IT Transformation of Emergency Services in North America

Simon Abrahams

Lead Analyst

teknowlogy Group, November 2019

Commissioned by

FUJITSU

teknowlogy GROUP

INTRODUCTION

Emergency services providers in the US and Canada face a hugely challenging balancing act, having to meet a growing demand for services while operating within tightening budget constraints. At the same time, rapid advances in technology are presenting new opportunities for transforming the way that emergency medical, police and fire services are delivered.

To explore this topic in more detail, teknowlogy Group has partnered with Fujitsu to study how public safety organizations on both side of the border are putting digital transformation front and center of their future strategies.

This paper aims to highlight how public safety services are already using data management and analytics, cloud computing and the Internet of Things to overhaul and improve existing services. This paper should also help first responder decision-makers understand the progress of their organization's IT transformation relative to their peers.

Many emergency organizations have already made a start on modernizing their IT, but progress is uneven, and difficult to manage in such mission-critical environments. Many first responder organizations have found that cloud helps them become more responsive and collaborative. Chatbots are being used to handle non-urgent enquiries, freeing more staff to support actual emergencies. AI and Big Data are identifying expected future trouble-spots, while data from drones, body cams and IoT devices provide first responders with deeper insight into incidents.

At the same time public safety ICT transformation needs to avoid any negative impact on citizen experience, citizen safety or citizen trust, which are critical for effective emergency services. This means that legitimate citizen concerns about the ethical use of IT have to be handed sensitively. Data privacy and cyber security concerns also need to be addressed, since first responders have access to highly personal citizen information. While data breaches in any sector are mostly accidental, the public is also concerned that first responders' ability to protect them could be maliciously compromised by a cyber incident.

In summary, modernizing public safety solutions is central to driving transformational change, improving collaboration, effectiveness and value-for-money. This in turn is critical to improving the services' ability to deliver their core function - to protect the public, prevent crime, and save lives.

KEY FINDINGS

North American public safety organizations are mid-transformation

The challenges are clear – limited resources, increasing demand, growing security threats and elevated citizen expectations. Services are keen to embrace change, but the need to adapt while maintaining continuity of service is daunting.

Cloud is a game-changer

While IT professionals have heard more than enough hype around cloud, for Government safety agencies, cloud will transform the ability to share and collaborate. In a sector plagued by complex and aging legacy systems, the ability to share with colleagues and across agencies is critical – and is enabled by cloud.

Chatbots free up staff for emergencies

The role of chatbots to guide consumers through structured Q&A to provide a curated FAQ is well understood in the consumer sector. Chatbots can also be a huge help for handling the non-urgent enquiries to emergency services, freeing time and resources for actual emergencies.

Big Data and Artificial Intelligence can identify problems before they happen

The proliferation of data sources (video, social media, IoT, etc.) and the growing volume of new data created every day provides valuable new sources of insight for public safety services. When combined with AI/ML, this is enabling police, fire and emergency medical services to predict future problem locations.

Edge computing will become increasingly important

Police, Fire and Emergency Medical Services are by definition real-time activities. This means that some IT has to be delivered on-site, and increasingly this will involve edge and IoT technologies. These provide local solutions, eliminating the latencies and network risks of remote data centers.

CHALLENGES FACING EMERGENCY SERVICES

Public safety organizations are keen to become more efficient, more effective and more responsive to citizen needs. Their efforts to change are hampered by the fragmented structure of the sector, the limited funding available, and the age and complexity of supporting systems and processes.

BUDGETS

US Federal and local government spends around 4% of general spending on police, and together Police and Corrections has been the fifth or sixth largest category of US government spending for over 40 years. While absolute funding is broadly increasing over time, all government services are under sustained pressure to contain costs, become more efficient, and spend more of their funding on front-line services rather than on management and administrative overheads.

$20-30k

IT license costs saved annually by Clarkstown Police Department after moving 230 officers and staff to a cloud platform for collaboration

IT transformation has for many years been championed by industry and commerce as a lever to drive efficiency. Although public safety organizations have not been at the forefront of these changes, many departments and agencies are now looking to their systems to drive economies of scale. A very common starting point across all sectors is the shift towards cloud-delivered IT, often triggered when some aspect of legacy IT systems or equipment becomes irredeemably broken.

As other sectors have already found, not all systems are good candidates for moving to cloud, and in any case moving systems to cloud is not a magic source of cost reduction. What moving systems into cloud can do is reduce the risk of the investment, since all cloud solutions provide greater flexibility to accommodate unexpected future requirements. At the same time, some cloud services really are very low priced, and if these fit a need (for example, for IT testing) then there is potential for public service organizations to benefit from cost savings.

INFORMATION SILOS

Paper systems have been widely replaced by databases within federal IT and related public services, but these are still often designed around previous organizational structures, rather than current operational needs. This can leave police, fire and medical staff juggling multiple incompatible systems and wasting time on tasks such as duplicate data entry, document scanning and reuploading, etc. While this may be

necessary to capture important records staff still sometimes struggle to access case records, especially when on the move.

When lives, justice and the rule of law are at risk, it's essential that documents, records, evidence and data can all be shared quickly, easily and securely with authorized individuals. While this is partially true today for individual systems and their primary users, it's very common that collaborating colleagues from different services find it difficult and slow to share information about a location, incident or individual.

SPEED AND EFFICIENCY

The need for speed in handling true emergencies (i.e. Priority 1 calls) is fundamental, whether responding to fires, medical emergencies or stopping criminals.

Emergency medical units typically attend the scene of an incident within seven minutes of a 911 priority 1 call, and police respond on average within five to six minutes. Data on fire department response times is harder to assess, but for LAFD responses average a little over five minutes. Of course, location has a big impact, and medical emergency response times broadly double for incidents reported from rural locations.

Whatever the location, speedy response is essential, and underperforming systems and tools can become as much a hazard to citizens as traffic dangers or flash floods. When citizens and first responders alike have lives at risk, there is a growing intolerance of system- and database-caused delays.

TRUST AND SECURITY

Public safety services by definition need access to sensitive and personal data - medical, financial, legal, etc. However, data leaks from all manner of sources (banks, hotel groups, social media, etc.) have all highlighted the risks to data privacy. Unfortunately, federal IT services and public sector IT solutions are also not immune to breaches: in July 2019, the LAPD admitted that personal details of 20,000 serving officers and job applicants had been stolen by hackers.

In addition, government technology and public safety solutions are often high-risk / high-profile targets for malicious activity, attracting unwanted attention from cyber criminals and hacktivists alike – 2018 saw cyber-attacks on Baltimore's 911 service, and on Atlanta's criminal records systems.

Ultimately, citizen confidence is essential for public services to function effectively, but data privacy concerns remain widespread, and some more marginalized communities are wary of interacting with any uniformed services.

To restore faith among the general population, police forces in particular are adopting body cameras. In parallel, all public services are increasingly aware of the need to invest in securing their sensitive data assets, to align with compliance requirements, and to maintain the confidence of their communities.

BUSINESS AND TECHNOLOGY ENABLERS

FLEXIBLE IT

Business and industry have already embraced the flexible IT that cloud computing and as-a-service capabilities can deliver. In comparison, emergency services have been more cautious about adopting these solutions, partly through legitimate concerns around security and compliance.

Where IT-as-a-service is appropriate, it can significantly help to de-risk funding decisions, and allows public services to tailor their costs more closely to their (changing) needs. The US Marshals Service recently confirmed that it has almost completely moved its infrastructure to public cloud. Like many organizations, the USMS found that a few systems were unsuitable for cloud, and these have now been relocated to FBI data centers. This is a typical best-case outcome for many public sector IT services: a hybrid combination of traditional and flexible IT is often the optimal solution.

"We have bought our last set of hardware"

CIO, US Marshals Service, Karl Mathias

"Smart Cloud, Smart Government" workshop, August 14, 2019

DATA SHARING AND AGGREGATION

Sharing information is a critical part of enabling emergency staff to understand the full scope and context of issues they are dealing with. For example, the "Hub model" of multi-agency crime prevention is becoming widespread across Canada, enabling collaboration of public health, safety, law-enforcement and social professionals. In the hub model, proactive interventions are triggered by the Risk-driven Tracking Database, which helps communities collect together information on local risks, vulnerable groups and related factors. By sharing the data, services in each community are able to pre-empt issues for individuals before criminal or healthcare events can occur.

More systematic data sharing is also gaining traction for public sector IT solutions, and moving siloed data towards a single target environment is increasingly accepted as a strong first step toward making legitimate data access easier. The goal is to ensure that authorized staff can access the data they need wherever and whenever they need. By building mobility into the design of the new target systems, the services can also

support emergency telemedicine initiatives such as the mobile stroke units used at New York-Presbyterian Hospital.

Many public services are turning to cloud-based secure file sync and share platforms as an effective way to ensure that documents are available to authorized users. While these solutions are not new, initial adoption was slowed among safety agencies by concerns that sensitive data could get leaked. As cloud services have become more familiar with users and decision-makers, focus is moving from "what is the risk of this information being part of an un-authorized leak?" to "what is the risk of this information not being shared with someone who needs it in an emergency?".

ANALYTICS AND MACHINE LEARNING

Once consolidated, public safety data is a target for new analytics capabilities. These are able to highlight probable hotspots of activity, based on historic data. The City of Los Angeles is focusing on these capabilities as part of LAPD's 2020 strategic goals, expanding existing proven data-driven crime prevention methods from their initial focus areas to benefit all communities, alongside experimenting with data-driven traffic collision prevention programs. The force is also using machine learning to make analysis of video evidence more efficient, using ML software to highlight specific sections of recorded evidence for human review. This is becoming a critical requirement driven by the adoption of body-worn cameras mentioned earlier, since each camera can generate between 1GB-6GB of data in a single shift.

"Cutting-edge data-driven crime prevention programs"

Vision for LAPD in 2020, Mayor of Los Angeles, Eric Garcetti

The US Department of Homeland Security (DHS) is going further than machine learning, working with artificial intelligence on the challenge of reducing data overload on public services. The DHS is partnering with NASA's Jet Propulsion Laboratory, which has already developed its *Assistant for Understanding Data through Reasoning, Extraction, and Synthesis,* known as "AUDREY". Together, DHS and NASA are working to apply the AUDREY AI to data from first responder equipment and IoT sensors. AUDREY will then provide actionable recommendations to specific relevant field operatives, in a way and at a time that will not distract them from their task at hand.

AUTOMATION

Automation is also already commonplace in dispatching, and is being extended through robotic process automation to other tasks.

Chatbots are being tested as a way to handle non-urgent enquiries. Their role in providing answers to frequently asked questions is already familiar in retail and consumer settings and is equally applicable to public safety and health. Chatbots are also being tested to help triage calls waiting in queues, to ensure urgent calls are

prioritized. In some cases, automation is also being used to transcribe calls, sometimes as part of the legal disclosure process.

The widespread popularity of social media now means that public safety organizations are keen to communicate with citizens via platforms like Twitter and Facebook. This is a true two-way communication, since it allows public safety services to alert the public to potential risks. At the same time, it can also alert emergency services to unreported incidents through social listening. While many services still operate their social media accounts manually, some have adopted more specialist software. As an example, San Francisco Fire Department manages and partially automates their use of social media using a specialist SaaS cloud offering.

INTERNET OF THINGS

There is huge potential to apply Internet of Things ('IoT') approaches to public safety solutions, as a growing range of equipment, buildings and civic infrastructure is fitted with IoT sensors.

For example, IoT technologies are used in industry to track the location and status of expensive equipment, and public safety services are now beginning to do the same. This helps ensure that the location of critical equipment is known at all times, and increasingly also offers real-time information on operational performance.

Another widespread example is the use of unmanned drones, which are being used or trialed by many North American public safety services to provide remote visibility of potentially hazardous locations, and to monitor suspects, crowds and traffic. While there remains some public controversy regarding potential misuse, use continues to grow. In December 2018, the NYPD announced it was deploying 14 new drones, becoming one of over 910 US emergency agencies to acquire drones, according to the Center for the Study of the Drone at Bard College.

Separately, many law enforcement services have equipped staff with body-worn cameras to provide a record of their actions in context. While less common, helmet cams have also been specifically developed for use by firefighters, and these can help incident commanders get a quicker and more accurate understanding of an evolving situation.

47%

of US law enforcement agencies had acquired body-worn cameras in 2016

Body-Worn Cameras in Law Enforcement

CYBER SECURITY

All government IT services – and particularly in the public safety sector - need to be robustly secured, as the city of New Bedford Massachusetts learned this summer, when it became the target of a ransomware attack. Although fire department desktops were infected, only administrative tasks were disrupted. The city escaped a worse impact

because the attack occurred over the 4th of July holiday, when most IT was turned off. In this case the scheduling of the attack enabled the city's MIS team enough time to isolate the issue.

Historically, public sector technology investments in cyber security have been much more modest than those in the commercial sector. However, public safety services are a uniquely vulnerable part of the civil infrastructure that citizens would not want to see compromised, and this is plainly understood by the full spectrum of bad actors.

Public safety organizations are now well aware of the need to defend themselves from ransomware (a lesson widely leant from 2017's WannaCry exploit), while the NotPetya attacks are known to have significantly delayed medical treatments – a clear case of putting lives at risk.

The importance of emergency services can make them irresistible to cyber criminals. Public sector IT services have no choice but to match the high level of risk with significant investments in security, as a necessary element of service assurance.

CONCLUSIONS

Emergency services are under pressure to become more responsive, engage better with citizens, collaborate with each other to deliver joined up services and most of all deliver a more effective and more efficient service. Faced by this barrage of demands, public safety services are turning to technology with some success.

Flexible IT services are proving to be an effective way to future-proof IT investments. By pooling information using cloud services, police, fire and emergency medical organizations are becoming better at sharing information both internally and with other services. By deploying chatbots, services are reducing the load on their human operators, enabling them to spend more time on real emergencies.

As the volume of data from dash cams, body cams and helmet cams grows, public safety services are turning to machine learning to identify critical moments in video streams for further investigation. And with Big Data analytics, safety services are triangulating between multiple data sources to predict future problem locations.

Ultimately, the most important part of any emergency service is its people - technology is clearly a critical enabler helping steer North America towards a safer future.

ABOUT FUJITSU

Fujitsu is the leading Japanese information and communication technology (ICT) company, offering a full range of technology products, solutions, and services. More than 140,000 people at Fujitsu support customers in more than 100 countries. We use our experience and the power of ICT to shape the future of society with our customers. Fujitsu Limited (TSE: 6702) reported consolidated revenues of 4.0 trillion yen (US $36 billion) for the fiscal year ended March 31, 2019:

- 5th largest ICT service provider in the world
- global provider of managed services centers (5 distribution centers serving 160 countries, 40 languages, 24-hour services)
- among the top 10 global server manufacturers
- global portfolio of over 257,000 patents
- R&D investments of more than $2 billion per year
- 80 years of innovation

For more information, please visit www.fujitsu.com.

ABOUT FUJITSU AMERICA, INC.

Fujitsu America, Inc. is the parent and/or the management company of a group of Fujitsu-owned companies operating in North, Central and South America and Caribbean, dedicated to delivering the full range of Fujitsu products, solutions and services in ICT to our customers in the Western Hemisphere. These companies are collectively referred to as Fujitsu Americas.

Fujitsu promotes a Human Centric Intelligent Society, in which innovation is driven by the integration of people, information and infrastructure.

As a world-leading IT services and solutions provider for the Public Sector, Fujitsu delivers efficient and reliable solutions that make the most of restricted government budgets and has experience transforming services for end-users while reducing operating costs within the areas of; healthcare, education, policing, social services, environment, public safety, defense, etc.

Fujitsu provides a complete portfolio of business technology services, computing platforms, and industry solutions based on scalable, reliable and high-performance server, storage, software, point-of-sale, and mobile technologies. Fujitsu also offers end-to-end digital transformation drawing on the right skills and technologies, whether that's consultancy, testing, infrastructure, delivery, security, or ongoing managed services.

For more information, please visit: https://www.fujitsu.com/us/

ABOUT TEKNOWLOGY GROUP

teknowlogy Group is a leading independent research and consulting firm in the fields of digital transformation, software, and IT services. It brings together the expertise of three research and advisory firms: Ardour Consulting Group, CXP and PAC (Pierre Audoin Consultants).

We are a content-based company with strong consulting DNA. We are the preferred partner for Global user companies to define IT strategy, govern teams and projects, and de-risk technology choices that drive successful business transformation.

We have a second-to-none understanding of market trends and IT users' expectations. We help software vendors and IT services companies better shape, execute and promote their own strategy in coherence with market needs and in anticipation of tomorrow's expectations.

Capitalizing on more than 40 years of experience, we operate out of seven countries with a network of 140 experts.

For more information, please visit www.teknowlogy.com and follow us on Twitter or LinkedIn.

teknowlogy GROUP