WELCOME DISRUPTION

WHY PUBLIC SAFETY AGENCIES MUST FAST-TRACK INNOVATION
Public safety agencies—those responsible for policing, justice and national security—find themselves in the center of a digital storm that will disrupt every aspect of their operations. The question is whether they will emerge stronger—or significantly weakened—as a result.

The technological capabilities of the citizens they serve and the criminals they target are increasing at an unprecedented pace. Some agencies have made significant advances with emerging technologies such as analytics, but most—in particular those involved with policing and justice—are struggling to keep up with the pace of innovation and the relentless impact of digital disruption.

Criminal groups’ digital capabilities grow more sophisticated by the day. And citizens grow ever more fearful of the consequences. According to a recent Accenture cybersecurity survey, 65 percent of citizens lack confidence in the ability of law enforcement to investigate and prosecute cybercrime, while 30 percent of citizens report being victims of cybercrime.¹

Like businesses, criminals use digital capabilities to organize, expand their reach and create new markets and opportunities. Hacking and other forms of cybercrime are just one manifestation. Suddenly it is not just the physical world that must be policed, but the virtual as well. With this comes a new range of vulnerabilities that must be addressed, and new virtual communities that must be protected.

THE KNOWLEDGE GAP

32% of agencies agree that citizens are better informed about technology than their organization.
Community members nearly everywhere are mobile-savvy, for example. In the U.K., one in three adults regularly use their mobile device for shopping, and more people use it for banking than any other channel, digital or physical. Such behavior is starting to cross over to the public safety sphere—citizens use smartphones to record criminal activity, and seek the opportunity to share film clips and images easily with police. Footage taken from mobile devices helped identify the suspects in the Boston marathon bombing.

Put simply, public safety agencies can no longer delay in embracing emerging technologies. Inactivity and hesitation risks not only giving criminals the upper hand, but also reducing levels of citizen engagement and satisfaction. Harnessing the capability and potential of emerging technologies will require new thinking and potentially new approaches, but they represent an opportunity that is within agencies’ reach.

Gangs are skilled in using social media to communicate with and mobilize their members—a phenomenon that was seen as early as the U.K.’s 2011 London riots. The “dark web” is used to trade weapons (it has been reported that the recommissioned weapon used in the July 2016 shooting at a Munich shopping center was purchased on the dark web) and other illicit goods. According to a recent study, illegal drugs sales on “cryptomarket” sites tripled between 2013 and 2015 to about $250 million annually. Terrorists are digitally savvy, too, using the internet and social media to radicalize the vulnerable and disaffected and recruit them to their cause.

Meeting rising citizen expectations of better service delivery, meanwhile, is considered a top priority by public safety agencies, judging by a recent Accenture survey. Digital is driving demand from citizens for a faster, easier and more personal service, similar to their interactions with the private sector. They want to use digital channels more widely to engage with public safety agencies, including with the police.

The public can influence services indirectly, as we start to engage them more via digital channels.

Angus McCallum, CIO, Metropolitan Police Service (London, U.K.)
Public safety agencies can only meet these digital challenges by weaving people, processes and emerging technologies together. Encouragingly, a majority of survey respondents suggest they are aware of emerging technologies and are ready to make process changes to accommodate them. Far fewer, however, have made the workforce changes needed to implement the technologies. For their part, public safety staff themselves expect their agencies to embrace such technologies, believing them to be empowering rather than a threat to their jobs.

Machine learning, robotics and so on will have a great impact and may change roles that people will play. But it is difficult to foresee a point at which human intervention will not be necessary in decision-making and many key processes.

David Irvine, Former Director-General Australian Secret Intelligence Services
The generation of emerging technologies promises to liberate rather than displace. For example, much policing work remains manual, and the next waves of technology automation (eventually powered by artificial intelligence) will streamline case management and investigative processes.

Analytics can enable the rapid provision of actionable information about individuals and their histories to officers on the street. This gives officers the necessary context to deal with situations in front of them and helps them to make informed decisions in real-time. Robotics, meanwhile, can not only help with case processing but also with providing information and support to citizens. And emergent technologies such as blockchain have the potential to transform the security of transactions and the security of evidence continuity.

The potential is huge. Some wearables offer huge opportunity—particularly glasses, because they can supply information very quickly and readily in front of the user. So you could get a picture of someone and link it all the way back to a database and check, for example, if someone has just given the wrong name.

Angus McCallum, CIO, Metropolitan Police Service (London, U.K.)
This may sound futuristic, but some public safety agencies are actively piloting emerging technologies. Police forces are using predictive analytics, for example, to take “hotspot” analysis to new levels of sophistication. One such force is West Midlands Police in the U.K. “What we’re trying to do, first and foremost, is the analytics,” says Chief Constable Dave Thompson. “We’re analyzing the information we’ve got to better predict harm, risk, threats and direct results.”

Forces are also realizing the potential of video analytics—software that analyzes live and stored video footage to detect events. The use of video analytics and automation technologies by France’s National Police Force, for instance, has been shown to enhance existing safety measures at major events such as the Grande Braderie de Lille, the city’s annual market which is among the largest in Europe. In Singapore, meanwhile, advanced video analytics has been trialed to help the government manage public safety in large crowds and respond to incidents in real time.
Wearables and embedded sensors, which are becoming increasingly prolific—embodying the Internet of Things—are also being piloted, and are enabling real-time monitoring of situations in the field. In the U.S., the City of San Francisco has recorded a 35 percent reduction in firearms violence since deploying sensors in streetlights in 2014. The sensors detect and locate gunfire; alerts are then broadcast to dispatch centers and patrol cars so that they can respond.

The Accenture survey shows that predictive analytics are being widely piloted (by over half of agencies in the survey), and that piloting of video analytics, as well as biometrics and identity analytics, is also under way. Full deployment of all these technologies, however, is limited. It is important for agencies to be ready to move to mainstream implementation once the technologies are proven, and to be clear on what success criteria they need to achieve in order to move from piloting to full deployment.
Community policing can be greatly enhanced by emerging technologies. Survey respondents see the improvement of citizen engagement as a key benefit of investing in analytics and other emerging technologies: 28 percent say they have already seen this materialize, and 41 percent expect it to in the future.

In addition to helping agencies to prevent crime, advanced analytics can help them to better understand what citizens’ needs, perceptions and expectations are of public safety agencies. Effective use of mobile and social media tools—and more citizen-focused and interactive web portals—can expand communication channels and enable greater citizen cooperation in policing. All of this helps to reduce not only crime but also the fear of crime—thus helping to increase levels of public engagement and reassurance.

The public trust piece transcends everything. That’s the business we are in. Policing is and always will be a people’s business. And that is one job for us—to be able to restore that trust, to be able to engage the community, to help us do the job as well as it can be done.

Jim McDonnell, Sheriff, Los Angeles County Sheriff’s Department (U.S.)

Some of the ways we communicate, share problems, and share data and information about problems are through communities. They can empower themselves more around the information we give them.

Dave Thompson, Chief Constable, West Midlands Police (U.K.)
The Impact of Emerging Technologies

Of Public Safety IT leaders expect to achieve or have achieved increased citizen engagement and collaboration as a result of emerging technologies:

- **69%**
  - OF PUBLIC SAFETY IT LEADERS EXPECT TO ACHIEVE OR HAVE ACHIEVED INCREASED CITIZEN ENGAGEMENT AND COLLABORATION AS A RESULT OF EMERGING TECHNOLOGIES

- **90%**
  - OF PUBLIC SAFETY IT LEADERS EXPECT TO ACHIEVE OR HAVE ACHIEVED REDUCED COSTS THROUGH SMARTER WAYS OF WORKING AS A RESULT OF EMERGING TECHNOLOGIES

Public trust is at the heart of policing. Emerging technologies can help police forces not only win it but also keep it, allowing the police to embrace new forms of communication and wider transparency, sharing faster, further and in a more personalised way.

*James Slessor, Managing Director, Global Public Safety, Accenture*

*Of those which are piloting or implementing emerging technology projects*
NO EXCUSES

When public safety agencies’ technological innovation projects flounder, legacy systems often get the blame. Indeed, our survey respondents cite legacy as the dominant barrier to the implementation of emerging technologies. Platform and data-sharing technologies, however, have advanced to the stage where legacy systems and databases are no longer reasons for not using advanced analytics, mobile and other advancing technologies.

The value of legacy systems is largely in the data they contain. And now, it can be extracted, stored in a data warehouse or moved to the cloud or a data lake and readily searched and catalogued. Some agencies employ a two-track approach, keeping legacy applications running while deploying new ones on a wholly separate, flexible platform. Eventually, the data in the old systems is migrated to the new platform.

Top Three Barriers to Implementation

1. LEGACY SYSTEM INTEGRATION
2. LACK OF LEADERSHIP SUPPORT OR UNDERSTANDING OF POTENTIAL
3. LACK OF INTERNAL SKILLS OR ABILITY TO HIRE

Once upon a time, we built our IT around buying into software. Now, it’s a more app-driven world. It’s actually easier for us sometimes to build some cheap disposable software app-based work. We’re not building the great big legacy systems that police forces have done in the past. But I think for some of the tighter, more agile pieces of work, we’re likely to develop the capability to do it ourselves.

Dave Thompson, Chief Constable, West Midlands Police (U.K.)
ACCESS TO TALENT

Cultural resistance to change is a genuine impediment to innovation, but it too can be overcome. One way is by leveraging external assistance. For example, partnerships with universities, research institutes and private sector companies can bring outside expertise to bear in solving agencies’ technology-related problems. Accenture’s Innovation and Integration Partnership with West Midlands Police in the U.K. is an example of such a collaboration. And Accenture’s Analytical Innovation Lab, based in Singapore, acts as a hub for public safety agencies to master emerging technologies, and connects agencies with leading experts from around the world in order to learn from their experiences and share ideas.

Agencies can also call on online communities to help solve what to technologists are extremely interesting public safety challenges. This is an opportunity to test and prove their levels of innovation and the bounds to which they can push new technologies.

“Police agencies will never have their full suite of capabilities for all they need to do ... I certainly believe there’s a strong place for the private sector. That’s only going to grow in future years, because the cost of the public sector going on its own is going to be so prohibitive. It’s going to force public sector agencies to [build] these kind of partnerships. It’ll be for the better, in my view.”

Jon White, CEO, Australia New Zealand Policing Advisory Agency (Australia)

“We’re definitely recruiting on more of a digital pathway, taking on people who are headed to a digital profession, to deal with the sort of services we have to provide now for the work we do.”

Dave Thompson, Chief Constable, West Midlands Police (U.K.)
Seattle police, for example, conducted a public hackathon in December 2014 to work out how to redact video streams from officers’ body-cameras. In June 2015, Israel’s National Crime Unit took part in a similar event organized by Ben-Gurion University of the Negev; the event brought together more than 100 police officers and private security experts, as well as professional and amateur technology experts and hackers, with the goal of devising solutions to combat various forms of cybercrime.

More targeted recruiting and development practices are another way to bring about cultural change. Law enforcement may not always be able to offer private sector salaries, but young tech-savvy specialists are not motivated by financial packages alone—they are also interested in exciting technology challenges and a mission with real purpose.

Agencies need to adjust to a world of fluid talent recruitment. They must devise more flexible employment and incentive models to attract the right people for shorter periods of time. Secondment of employees from other sectors can also bring talent into agencies to help solve specific problems and question established processes.

You’ve got a lot of people who are stepping in from a generation of comfort with use of technology and confidence in it. That’s going to lead to a much broader cultural shift about how these things work.

Jon White, CEO, Australia New Zealand Policing Advisory Agency (Australia)
LEARN FAST, FOLLOW FAST

Public safety agencies do need to understand emerging technology and how it can be applied to deliver their outcomes, but they do not necessarily need to be ahead of the adoption curve. With restricted budgets and limited scope for taking risks, agencies can be “fast followers”—learning from early adopters in all sectors what works and what doesn’t, and adapting their implementation approaches accordingly.

They do, however, need to be out front in one area: understanding the potential criminal uses of emerging technologies. For example, horizon-scanners should be busy analyzing the potential criminal uses of machine learning and blockchain, among others, and proactively looking at and learning from others.

“One of my roles is setting up innovation days to understand the capabilities of some of these things, and where they might lead in the future. There’s sporadic knowledge at different levels in the organization, but it’s good for people to be able to see and touch and understand how other organizations—not just public sector organizations or police forces—are using them.”

Angus McCallum, CIO, Metropolitan Police Service (London, U.K.)
Police and other law enforcement bodies are inherently practical and innovative and demonstrate this in their everyday problem-solving. A small handful of agencies are beginning to apply analytics and other emerging technologies to enhance such problem-solving. They also need to share and collaborate among themselves. Their numbers must grow and the time lag reduced between new technologies’ emergence and their adoption. There is no other way to ensure that agencies will continue to be able to combat the threats to public safety effectively.

Learning and education, in this and other contexts, is the first step to understanding what emerging technologies can do, and what needs to be done to speed up their implementation. This is a need that is particularly acute at the senior and middle levels of management.

35% of agencies say that senior leaders are informed about emerging technologies and their potential.

Police officers are willing to do police work. They are not really keen on routines that are not important. They are keen to do something that is actually beneficial, so I think that they are willing to adopt it, but we have to start with education.

Anne Aaltonen, Assistant Police Commissioner (Finland)
In order to fast-track their innovation strategies, agencies must view the speed and scale of digital disruption as an opportunity as much as a threat.

In the digital world, legacy is no longer an excuse for delaying implementation, so swifter adoption of selected emerging technologies is a must. But so is the ability to find the right people to exploit these technologies.

Agencies need not be alone in finding the best way ahead: adopting technologies in collaboration with partners can often be the most productive approach.

Emerging technologies will not replace the activity of policing, but they have the power to make it more effective. They can free up resources on the front line, and help officers to make informed decisions in real time.

Emerging technologies, used in the right way, can also help to develop and build trust with citizens and communities.

Agencies don’t need to be first movers, but they do need to do their homework: by learning about emerging technologies and their success in other sectors, leaders will be better equipped to exploit their potential.

Those agencies that take these steps will emerge stronger from the digital storm: more connected to the people they serve and better able to outmaneuver the criminals they target.
Advanced analytics and predictive modeling
These techniques use algorithms that analyze data from past and present events in order to predict future events.

Video analytics
Software that analyzes live and stored video footage to detect events and alerts.

Intelligent process automation
This software copies other computers and humans, enabling clerical processing to be replaced by robots/automation that learn and complete processes.

Biometrics/identity analytics
This involves digitizing people’s physical characteristics—such as fingerprints, voiceprints and irises—as a way to identify them.

Machine learning
A feedback-loop process that enables computers to adapt the way they operate and predict a correct course of action.

Internet of Things
The connection of physical “objects” (devices, buildings, vehicles) that are embedded with sensors, network connectivity and software, which allows them to exchange data with each other or with centralized systems.

Natural language processing/generation
Software that analyzes human-generated text and live or recorded voices to look for patterns and extract meaning.
ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world’s largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 384,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

AUTHOR

James Slessor
MANAGING DIRECTOR, GLOBAL PUBLIC SAFETY

james.w.slessor@accenture.com
@slessor_james
https://uk.linkedin.com/in/jslessor

ABOUT THE RESEARCH

The Accenture Public Service Emerging Technologies research surveyed 774 IT leaders from public service organizations in nine countries (Australia, Finland, France, Germany, Japan, Norway, Singapore, the U.K., and the U.S.). The telephone survey (CATI) was conducted by Longitude Research between April and May 2016. The survey was supplemented by in-depth qualitative interviews with experts across these countries.

REFERENCES

1  Accenture Public Service Pulse Survey—Cybersecurity, 2016
3  Internet-facilitated drugs trade: An analysis of the size, scope and the role of the Netherlands. RAND Europe. 2016.
6  Mobile phone apps become the UK’s number one way to bank. BBA press release. 14 June 2015.
7  http://channel.nationalgeographic.com/inside-the-hunt-for-the-boston-bombers/articles/how-they-identified-the-bombers/
10 http://www.idc.com/getdoc.jsp?containerId=prUS41718216