Key Trends in Digital Evidence

2024 AXON DIGITAL EVIDENCE COMMONWEALTH COUNTRIES TRENDS REPORT

AXON

Executive Summary

The quantity and quality of digital evidence available to police forces and government agencies continues to grow and evolve. While this data is helping agencies solve more cases than ever before, it has also presented a key set of challenges.

Police forces and government agencies need a scalable solution to identify, store, manage, investigate and share their ever-growing collection of digital evidence files. This solution must be secure and ensure evidence is not lost or altered during the investigative process.

Axon Enterprise is on a mission to Protect Life, Preserve Truth and Accelerate Justice by providing police forces and government agencies with the tools they need to collect and manage vast amounts of digital evidence. As part of this work, we conducted a digital evidence trends survey featuring 200 responses from police forces and government agencies in the United Kingdom, Australia and New Zealand. This survey provided valuable insight into how agencies are maturing their digital evidence strategies to handle the modern challenges of digital evidence.

Key Findings

1. **Body-worn cameras are making a positive difference:** Officers believe that body-worn cameras (BWCs) are helping to build trust, improve safety and make their jobs easier.
2. **Video evidence is everywhere:** The amount of digital evidence available to police forces and government agencies is rapidly multiplying as BWCs, CCTV cameras, smartphones, doorbell cameras and other recording devices continue to grow in use.
3. **The storage of digital evidence is an ever-growing challenge:** Countless sources of evidence create headaches for agencies looking to store digital evidence.
4. **Accurate playback is an unrecognised challenge for many police forces and government agencies:** A vast array of digital evidence file types has created challenges for accurate playback of video evidence.
5. **Digital evidence management takes up valuable time:** Redaction, uploading and searching for evidence all remain a critical and time-consuming part of the digital evidence management process.
6. **Security and efficiency continue to be the top criteria when evaluating digital evidence management systems (DEMS):** When it comes to digital evidence management, modern challenges call for secure solutions.

We will now do a deep dive into the data.

Body-Worn Cameras Are Making a Positive Difference

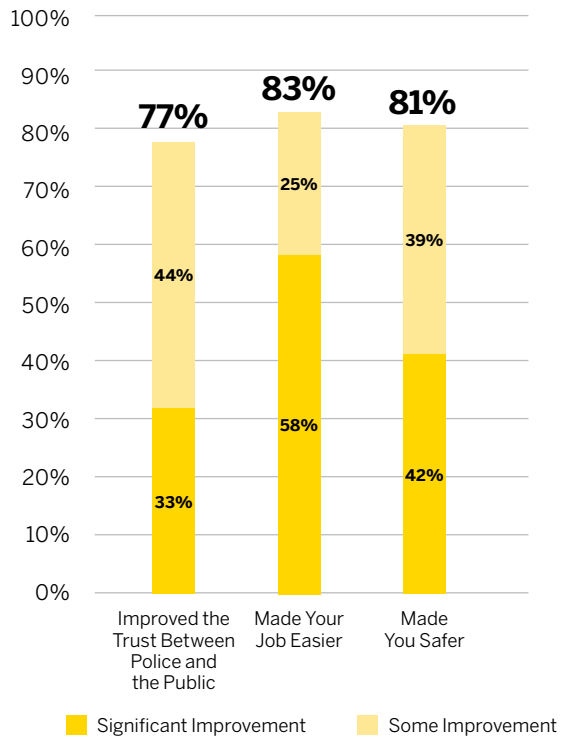
Officers believe that BWCs are helping to build trust, improve safety and make their jobs easier. One of the primary goals of body-worn camera technology is the preservation of truth.

Additionally, our survey found that approximately 8 in 10 police officers believe that BWCs have had a notable improvement in making officers safer, making their jobs easier, and improving trust with the public. This highlights the power and opportunity of using technology to meet the needs of police forces and government agencies.

For police officers in the United Kingdom, 95% said that BWCs have made their jobs easier.

TO WHAT EXTENT DO YOU FEEL BODY-WORN CAMERAS HAVE:

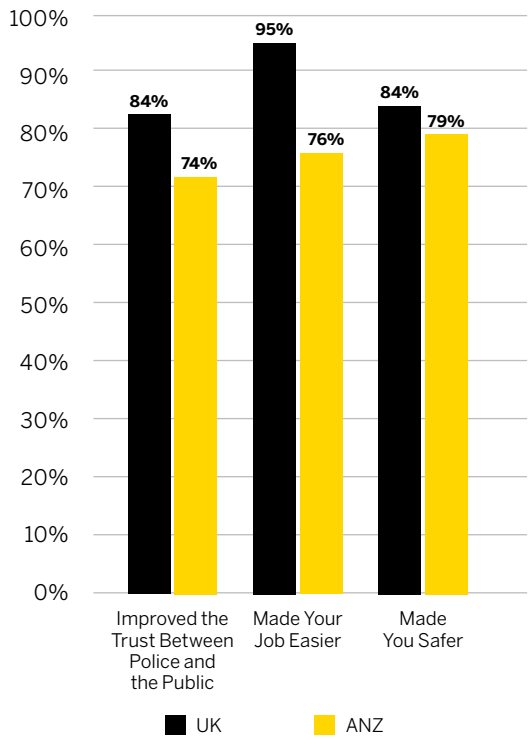
Significant + Some Improvement



ADDITIONAL INSIGHTS INTO THE DATA:

ANALYSIS BY COUNTRY

Significant + Some Improvement



Because of these positive improvements, the prevalence of body-worn cameras will only continue to increase. As technology evolves, we will continue to see BWCs as a rich source of evidence by virtue of their efficiency and how easily they can sync with a cloud-based Real-Time Crime Center and Digital Evidence Management Solution.

Footage from BWCs may be the most common type of video evidence, but it is just the tip of the iceberg when it comes to the types of digital evidence available to today's police forces and government agencies.

Video Evidence is Everywhere

The amount of digital evidence available to police forces and government agencies is rapidly multiplying as BWCs, CCTV cameras, smartphones, doorbell cameras and other recording devices continue to grow in use.

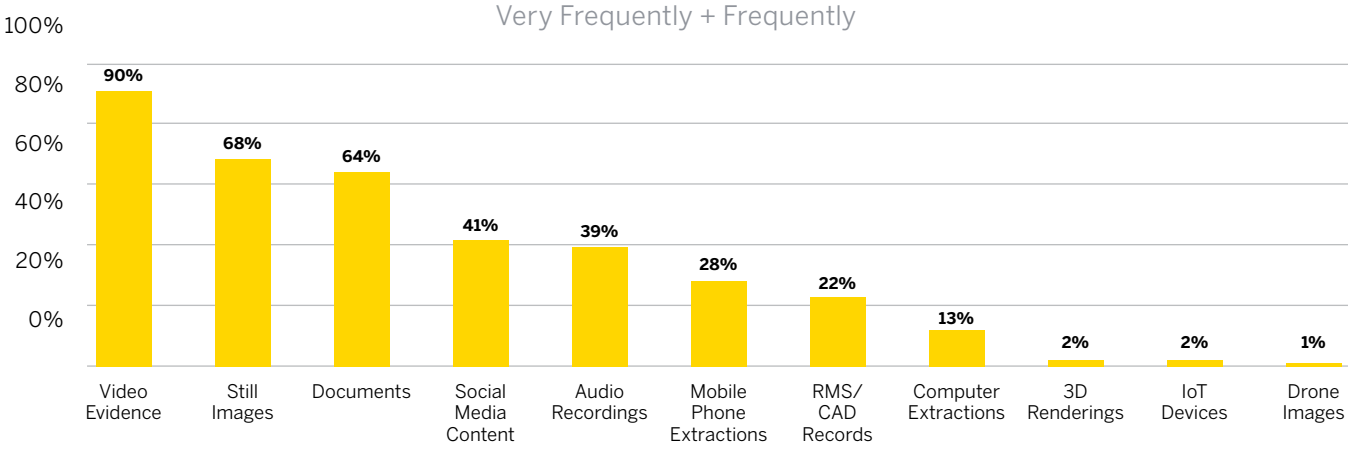
Video evidence is the most prevalent source of digital evidence being utilised by police forces today. In fact, 9 in 10 respondents noted they very frequently or frequently encounter video evidence within their investigations.

9 IN 10

RESPONDENTS NOTED THEY VERY FREQUENTLY OR FREQUENTLY ENCOUNTER VIDEO EVIDENCE WITHIN THEIR INVESTIGATIONS

In other words, reviewing video evidence is no longer the work of a few specialists. Anyone and everyone at an agency may be required to watch and investigate video evidence.

HOW FREQUENTLY DO YOU ENCOUNTER THE FOLLOWING DIGITAL EVIDENCE SOURCES?

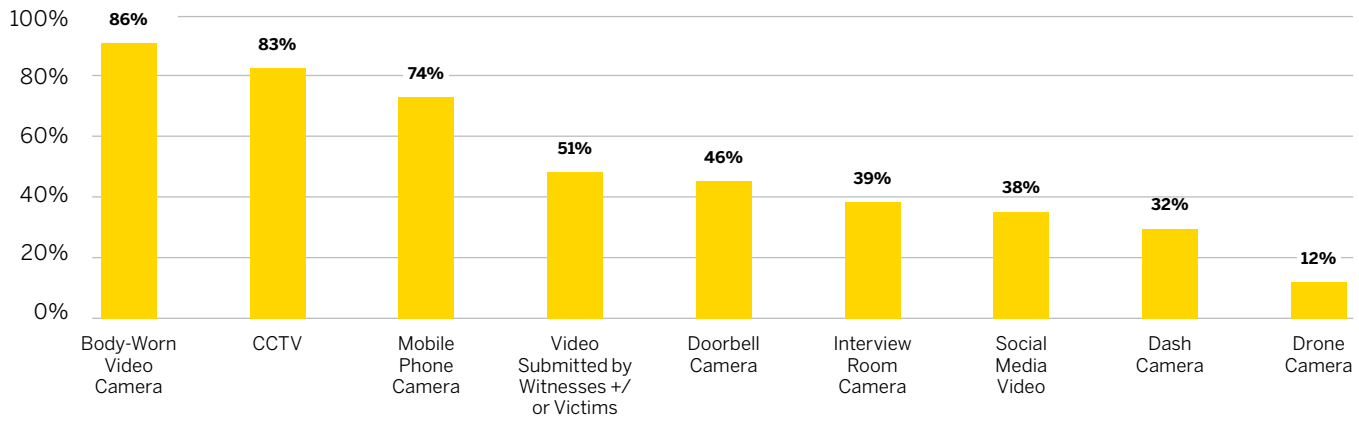


Diving deeper into video evidence, the survey asked respondents the various types of video evidence encountered. The most frequently encountered video evidence is BWC footage. 86% of respondents stated that they very frequently or frequently encounter BWC videos in their investigations.

The second most common type of video evidence is CCTV, which is frequently encountered by 83% of participants. 74% stated they frequently encounter mobile phone videos, while 51% frequently receive video from witnesses and/or victims. Other video sources like doorbell cameras, interview room cameras, social media video, dashboard cameras and drone cameras are all seen by a sizeable number of officers as well.

HOW FREQUENTLY DO YOU ENCOUNTER THE FOLLOWING VIDEO SOURCES?

Very Frequently + Frequently



When looking at our past trend reports, the data shows that these different video sources will continue to grow, which means the prevalence of video evidence cannot be ignored. Every police officer will likely engage with video evidence at some point, so each should be equipped with the tools and training to review evidence in a forensically-sound way.

While the rapid growth of digital evidence is helping agencies close more cases and build trust with their communities, this vast expansion of digital evidence has also created challenges, including questions of proper storage and accurate playback.

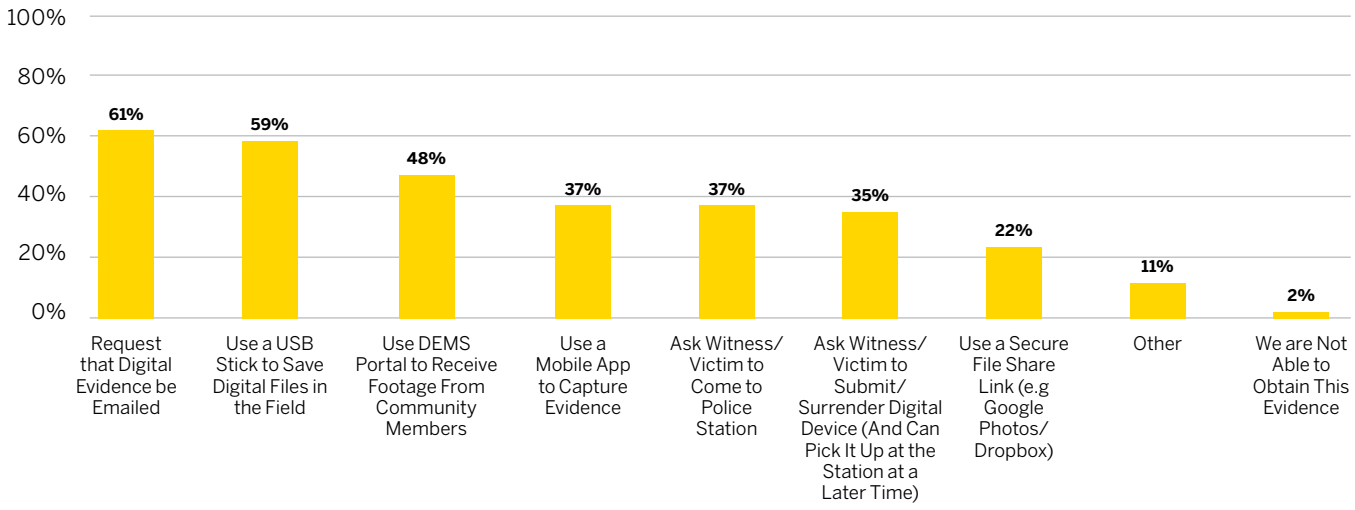
The Storage of Digital Evidence is an Ever-Growing Challenge

Countless sources of evidence create headaches for agencies looking to store digital evidence.

With so many different sources of digital evidence, it is no surprise that there are many different methods for collecting this evidence from the field. Our survey found that 61% of respondents request digital evidence via email, while 59% physically visit a location to retrieve digital files onto a USB stick.

HOW DO YOU TYPICALLY COLLECT DIGITAL EVIDENCE IN THE FIELD?

(Select all that apply)



Each of these collection methods poses challenges. Emailing digital evidence can save time, but does not work on files of a certain size. And even when files are small enough to be emailed, the evidence will often be compressed or transcoded before sending. USB sticks provide the opposite problem. Officers can use a USB stick to retrieve the original, full-sized file, however this method of collection requires a physical trip and can be extremely time-consuming. Both of these methods introduce new storage locations for digital evidence, increasing the chances of mishandled or lost evidence. And there is no chain of custody while the evidence is in transit, which poses a security risk for agencies.

7 IN 10

RESPONDENTS SAID THEY HAD BEEN INVOLVED IN A CASE WHERE DIGITAL EVIDENCE WAS LOST OR MISPLACED

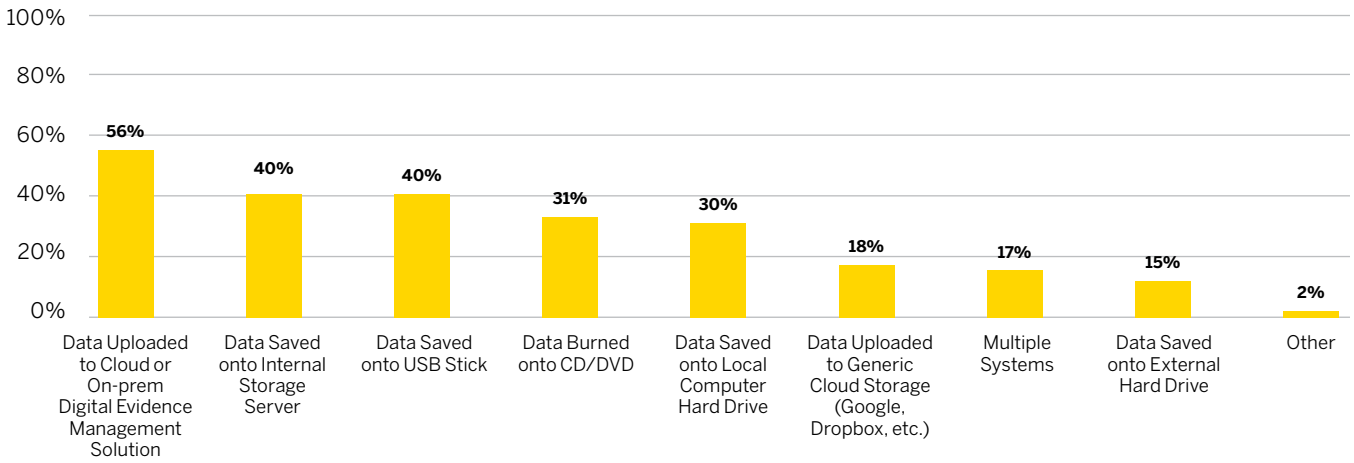
One alarming result from our survey was that 7 in 10 respondents said they had been involved in a case where digital evidence was lost or misplaced. Many respondents stated this will "continue to occur." Why is the misplacement of evidence so prevalent?

42% of respondents noted that today, their agency uses 3 or more methods to store digital evidence. 56% of respondents stated their agency stores video evidence on a digital evidence management system (either on-premises or in the cloud). 40% stated their agency stores digital evidence on an internal server, while 40% stated their agency uses USB sticks. 31% of agencies are still burning data onto DVDs, 30% are saving digital evidence to their local computers' hard drive, and 18% are uploading digital evidence to generic cloud storage solutions (such as Dropbox or Google Drive).

The solution for secure digital evidence collection is currently the third most popular method of collection: using a DEMS portal to receive footage from community members. DEMS portals allow agencies to request evidence directly from their DEMS solution, removing the need to physically travel to collect evidence, and providing a simple method for the upload of original, uncompressed files. By collecting evidence correctly through their DEMS platform, agencies reduce the risk of lost evidence, and ensure chain of custody can be tracked throughout the evidence collection process.

HOW DOES YOUR FORCE TYPICALLY STORE VIDEO EVIDENCE?

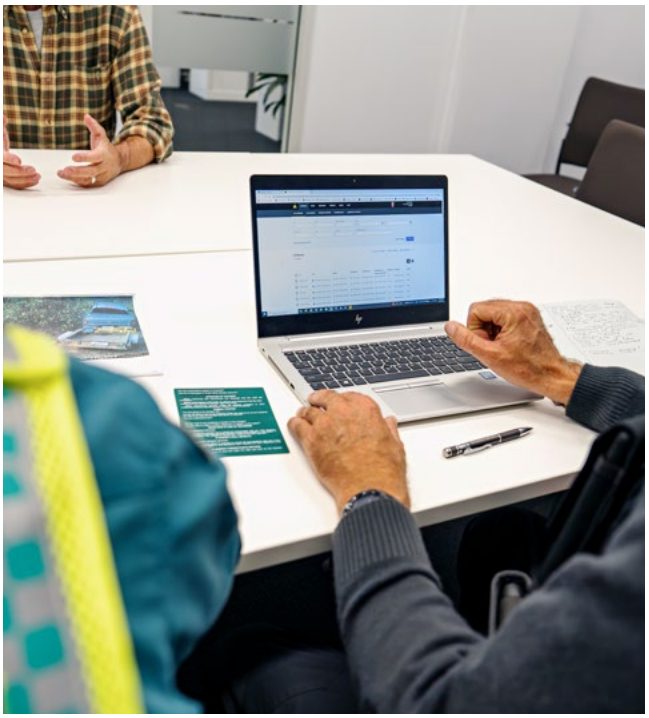
(Select all that apply)



When digital evidence is collected and stored in multiple locations, it is natural that evidence begins to be misplaced. Not only is this process not secure, but it is also inefficient: "Our current practice is to export about 20 gigabytes of photos from an internal hard drive to multiple DVDs, and then onto an external hard drive as a backup. This process takes hours every week" wrote one respondent.

Interestingly, agencies that use multiple tools for storing digital evidence don't usually make a concerted decision to do so — the number of storage tools simply evolved over time as new sources of digital evidence popped up.

The growth of digital evidence is not slowing down. For this reason, it is imperative that agencies pause and evaluate their data collection and storage methods. There are several benefits to bringing all the digital evidence into a single, secure location.



Accurate Video Playback is an Unrecognised Challenge for Many Police Forces and Government Agencies

A vast array of digital evidence file types has created challenges for accurate playback of video evidence.

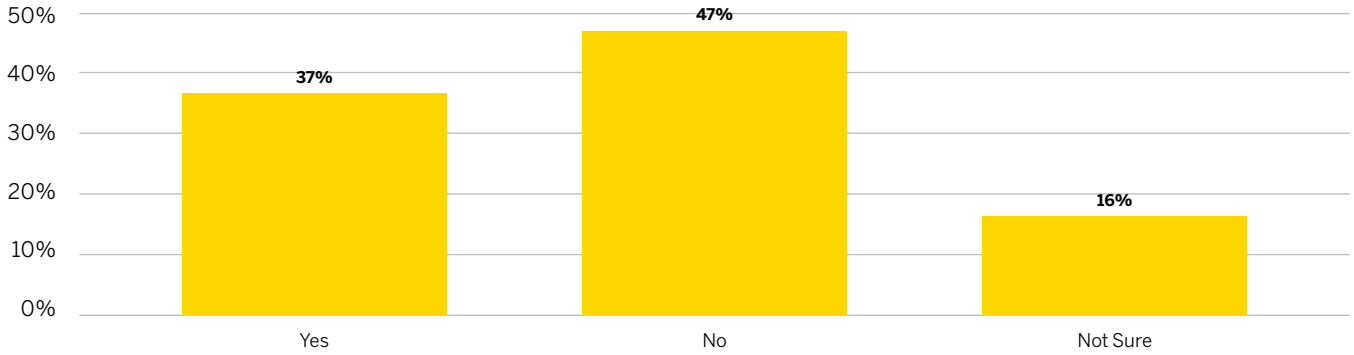
The growth of video recording devices has led to an equally rapid growth in file formats. Many CCTV cameras (the second most popular video source according to our survey), for instance, record to proprietary video formats like .dav, .exe. and .g64. Playback of these third party video formats is a major challenge and risk to police forces and government agencies.

Grant Fredericks, a leading expert in forensic video analysis who has testified in Canada, the United Kingdom, Australia and New Zealand explained the problem this way:

> **"I think the biggest challenge today for video analysts is to understand that proprietary video systems like CCTV cameras and Ring doorbells...they're all proprietary. They don't talk to each other."**

It's frustrating for officers to not be able to play a key piece of video evidence due to a file type not being recognised. It can be even more frustrating, not to mention putting the integrity of the investigation at risk, when an officer converts a video file without realising that the conversion may have altered the video itself.

HAVE YOU EVER BEEN INVOLVED IN A CASE WHERE THE FRAME-RATE OF A VIDEO IMPACTED AN INVESTIGATION IN A NEGATIVE WAY?

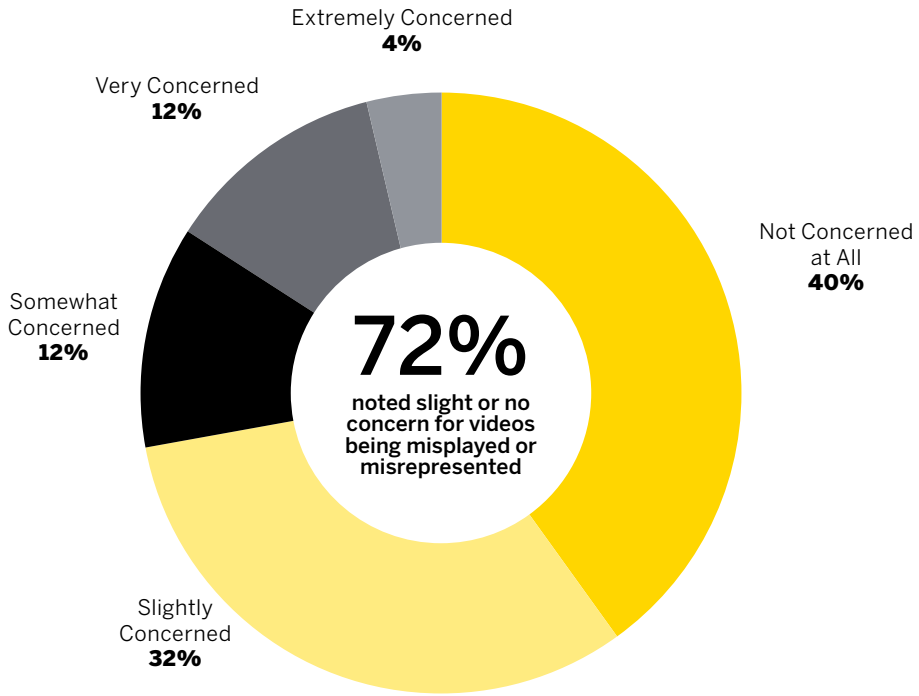


37% of forensic video experts surveyed have been involved in a case where misplayed video had a negative impact on the investigation. Some examples of misplayed evidence include:

- Playback where the video is mirrored or inverted
- Playback where compression removes details from the image
- Playback where frame rates are dropped, altering the perception of speed or force
- Playback where the aspect ratio is altered, changing the apparent width or height of objects

Despite these issues, nearly 75% of Detectives noted slight or no concern for videos being misplayed or misrepresented. Officers need to understand the risks of misplaying evidence. Misplayed evidence can be just as detrimental to an investigation as altering physical evidence like fingerprints. This use of force case in Ottawa, Canada, provides a striking example of the risks of misplayed evidence to an investigation.

WHEN REVIEWING VIDEO EVIDENCE, PLEASE RATE YOUR LEVEL OF CONCERN FOR VIDEOS BEING MISPLAYED OR MISINTERPRETED



To prevent misplayed evidence, agencies need proper training and tools for evidence playback. Tools for viewing video evidence should be forensically-sound and designed specifically for public safety. Leveraging a solution like Axon Investigate will help ensure videos are playable and accurate. Popular consumer tools like Windows Media Player and VLC lack the same capabilities of forensically-sound tools like Axon Investigate.

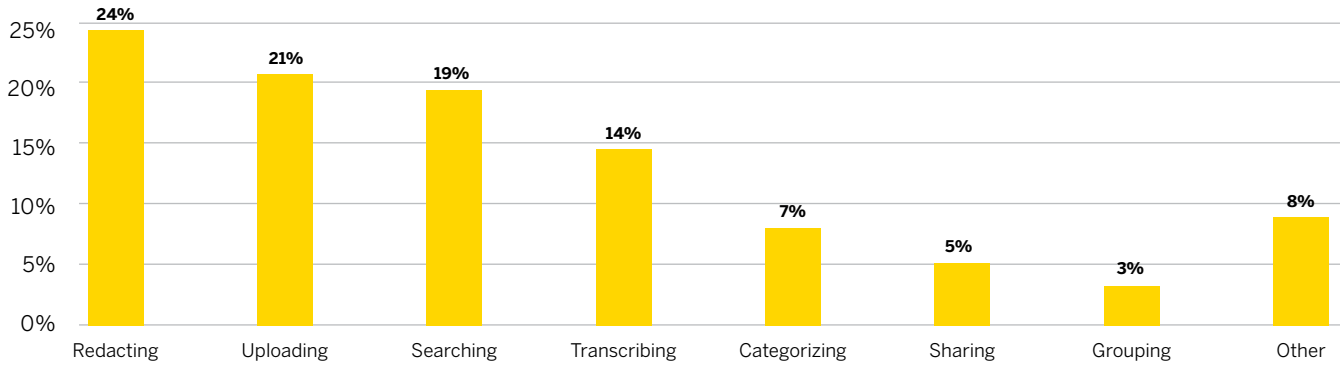
Digital Evidence Management Takes Up Valuable Time

Redaction, uploading and searching for evidence all remain a critical and time-consuming part of the digital evidence management process.

Today, police forces and government agencies are being asked to do more with less resources. Efficiency in digital evidence management is therefore critical. Our survey looked to uncover the biggest time drains in the digital evidence management process.

We asked survey participants, "What takes you the most time when managing digital evidence?" The top three answers were 'Redacting,' with 24% of respondents citing this as the most time-consuming portion of digital evidence management, 'Uploading' (21%), and 'Searching' (19%).

WHAT TAKES YOU THE MOST TIME WHEN MANAGING DIGITAL EVIDENCE



"Waiting for it to upload, redacting, transcribing and sharing"

– Marvin M., UK

"Running reports"

–Dianne B., NSW, Australia

"Watching on mobile devices"

– Matthew T., Australia

These challenges are not new to Axon. In fact, our product development process has been guided by a desire to curb each of these pain points. Over the last few years, Axon has introduced features such as Audio Redaction via Transcript, Upload XT Version 2, Transcript Keyword Search and Auto-Transcription. Each of these features is designed to save police officers time on data management so they can spend more time doing the work that is important to them.

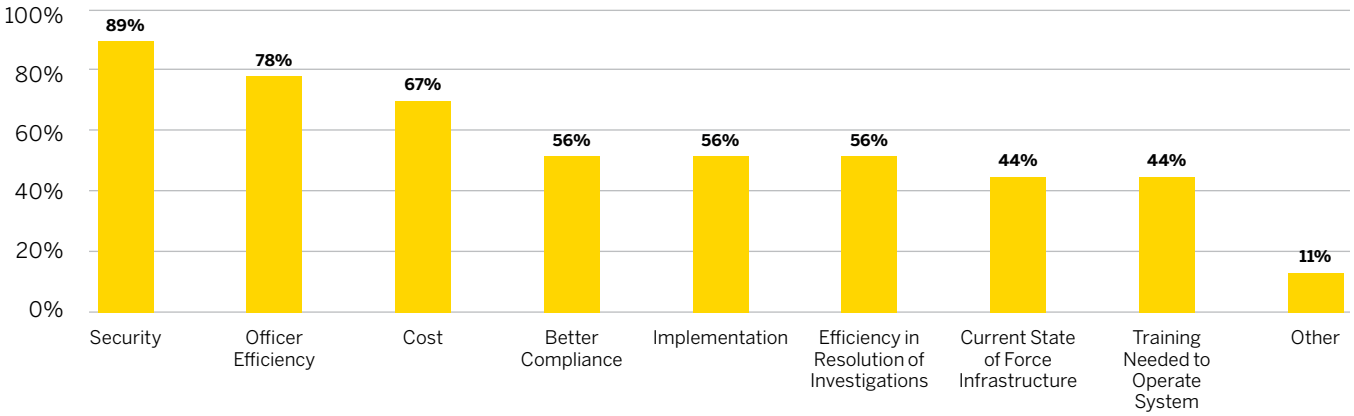
In order to address the issues of redaction, upload, search and transcription that currently plague the evidence management process, many agencies are now turning to cloud-based DEMS to help streamline their workflows.

Security and Efficiency Continue to Be the Top Criteria When Evaluating DEMS

When it comes to digital evidence management, modern challenges call for secure solutions.

According to survey respondents, when evaluating a Digital Evidence Management System, the top three criteria are: 'Security,' 'Officer Efficiency' and 'Cost.' Agencies also look for DEMS that can improve compliance, efficiently resolve investigations and are easy to implement.

WHEN EVALUATING A DIGITAL EVIDENCE MANAGEMENT SYSTEM, WHAT ARE THE KEY CRITERIA IN YOUR EVALUATION?



Security is a major concern when uploading, managing and sharing digital evidence. Police forces and government agencies frequently handle sensitive information, so it must be secure at all times. When evaluating a DEMS solution, it is always important to ensure the platform matches the security standards and regulations for both the agency and the country.

Security risks are lower overall when using cloud-based solutions as opposed to traditional on-premises options. In fact, the rash of ransomware incidents over the past few years has almost exclusively impacted on-premises storage systems. Modern cloud environments are frequently updated to maintain high-security standards and protect data. To learn more about cloud storage security, read the white paper On-prem vs. cloud storage: 5 considerations for digital evidence.

As discussed previously, officer efficiency is also more critical than ever. Tasks like redaction, upload, search and transcription can take significant amounts of time. Selecting a DEMS that helps drive officer efficiency will improve the user experience, increase adoption and allow officers to spend more time each shift in the community.

A well-designed DEMS can support officer efficiency in a myriad of ways, including:

- Leveraging body-worn cameras that automatically load video recordings to the cloud via WiFi or docking the camera
- Auto-transcription services that make it easier to review and search evidence
- Redaction tools that automatically identify faces, vehicle number plates and keywords
- Upload tools that expedite the upload of large amounts of data
- Playback tools that facilitate the secure playback of a wide variety of video file types
- Sharing tools that securely and efficiently help agencies share evidence with the Crown

Lastly, cost is a major factor when evaluating potential DEMS solutions. As the amount of digital evidence continues to grow, the cost of storing that evidence can skyrocket. Centralising all storage into a single location can help keep costs down, especially if an agency's DEMS solution offers unlimited storage options. Unlimited storage provides several benefits, including budget predictability.

The world of digital evidence will continue to grow and change quickly, and the ability to seamlessly update and upgrade cloud-based DEMS solutions will help agencies keep up with the changing demands.

Conclusion

Digital evidence has dramatically changed the criminal justice process throughout the Commonwealth. While more evidence has helped many agencies solve more crimes, the massive flood of evidence has created challenges.

As technology evolves, it remains important for agencies to understand the latest trends in digital evidence management. By understanding both the benefits and challenges that come with new technology, agencies can identify the right training and technology solutions they need to help keep their communities safe.

About Axon

Axon is committed to Protecting Life, Capturing Truth and Accelerating Justice. As the world of digital evidence continues to evolve, the Axon DEMS platform provides agencies with an end-to-end solution for their digital evidence management.

Whether agencies work with BWC footage, CCTV footage, audio recordings, mobile phone extractions, drone footage or all of the above, Axon Evidence provides centralised and secure cloud-based storage and management for all digital evidence file types.

Connected solutions such as Axon Body 4, Axon Air, Axon Fleet 3, Fusus by Axon and Axon Investigate enable agencies to get the most out of their digital evidence. In addition to technology, training courses also provide agencies with key foundational knowledge on conducting video and digital investigations.

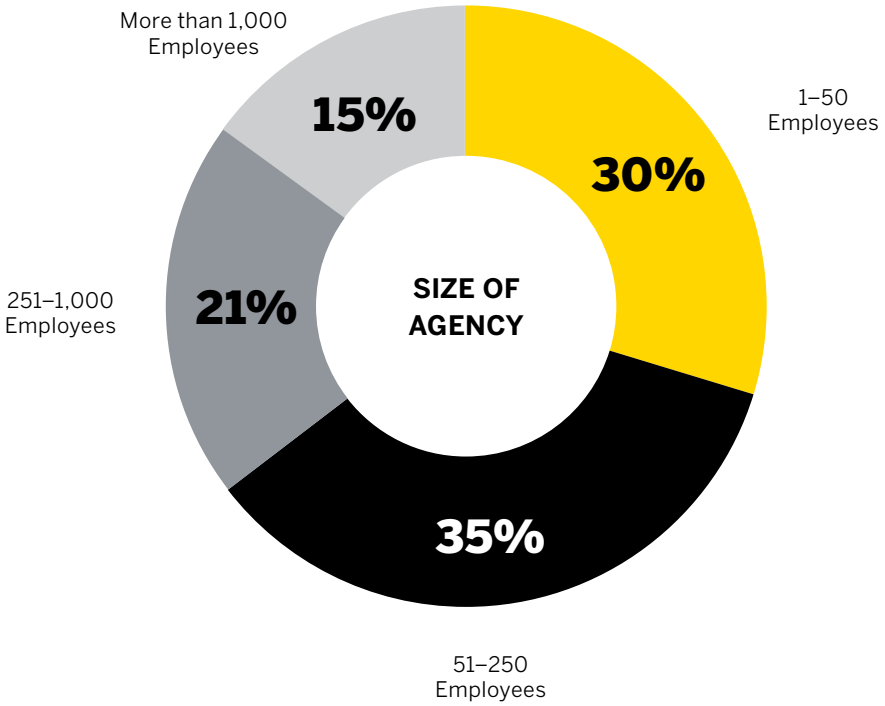
To learn more about how to solve the modern challenges presented by digital evidence, contact the Axon team via the UK Contact Form or the Australian Contact Form. Together, we will build the future of public safety technology.

Survey Methodology

The Axon 2024 Commonwealth Digital Evidence Trends Report survey ran from September - November 2023. Responses were collected via an online questionnaire. The dynamic survey followed different tracks based on roles, such as Police Officers, Detectives/Investigators, Criminal Justice, IT, Department Head, Forensic Video Analyst and Business Change/Transformation.

The survey received nearly 200 responses from Australia, New Zealand and the United Kingdom

Nearly half of respondents were from local police forces. Respondents represented small, medium and large organisations.



More Than 36 Agencies Participated in the Survey. Agency Logos Include:

Queensland Government
Department of Justice and Attorney-General
Department of Transport and Main Roads

AXON.COM