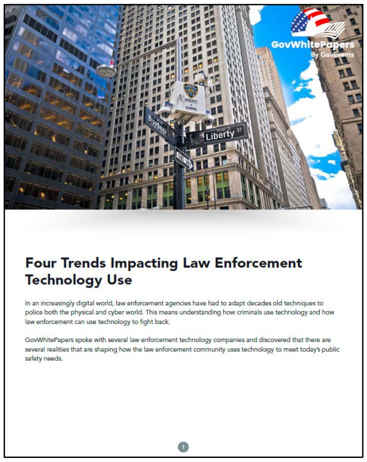
carahsoft.



Four Trends Impacting Law Enforcement Technology Use

In an increasingly digital world, law enforcement agencies have had to adapt decades old techniques to police both the physical and cyber world. This means understanding how criminals use technology and how law enforcement can use technology to fight back.

GovWhitePapers spoke with several law enforcement technology companies and discovered that there are several realities that are shaping how the law enforcement community uses technology to meet today's public safety needs.

1

Law Enforcement Technology Trends Report

Featuring: ADF Solutions, GovWhitePapers, Magnet Forensics, Mark43, and Voyager Labs

Thank you for accessing this Carahsoft resource.

To learn how to take the next step toward acquiring Carahsoft's law enforcement (LE) solutions, please check out the following resources and information:

For additional resources:
carah.io/LEResources

For upcoming events:
carah.io/LEEvents

For additional Carahsoft solutions:
carah.io/CarahsoftSolutions

For additional LE solutions:
carah.io/LEsolutions

To set up a meeting:
sales@carahsoft.com
703-871-8500

To purchase, check out the contract vehicles available for procurement:
carah.io/CarahsoftContracts

GovWhitePapers
By GovEvents

Four Trends Impacting Law Enforcement Technology Use

In an increasingly digital world, law enforcement agencies have had to adapt decades old techniques to police both the physical and cyber world. This means understanding how criminals use technology and how law enforcement can use technology to fight back.

GovWhitePapers spoke with several law enforcement technology companies and discovered that there are several realities that are shaping how the law enforcement community uses technology to meet today's public safety needs.

Trend 1: Managing High Value and High Volume Data

The data held by law enforcement agencies is some of the most sensitive data in existence. Not only is it highly personal, it has life altering impacts and must be handled with incredible care to maintain veracity. This high value data is valuable for good and bad actors alike, making law enforcement an attractive target for cybercrime, including ransomware.

Law enforcement systems are an incredibly attractive target for ransomware and ransomware attacks of this type are increasingly two pronged. The first request for money will restore access to systems, but that is frequently followed by a second request for payment to ensure information is not leaked. An example of this type of attack was a breach of the Washington, D.C., Metropolitan Police Department[1] computer network, resulting in detailed information about nearly two dozen officers, including Social Security numbers and psychological assessments being published.

Data Storage Concerns

Protecting this type of information is of paramount importance and becomes even more complex when you realize the sheer amount of data held by law enforcement. Body cameras, surveillance videos, patrol car data, and more must be stored, accessed, and interpreted by law enforcement agencies. Increasingly, law enforcement is turning to third party technology companies to provide the scale needed.

Cloud solutions are providing the storage capacity as well as processing power needed to fully utilize these terabytes of data. Dr. Stephen Boyce, Director, Magnet Digital Investigation Suite and Trey Amick, Director, Forensic Consultants with Magnet Forensics cited cloud as a critical tool in breaking down data silos, allowing for secure data sharing within and across organizations. The level of security cloud providers offer is far superior to current sharing techniques that often involve downloading information onto USB drives or CDs that could be easily misplaced, stolen, or broken.

Some jurisdictions are pooling resources to solve this challenge. North Carolina's Criminal Justice Analysis Center (CJAC) created a centralized, interactive portal for criminal justice data[2] collected by agencies across the state. The Justice Data Portal includes data from the North Carolina State Bureau of Investigation and the National Incident-Based Reporting System (NIBRS) (the FBI's crime database) making it available to other state and local law enforcement agencies. Idaho[3] and Colorado[4] have rolled out similar collaborative criminal justice data projects to help centralize and protect sensitive data.

Digital Evidence Management

Digital evidence is part of every case – not just cyber crimes. As Bret Peters, CEO of ADF Solutions points out, every victim and suspect has a phone that contains potentially important information. All of this information needs to be captured and stored, maintaining a chain of custody for use in charging and/or trials. For the past several decades this was done in specially built crime labs that served a regional area. This process worked well until the scale and scope of data being collected began to outpace the specially trained resources available.

Today, each law enforcement organization – from major metropolitan departments to small rural bureaus – requires some sort of in-house digital forensic capability to meet digital evidence needs. Peters reports that in the UK, police forces are able to use an app to do on-site triage of devices to determine if there is valuable information available. If none is found, the device can remain with the person (who could simply just be a witness) as opposed to being confiscated and held for days, weeks, or months while a crime lab works through a backlog. Boyce echoed this shift to field forensics citing technologies that allow officers to pull pertinent video and data off devices during the initial investigation, allowing victims and witnesses to retain their technology, building trust in and cooperation with the investigation.

In an effort to allow quicker in-region ballistics analysis[5], Ohio has invested in devices that help investigators compare microscopic markings on bullet casings recovered from a crime scene to images in the National Integrated Ballistic Information Network (NIBIN). This investment will increase the number of forensic units in Ohio from 5 to 16. Five units will be placed at the Bureau of Criminal Investigation's (BCI) state crime labs, and two portable units will test evidence on-site in underserved areas of the state, such as southeast Ohio's Appalachian region. These additional systems will help decrease turnaround time on testing results, more quickly identifying whether a firearm had been used in multiple shootings, and passing that information to law enforcement as an investigative lead.

Artificial Intelligence in Law Enforcement Leads to Real Insights

The volume of data in today's investigation cannot be effectively used with manual methods. A recent FBI investigation seized six petabytes of data, making it impossible for traditional methods to be used to analyze and make relevant insights. Courtney Bromley, CEO of Voyager Labs calls digital data the "crime scene of the 21st century." Effectively investigating this type of scene requires the use of Artificial Intelligence (AI), a critical emerging technology in law enforcement.

AI automates the data searching and trend analysis connecting dots that used to take analysts days or weeks. Those same analysts get the information in seconds allowing them to apply higher level analysis and pull in even more data to make additional connections. Bromley's team has seen law enforcement clients use AI to integrate visual data with search warrant data, and with analysis, one lead or data point leads to many others. Cases that begin with one suspect can evolve quickly into implicating a large crime ring.

Trend 2: Battling Bad Guys and Funding

Of course implementing these technologies comes at a cost. Not only do departments have to buy the software and devices, they have to train their forces to use them. Law enforcement agencies are part of the larger state and local government system and must compete for funding with so many other priorities.

Larry Zorio, CISO for Mark43, discussed several chicken and egg scenarios in play when it comes to funding. In order to justify budget requests, agencies need access to data – data that is spread across legacy systems (sometimes still on paper) – to build their case for investment.

The Seattle Police Department[6] captured data about the agency's interactions with people experiencing mental and behavioral health crises. A year of data showed Seattle police officers were engaging with people in serious mental crises about 10,000 times a year. Documenting the scope of mental health related work can go a long way in planning better programs and getting the funding needed to carry them out.

The Investment Does Not Stop With The Tech Purchase

When investments have been made in technology – be it body cameras or police software systems – even more investment is needed to make that tech useful. Many small departments are already looking to scale back their body camera programs[7] simply because they cannot afford to store and manage the thousands of hours of video footage.

Zorio shared that many agencies are meeting the demand for more tech and more tech expertise with Software as a Service (SaaS) solutions. Using SaaS vendors gets agencies the technology they need while alleviating staffing needs to manage that technology and helping to better manage cyber security risks. It's critical, he says, for law enforcement to work closely with SaaS vendors to ensure everyone is on the same page in terms of the data they need and the stories they want to be able to tell with that data. This helps to avoid being overwhelmed once they have systems in place to manage the vast information available.

Trend 3: Providing Transparency in Law Enforcement

The goal of many recent technology and program implementations is better transparency into policing. Data can help start a productive conversation with the community, providing a factual look at what programs are working and which are not. In fact, one of the goals of the NC Justice portal mentioned above is to "identify underserved victims, review the effectiveness of existing victim services and programs, or guide technical resource development for service providers."

In Seattle, police relied on data to tell their story to the community. They shared crime data, use-of-force data, mental and behavioral health crisis response data, and more. The agency even released raw data through their website to be as transparent as possible. Data sharing can be as simple as PDFs from an agency's records management system (RMS) or analytics software shared through the agency's website. However, the future is data portals that facilitate collaboration, allowing citizens to download and analyze that information independently.

There can be a downside to all of this data. Body cameras and surveillance video in particular are a murky area when it comes to proper use. Historically, regulation lags behind technology and adoption[8]. The fourth amendment, which protects against unreasonable searches and seizures, pertains to most government data collection, but there is a good deal of uncertainty about rights in regards to digital information. These legal gray areas when combined with new tech popping up on city streets can cause concern among civilians, impeding the goal of these technologies in the first place.

Trend 4: Fielding New Technology in the Field

Even with funding and well thought out data policy, technology rollouts can still fail if officers refuse to use it. Any technology introduced has to be easy to use and should streamline work rather than add to it. Mobile-first solutions are key to ensuring tech gets used by a field-heavy workforce.

Even the most tech-adverse officer likely has a smart phone they use personally. Having work applications mimic personal/consumer applications and making them available on those comfortable devices is key. Utilizing software and applications allow law enforcement agencies to maximize expertise in the field with the least amount of training. The goal being that by opening an app and performing a few clicks, software does the hard work of data collection and analysis allowing law enforcement to focus on the more personal aspects of policing.

5G is enabling a mobile-driven workforce and is built intentionally[9] to support certain technologies aligned with public safety sectors. Crime detection and surveillance can be improved with instant transfers of crucial video and audio recordings enabled by 5G networks. The 2022 New York subway shooting was resolved within a day; 5G surveillance may have reduced that time to a matter of hours or even minutes.

Moving Law Enforcement Technology Forward

Law enforcement agencies are under incredible pressure to deliver results quickly and accurately. Boyce attributes some of this pressure to the "CSI effect" – if the cops on TV can solve a crime using high tech devices in 45 minutes why can't my local police? Digital natives are also entering the workforce and expect the high tech tools used in their personal life and seen in entertainment. The inability to efficiently conduct business daily using cumbersome legacy technology leads to frustration and burnout of younger staff. The implementation of tech in law enforcement will only speed up in the coming years and agencies must prepare to meet the demand.

Implementing technology in the law enforcement community requires a sharing of experiences and best practices to improve the efficiency and transparency of policing.

GovWhitePapers will continue to explore the way technology is impacting policing and public safety, making valuable resources available to the government community. Our goal is to help the public sector navigate challenges, learn best practices, and stay up to date on technology innovations to continue driving public safety technology innovation forward.

References

1. Jeni Bergal, "Hackers threaten to release police records, knock 911 offline," *GCN*, May 14, 2021, https://gcn.com/cybersecurity/2021/05/hackers-threaten-to-release-police-records-knock-911-offline/316098/

2. Shourjya Mookerjee, "NC rolls out criminal justice data portal," *GCN*, April 13, 2022, https://gcn.com/data-analytics/2022/04/nc-rolls-out-criminal-justice-data-portal/365632/

3. Shourjya Mookerjee, "Idaho State Police upgrade crime dashboard," *GCN*, December 1, 2021, https://gcn.com/data-analytics/2021/12/idaho-state-police-upgrade-crime-dashboard/316320/

4. Stephanie Kanowitz, "How open data helps Boulder police, community tackle crime," *GCN*, August 11, 2021, https://gcn.com/data-analytics/2021/08/how-open-data-helps-boulder-police-community-tackle-crime/316205/

5. Susan Miller, "Ohio brings ballistics analysis in house," *GCN*, April 6, 2022, https://gcn.com/data-analytics/2022/04/ohio-brings-ballistics-analysis-house/364110/

6. Kristen Goode, "6 challenges impacting public safety & how agencies are adjusting," *Mark43* (blog), May 5, 2022, https://mark43.com/resources/blog/6-challenges-impacting-public-safety-how-agencies-are-adjusting/

7. Houston Thomas III, "Public safety agencies weigh storage requirements in the face of video demands," *StateTech*, April 25, 2019, https://statetechmagazine.com/article/2019/04/public-safety-agencies-weigh-storage-requirements-face-video-demands

8. Juliet Van Wagenen, "With public safety tech adoption, transparency is key," *StateTech*, December 15, 2017, https://statetechmagazine.com/article/2017/12/public-safety-tech-adoption-transparency-key

9. Prathamesh Khedekar,"How 5G can transform public safety," *GCN*, May 19, 2022, https://gcn.com/public-safety/2022/05/how-5g-can-transform-public-safety/367138/