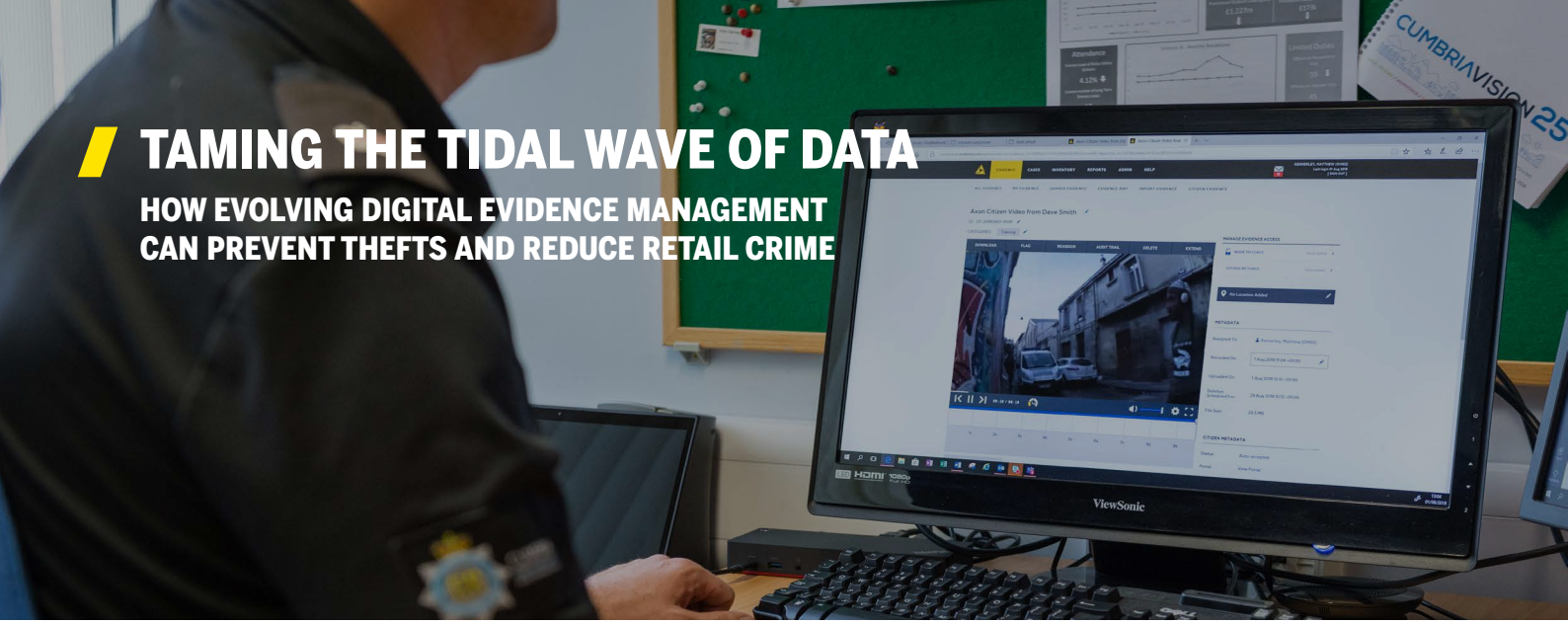

TAMING THE TIDAL WAVE OF DATA

HOW EVOLVING DIGITAL EVIDENCE MANAGEMENT CAN PREVENT THEFTS AND REDUCE RETAIL CRIME

In today's age of smartphones and CCTV footage, digital evidence is key to crime investigations in the retail environment. There is so much data, however, that without an effective way to manage it, evidence sharing and collection can be time consuming and ineffective. For retailers, this can mean thousands or millions of pounds of lost inventory or damage due to robberies, thefts, or other crimes. This is where digital evidence management systems come in to play, and where retailers can partner with their local police forces to efficiently share evidence so that it can be used most effectively for investigations.

/ WHAT IS A DIGITAL EVIDENCE MANAGEMENT SYSTEM (DEMS)?

A digital evidence management system, or digital asset management software, is the virtual command post for management of all digital forms of evidence in a police force, from collection to prosecution. From CCTV footage to body-worn video, to smartphone videos from the public, a DEMS/DAMS is a reliable hub to store and link data. DEMS/DAMS allow police forces to maintain continuity of evidence and audit trails over all evidence, tag and organise media from first- and third-party sources, and share evidence with relevant authorities, such as the Crown Prosecution Service.

/ HOW DO POLICE FORCES USE DEMS/DAMS, AND HOW CAN THAT HELP INVESTIGATE AND SOLVE RETAIL CRIME?

Forces use a DEMS/DAMS to link relevant evidence together for a more efficient investigation, share evidence electronically with needed parties, and reduce time in collecting evidence from the public and business. In the case of retail crime, it is the evidence coming in from stores that can make or break a case, so it is imperative that evidence is collected efficiently and securely.

Historically, Forces have collected evidence in a non-centralised fashion, with files shared from retailers via email, hard drives, or burned discs. However, the risk with this approach is that digital evidence collection can become corrupted, separated from other relevant files, and is quite simply a time-consuming activity for all parties.

In collecting evidence electronically via a DEMS/DAMS, Police and retailers can ensure that critical evidence is shared in a streamlined way, freeing up resources for core operational activities.

/ WHAT ROLE DOES YOUR ORGANISATION HAVE TO PLAY AND HOW CAN YOU PARTNER WITH LOCAL POLICE?

Private and public partnerships are key to boosting public safety in your community. Here are a few steps you can follow to partner with local police.

- Familiarise yourself with the DEMS or DAMS your local police force use, or if they don't currently use one, speak to the National Business Crime Centre about who you can partner with to ensure that becomes a reality for your business community.
- Ensure that forces have a secure method for community members or retailers to submit secure evidence, such as Axon Citizen. With straightforward sharing workflows, Axon Citizen makes it a seamless, painless process to input evidence and share evidence with the police.
- Proactively share CCTV footage, images, and other useful materials in the case of an incident.

/ IS THERE A COST TO RETAILERS?

As the costs for implementing and maintaining DEMS/DAMS go through local police budgets, there is no cost for retailers.

/ HOW SECURE IS A DEMS/DAMS?

Security is of utmost priority in any digital evidence management system, especially given the sensitive nature of the data. A good sign that a DEMS or DAMS prioritises safety of the data it stores is that it has key security certifications, such as ISO 27001. Set retention policies as well as configurable permissions and access also help to keep a DEMS/DAMS reliably secure and protect the important media stored within it.

In the case of Axon's solution, Axon Evidence, as an example, the following security safeguards are in place:

Mature, audited encryption key management procedures with evidence encrypted in transit and while at rest in storage

Tamper-proof audit logs and forensic fingerprint using the industry-standard SHA hash function to ensure data integrity

Multi-factor authentication, authorisation, secure sharing and permissions

Certified to industry standards and codes of practice, including OFFICIAL and OFFICIAL SENSITIVE data

Axon's compliance demonstrates our commitment to providing a trustworthy platform and offers customers a way to understand the controls that have been put in place to secure Axon Evidence and their data. Our certifications include:

- ISO/IEC 27001:2013 Certified
- ISO/IEC 27017:2015 Certified
- ISO/IEC 27018:2019 Certified
- SOC 2+ and SOC 3 Report
- Cloud Security Alliance - CSA STAR Attestation (Level Two)
- Cloud Security Alliance - CSA STAR Self-Assessment (Level One)
- Accessibility Conformance Report - WCAG 2.0 & VPAT/Section 508
- UK OFFICIAL Accreditation
- UK Cloud Security Principles Implementation
- Cyber Essentials Certified

/ WHERE IS THE DATA STORED?

With the increasing shift in cloud-based storage as opposed to on premise, many wonder where the servers are located. At Axon, all digital evidence is stored securely on Microsoft Azure cloud infrastructure, and it never leaves the UK.

You may wonder who can view your data and digital evidence. Police forces set role-based permissions in Axon Evidence based on responsibilities within the force. Due to the security of Axon's platform, the evidence will only be accessible to those with the proper permissions and will have robust audit logs to track activity by those authorised to manage the evidence.

To learn more about Axon Evidence's safety and security features please visit **uk.axon.com/compliance** and **uk.axon.com/security/axon-evidence**.