AXON

17 RILEY CLOSE, DAVENTRY
NORTHAMPTONSHIRE
NN11 8QT
UNITED KINGDOM

UK.AXON.COM

Axon Security Questions

Project Governance

A Privacy Impact Assessment should be sought (you thought your predecessor may have completed one), if not one should be completed.

- Axon can work with WMP to complete a PIA sufficient to the needs of the force.

A User SyOps should be created to clarify and enforce correct use of the cameras, including security incident reporting in the event of loss.

- Axon can provide supporting documentation to assist with the creation of a WMP User SyOps

Support resources should be identified and managed so that we leverage UK resources assigned to the UK company, rather than offshoring support / access rights to the US Parent Company.

- Support staff type, access level, and vetting information is provided in the Axon RMADS.

Requirements generated by BWV for connectivity with other systems, such as OpPolSol should be raised with all of those projects separately so that dependencies are captured and factored in

- Axon can assist in providing the information needed to support these considerations.

Cloud Environment

[redacted] to work with [redacted] to review the Solution design that Axon are proposing for the cloud environment. This will ensure that it is at least equal in protection to our own network.

- RMADS sent to [redacted] and [redacted]

AXON

20 RILEY CLOSE, DAVENTRY
NORTHAMPTONSHIRE
NN11 8GT
UNITED KINGDOM

UK.AXON.COM

Axon are in the process of conducting an ITHC / Pen Test of the [redacted] environment. This needs to be confirmed as a CHECK-certified third party, and WMP should obtain a copy of this report.

- Axon has [redacted] to perform the upcoming ITHC, who has CHECK-certified leads.

Axon and [redacted] should both provide evidence against the 14 Cloud Security Principles. These are comprehensively documented on the NCSC website, and will give us a starting point for conversations with them around the security of their cloud provision.

- Axon has created a Cloud Security Principles Implementation document that details the 14 Cloud Security Principles and explains how the specific security policies and practices for Evidence.com align with the principles. Also, detail is provided that depicts how Evidence.com has implemented the principles and how the implementation is validated and tested. Attached to email.

The exact physical location of our data should be sought.

- Axon uses [redacted] deliver the Evidence.com service. [redacted] not disclose the exact physical location of data centres, however, data centers are wholly in the UK and a PASF assessment has been performed.

Certification of the Data Centres, and the Axon environment should be confirmed as being compliant with ISO/IEC 27001, ISO/IEC 9001, and PASF.

- [redacted] ISO 27001 and ISO 9001 certified. Related to a PASF: a PASF assessment was completed in July by the home Office's National Police Information Risk Management Team (NPIRMT) who visited one of the Microsoft UK Data Centers and carried out a comprehensive review of physical security. At the conclusion of this review no remedial actions or non-compliance issues were raised. The detailed results of the assessment were not shared Axon or Microsoft but the NPRIMT PASF assessment is available to policing customers from the Home Office for individual Police Services to review as part of their own approach a risk assessment in utilizing cloud services.

AXON

17 RILEY CLOSE, DAVENTRY
NORTHAMPTONSHIRE
NN11 8QT
UNITED KINGDOM

UK.AXON.COM

Support staff should be identified, and their varying access levels clarified. National Vetting Policy should be applied based on these results.

- Support staff type, access levels, and vetting information is provided in the [redacted]

Local Infrastructure

InfoSec should review the designs for this with Architecture.

- Axon can provide the Evidence.com Service RMADS to assist with this activity.

An ITHC / Pen Test should be conducted on the infrastructure based on the above.

- An ITHC is planned for Q3/Q4 of 2017.

Cameras

Axon should provide evidence against the End User Device Principles. These are comprehensively documented on the NCSC website, and will give us a starting point for conversations with them around the security of their devices.

- Although Axon cameras can be viewed as end user devices, Axon has designed cameras to have limited functionality to support the needs of a body worn camera use case. Axon believes the UK End User Device Security Principles has limited applicability to Axon cameras.

Axon should provide evidence against how their devices meet or exceed the nationally mandated technical requirements for Bluetooth which were accepted at a local level by the DCC. Authority to use Bluetooth / NFC outside of these requirements has not be granted. Wi-Fi is governed by a separate document if that is what is used on the cameras.

AXON

20 RILEY CLOSE, DAVENTRY
NORTHAMPTONSHIRE
NN11 8QT
UNITED KINGDOM

UK.AXON.COM

- Axon initial response to Bluetooth and/or NFC concerns attached to email. [redacted]

Cameras should be subjected to an ITHC / Pen Test to confirm the efficacy of physical security controls around the devices. The results of this test will form the majority of the basis for any recommendation for applying device encryption. A supplier sourced CHECK-certified test, or a test sourced from digital forensics would be acceptable, however it would be a far stronger defence of any decision not to encrypt the devices if this was completed by a WMP-sourced CHECK-certified third party.

- A customer-sourced ITHC has been performed on the current generation of Axon cameras by GMP.

Certificates

The scope of the ISO/IEC 27001:2013 certificate is limited to [redacted] provides the physical building, physical security, environment controls and within dedicated virtual private clouds (VPC): computing capability, data storage, identity & access management and network connectivity." This doesn't cover the [redacted] but it is reassuring that the organisation has one. Maybe they just haven't updated their website? Can we get the current ISO cert?

- Axon's ISO certification scopes are updated on an annual basis to align with predefined audit periods and activity. Evidence.com on [redacted] in the UK is added to scope in 2017 testing. This updated certification will be available by end of year 2017. Axon operates the Evidence.com on [redacted] instance in an ISO 27001 compliant manner.

The SOC 2+ is an American standard, but is around DC management, can we see if it applies to the UK [redacted] cloud, and if so, get a copy?

- The Axon SOC 2+ focuses on Axon's controls over AICPA Trust Service Principles and Criteria. Similar to the timeline constraints in the ISO certification process, Evidence.com on [redacted] in the UK has been added to the 2017 scope with the report available near the end of 2017.

AXON

RILEY CLOSE, DAVENTRY
NORTHAMPTONSHIRE
NN11 8GT
UNITED KINGDOM

UK.AXON.COM

Axon are claiming accreditation to OFFICIAL. Has this product been accredited by the Home Office then? Their website hasn't been updated since CESG got absorbed in to NCSC a couple of years ago, and IS1 & 2 framework isn't supported by HMG anymore, but if we could get a hold of the RMADs for [redacted] then it would be an excellent starting point for us. The Cloud Security Principles document below claims the environment is suitable for OFFICIAL – SENSITIVE, which is on conflict with this so we just need to find out what we are working with.

- Evidence.com has not been accredited by the Home Office, however, we are actively engaged to undergo Home Office accreditation. Axon understands that the IS1 risk standard is dated, and is evaluating updating the risk framework in the RMADS to better suit the needs of our customers.

Evidence against the Cloud Security Principles was a good find. I've had a look and it gives some assurance for us, but there are some areas of concern. I'd like to go through this with you so that I can point out some areas where we might need additional information from Axon, or where they may need to change their responses. Before we do that however, can we confirm that this document is still current and applies to [redacted] the date suggests publication in Oct 2016 but I don't know if the [redacted] environment was stood up then.

- Axon operates all Evidence.com deployments in a similar fashion. While the Cloud Security Principles document was published prior to Evidence.com on [redacted] the UK's existence, the content is accurate for the service.