the force who click the dummy links are presented with phishing awareness guidance.
    - Results of the simulation are reported upon and will be used to baseline the force against expected results from similarly sized organisations.

The latest phishing simulation showed that 13% clicked the simulated suspicious link. This is 7% lower than the predicted click rate for similarly sized organisations following Microsoft’s

[2] Cyber security breaches survey 2023 - GOV.UK (www.gov.uk)

analysis of the email template sent out – to be clear, in this case being below the prediction is a good thing as it means less people clicked the suspicious link than Microsoft predicted. As a baseline this is a good result for the force, and will allow us to tailor our Phishing simulations, training, and guidance accordingly over the next 12 months.

Vulnerability Scanning and Penetration Testing

As part of Warwickshire Police's ongoing assurance efforts, both from a local level and from a national compliance level the Cyber Security team work to ensure adequate coverage of our environment in terms of vulnerability awareness.

Each year we are required to undertake an independent IT Health Check (ITHC) on 10% of our IT infrastructure. The purpose of an ITHC as defined by the cabinet office[3] is to provide assurance that the organisations external systems are protected from unauthorised access or change, and they do not provide an unauthorised entry point to the PSN (Public Services Network).

This ITHC forms part of our code of connection for the PSN – which contains national police systems and data that we require to effectively police Warwickshire. Our latest ITHC has been conducted and any vulnerabilities present have been remediated to a level whereby our assessors at the cabinet office are happy that we abide by the code of connection and in September 2023 issued us with our certificate, valid for the next 12 months. Our next ITHC is due to be completed in February 2024 with remediation actions to follow in suitable time to re-submit for a further year in August 2024.

In addition to this mandated ITHC, we also conduct independent ITHCs on areas of change within the organisation. In the last 12 months we have conducted (via independent third party) ITHCs on our newly installed Digital Interview Room solution and our new Child Abuse Image Database (CAID) network.

In terms of internal vulnerability scanning capabilities, we are looking to build upon these working with Police Digital Services (PDS), who, as part of the national cyber security strategy are working with forces to implement a centralised vulnerability scanning capability. This will allow the in-house cyber security team to expand our scanning of our environment for vulnerabilities and remediate them more efficiently. This is scheduled by PDS for Q4 of the 23/24 fiscal year, with implementation in forces following this. The force currently utilises the Microsoft Defender suite of capabilities to identify vulnerabilities within our Microsoft environment and use our secure score to drive improvements.

Cyber Security Intelligence

It is important for Cyber Security teams to keep on-top of the cyber security threat landscape, both from a holistic perspective and from a Policing and national infrastructure perspective.

There are a wide range of threat actors that could attack Warwickshire Police, and these range from those with basic skills and funding to highly skilled and resourceful hackers funded by unfriendly nation states. Each of these pose a unique threat, however a key to defending against all of them is strong basic cyber hygiene.

[3] IT Health Check (ITHC): supporting guidance - GOV.UK (www.gov.uk)

Our Microsoft implementation allows us to utilise a wide range of mature security tools and protections. Some examples of this include the following malicious activities automatically detected and blocked within a single month*:

- 910 Spam emails
- 365 Phishing emails

At Warwickshire, we receive threat intelligence from the National Management Centre (NMC) which is part of the wider Police Digital Services who have key links with the National Crime Agency (NCA). These threat intelligence alerts aid forces to keep abreast of the changing landscape and provide information of threats that may affect the force.

The Cyber Security team regularly act upon this intelligence to ensure that Warwickshire's systems are protected, some examples include:

- Blocking of internet traffic originating from Russia, Ukraine, and Belarus in response to the Russian invasion of Ukraine
- Blocking of specific internet (IP) addresses or email addresses based upon intelligence gathered nationally.
- Patching of critical systems based upon vendor alerts to vulnerabilities.

On top of intelligence from the NMC, members of the Cyber Security team are also members of the CISP[4] (Connect Inform Share Protect) platform where cyber security professionals in the UK can share and collaborate on threat intelligence. The service is owned and managed by the NCSC and is currently in the process of being re-developed onto a new platform allowing even greater collaboration opportunities.

We also liaise with the force Cyber Crime team and the wider Warwickshire Local Resilience Forum as well as regularly keeping up to date on the latest cyber security news and blog posts online. We are currently developing a monthly cyber security report featuring cyber statistics for Warwickshire that will be presented to senior management along with ad-hoc papers that are written in response to specific events.

[4] About CISP - NCSC.GOV.UK

* Statistics related to the period between 22/10/2023 and 22/11/2023